CA Service Management - 14.1

CA Service Management Home

Date: 11-Mar-2016

Table of Contents

CA Service Management Home

Announcements & News

- CA Service Catalog 14.1.02 Cumulative Patch is now Available (https://docops.ca.com/display/CASM1401/2015/11/20/CA+Service+Catalog+14.1.02+Cumulative+Patch+is+now+Available)
- CA Service Management 14.1.02 is now Available (https://docops.ca.com/display/CASM1401/2015/11/09/CA+Service+Management+14.1.02+is+now+Available)
- Wiki Announcement: Availability of CA Service Management Mobile Application 3.1.4 (https://docops.ca.com/display/CASM1401/2015/02/26/Wiki+Announcement%3A+Availability+of+CA+Service+Management+Mobile+Application+3.1.4)

Implementing

Learn how to plan, install, and upgrade the product.

Administering

Learn about administering and configuring your product.

Using

Know more about how to use the different capabilities of the product.

Building

Learn how you can build and extend the product to suit your requirements.

Troubleshooting

Troubleshoot the issues yourself using the troubleshooting tips.

Integrating

Explore the products that you can integrate with and learn how to integrate the product.

Reference

Refer to the commands, table descriptions, CMDB reference, Web service APIs, and other reference information.

TechDocs, Courses, GreenBooks

Access the links to TechDocs, Greenbooks, and education courses.

Connect

Access the links to the user community, YouTube channel, Flipboard, and so on.

Release Information

This section shares the following information:

What's New in this Release

This section contains the following CA Service Management Release and Patching information regarding new features and enhancements:

CA Service Management Release 14.1.02 Enhancements

CA Service Management 14.1.02 is a cumulative patch for CA Service Management 14.1 release. It includes new features, enhancements, performance and security improvements, and bug fixes. For more information about how to install and avail enhancements for this patch, see Implement the CA Service Management Patch 14.1.02 (see page 686). You can download the patch from CA Support Online (https://support.ca.com/irj/portal/newhome).

Following are the new features and enhancements:

CA Service Desk Manager Enhancements

Environment Promotion

CA SDM Administrators can now promote customization, configuration, and application metadata changes (objects and attributes) across development, test, pre-production, and production systems. For example, you can promote the modified forms, new tables, columns, spel, majic files, object data to the production system.

For more information, see CA SDM Environment Promotion (see page 1372).

Save Search Filters

CA SDM now provides an option for analysts to save search conditions. These saved searches are displayed on the analysts' scoreboard. CA SDM search filters are available for all ticket types, announcements, contacts, workflow tasks, and Configuration Items. Search fields for such objects need not be defined every time a search is performed. Saving the search filters enable users to update search criteria values in the search form and save the filter values for further use.

For more information see, Save Search Filters (see page 2323).

User and Group Assignment

Incidents, Change Orders, Problems, and Requests details now have improved filters. The Assignee and Group filters are interdependent. If you select an assignee, the groups that are associated with this assignee are displayed in the **Group** field. Similarly, when you select a group, assignees associated with this group are displayed in the **Assignee** field.

For more information, see Incident Management. (see page 2080)

CA Asset Portfolio Management

Environment Promotion

CA APM Administrators can now promote configurations, searches, export definitions, lists, and content changes across development, test, pre-production, and production systems.

For more information, see CA APM Environment Promotion (see page 1669).

Unified Self-Service

Customize CA SDM Data Source Property

USS Administrators can now define the maximum number of CA SDM fields that a user can configure in the Unified Self-Service console.

For more information, see *Customize the CA SDM Data Source Property* in the How to Configure the CA SDM Data Source (see page 1688) section.

Configure Visibility of Communities

USS administrators can now enable or disable the **Communities** for all or specific tenants.

For more information, see *Enable or Disable the Community* in the How to Create and Manage Communities (see page 1696) section.

Manage User Password

USS users can now reset their password from the login page after it expires.

For more information, see Manage User Password. (see page 3248)

MDB Level Setting for CA Service Management

CA Service Management now provides you the capability to move MDB from the source system and configure it to work with the target system. For more information, see Move MDB Database from Source to the Target System (see page 747).

CA Service Management Common Patch Installer

Use the CA Service Management common patch installer to install CA Service Management 14.1.02 patch. For more information on how to install the patch, see Implementing CA Service Management 14.1.02. (see page 686)

SMPatchReport Utility

Use SMPatchReport utility to identify and list the CA Service Management product patches installed in your system. For more information, see Run SMPatchReport Utility to Get Installed Patches List. (see page 742)

Fixed Issues - 14.1.02

The following issues are fixed in CA Service Management 14.1.02.

- Issues Fixed in CA Service Desk Manager (see page 71)
- Issues Fixed in CA Asset Portfolio Management (see page 80)
- Issues Fixed in CA Service Catalog (see page 83)

Issues Fixed in CA Service Desk Manager

The CA Service Management 14.1 cumulative patch #2 (14.1.02) includes a number of fixes denoted by the CA Service Desk Manager component: Service Desk Server (USRD). The following table lists the defect fixes that are resolved in the cumulative patch. For more information, search the knowledge base on CA Support Online (http://support.ca.com/).

For more information about the fixes in the CA Service Desk Manager 14.1.01 patch, see CA Service Management Release 14.1.01 Patch Information (see page 104).

S. No.	Problem No.	Summary
1	USRD 432 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=432)	LDAP UPDATE NOT WORKING FOR CONTACT WITH SINGLE QUOTE
2		OUTER JOINS MISSING IN REPORTS

S. No.	Problem No.	Summary
	USRD 709 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=709)	
3	USRD 1071 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=1071)	CREATION OF INCIDENT WITH INCIDENT AREA FAILS FOR EMPLOYEE
4	USRD 1638 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=1638)	EVENTS AND NOTIFICATION RULES FROM SUPERTENANT DO NOT APPLY
5	USRD 1960 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=1960)	UTF8 TO MULTIBYTE STRING CONVERSION ERROR
6	USRD 1977 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=1977)	AHD04608 ERROR IS RETURNED WHEN DOING EDIT IN LIST
7	USRD 2122 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2122)	BLANK WEB REPORTS WHEN DATA PARTITION RESTRICTION ON IMPACT
8	USRD 2162 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2162)	CANNOT INITIALIZE STATUS FIELD FOR COPIED CHANGE ORDERS
9	USRD 2426 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2426)	SESSION COUNT MAY GO BELOW ZERO
10	USRD 2569 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2569)	IMAGES MISSING IN NOTIFICATION EMAILS
11	USRD 2723 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2723)	VIEW RISK SURVEY PAGE MIGHT NOT DISPLAY CORRECTLY
12	USRD 2842 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2842)	EXPORT BUTTON REMAINS DIMMED OR DISABLED
13	USRD 2906 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2906)	WIS 10901 ERROR WITH BOXI WEB INTELLIGENCE REPORTS
14	USRD 2908 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2908)	TABBING OUT OF ROOT CAUSE MAY NOT POPULATE UNIQUE VALUE
15	USRD 2911 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2911)	NAVIGATING TO NEXT KNOWLEDGE DOCUMENT PAGE MAY FAIL
16	USRD 2913 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2913)	SECONDARY SERVER USING UNEXPECTED HTMPL FILES
17	USRD 2917 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2917)	MISALIGNED ENTRIES IN MONTHLY VIEW OF CHANGE CALENDAR
18	USRD 2920 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2920)	LOOKUP NO LONGER WORKS AFTER AN AUTOSUGEST VALUE IS SELECTED
19	USRD 2921 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2921)	REGISTRATION ERROR WHILE UPDATING CONFIGURATION ITEM
20	USRD 2931 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2931)	KNOWLEDGE DOCUMENT TEMPLATE PAGE DISTORTS
21	USRD 2933 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2933)	SUMMARY FIELD MAY NOT WRAP FOR THE EMPLOYEE INTERFACE
22		

S. No.	Problem No.	Summary
	USRD 2936 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2936)	INCORRECT MENUBAR DISPLAYED IN QUICK PROFILE
23	USRD 2940 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2940)	LIST TITLE FONT MAY UNEXPECTEDLY CHANGE IN INTERNET EXPLORER
24	USRD 2950 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2950)	RUNNING PDM_CONFIGURE LEAVES TMP_SQL.SQL FILE IN LINUX
25	USRD 2953 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2953)	SLA TRIGGERS ON INACTIVE TICKETS
26	USRD 2954 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2954)	KNOWLEDGE SEARCH MAY FAIL WHEN CREATING A NEW TICKET
27	USRD 2960 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2960)	REDIRECTINGURL NOT PARSED
28	USRD 2961 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2961)	KD COMMENTS GET DUPLICATED
29	USRD 2963 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2963)	EXPORT BUTTON REMAINS DIMMED OR DISABLED WITH NON-IE BROWSER
30	USRD 2964 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2964)	AUTOCOMPLETE DOES NOT WORK UNDER CERTAIN CIRCUMSTANCES
31	USRD 2972 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2972)	INCORRECT NAME OF BUTTON ON REQUEST STATUS CHANGE PAGE
32	USRD 2975 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2975)	MISSING HTML MESSAGE IN TICKET NOTIFICATION
33	USRD 2976 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2976)	PDM_ISQL RETURNS ERROR WHEN PDMWEB.EXE IS RENAMED
34	USRD 2979 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2979)	VALUE OF FALSE ON EDIT IN LIST FILTER
35	USRD 2980 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2980)	INTERNAL LOGS SHOWN FOR EMPLOYEE\CUSTOMER VIA REST
36	USRD 2983 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2983)	CI BASED AUTO ASSIGN ALWAYS OVERRIDES WHILE EDITING A TICKET
37	USRD 2984 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2984)	REST DEPLOY FAILS WHEN COMMON_NAME ATTRIBUTE TYPE IS DOUBLE
38	USRD 2986 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2986)	TENANTED KNOWLEDGE ACTIVITY NOTIFICATION RULES MAY NOT FIRE
39	USRD 2987 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2987)	SHOW ENTIRE TREE BUTTON INCORRECTLY DISPLAYED
40	USRD 2988 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2988)	NOTIFICATION HISTORY NOT UPDATED FOR STAKEHOLDER CONTACT
41	USRD 2989 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2989)	INVALID NOTIFICATION RULES SHOWN FOR ACTIVITY NOTIFICATION

S. No.	Problem No.	Summary
42	USRD 2990 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2990)	INCOMPLETE DROPDOWN LIST IF CODE CONTAINS COMMA
43	USRD 2994 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2994)	NO WARNING ABOUT PENDING UPDATES ON CLOSE WINDOW
44	USRD 3000 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3000)	VISUALIZER REDIRECTS TO WRONG URL WHEN PDMWEB.EXE IS RENAMED
45	USRD 3005 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3005)	AHD04106 ERROR RETURNED WHEN RUNNING WEBI REPORT
46	USRD 3006 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3006)	TENANT VALUE CHANGED TO LOGGED IN USERS TENANT
47	USRD 3008 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3008)	BLANK DOCUMENTS MAY BE DISPLAYED ON KNOWLEDGE SEARCH
48	USRD 3013 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3013)	DISABLED CATEGORIES ARE SEEN WHEN COPYING A TICKET
49	USRD 3015 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3015)	AUTO CLOSE EVENT MIGHT NOT BE CANCELED
50	USRD 3016 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3016)	UNABLE TO ATTACH SERVICE PROVIDER CONFIGURATION ITEMS
51	USRD 3021 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3021)	EVENTS NOT GETTING TRIGGERED
52	USRD 3028 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3028)	GETOBJECTVALUES WEB SERVICES METHOD RETURNS DELETED DATA
53	USRD 3031 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3031)	WRONG EXPIRATION DATE MAY APPEAR IN REPORTS
54	USRD 3035 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3035)	SEARCH DOES NOT WORK WHEN SOME FIELDS ARE MADE DROPDOWN
55	USRD 3045 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3045)	ATTACHMENTS FAIL WHEN THE REMOTE REP_DAEMON DISCONNECTS
56	USRD 3046 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3046)	GRLOADER UPDATES LAST UPDATE DATE FIELD FOR CI
57	USRD 3047 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3047)	UNABLE TO SET CACHE-CONTROL HEADER TO DISABLE CASHING
58	USRD 3056 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3056)	CONTACT COPY MIGHT CREATE INCORECT GRPMEM RECORDS
59	USRD 3058 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3058)	SLUMP PROCESS ABNORMALLY TERMINATES ON SHUTDOWN
60	USRD 3062 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3062)	LOOKUP NOT TRIGGERING ONMOUSEOUT IN SEARCH LIST PAGE
61	USRD 3063 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3063)	UNABLE TO PERFORM ACTIONS WHEN TITLE PAGE IS REFRESHED IN IE
62		

S. No.	Problem No.	Summary
	USRD 3078 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3078)	AUTO ASSIGNMENT FAILURE REASONS TO TICKET ACTIVITY
63	USRD 3079 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3079)	INACTIVE RECORDS MIGHT BE RETURNED
64	USRD 3083 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3083)	ANALYST UNABLE TO NAVIGATE PAGES IN KNOWLEDGE SEARCH
65	USRD 3085 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3085)	EDIT IN LIST HEADER TEXT MAY DISPLAY INCORRECTLY
66	USRD 3117 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3117)	TAB SWITCH CAUSE SCROLL ISSUE WITH INTERNET EXPLORER
67	USRD 3124 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3124)	SLOW PERFORMANCE DUE TO QUEUED TRANSACTIONS ON UPDATE AGENT
68	USRD 3126 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3126)	ARGUMENT ERROR ON REWORKING PUBLISHED DOCUMENTS
69	USRD 3131 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3131)	PERFORMANCE PROBLEM WHEN VIEWING KNOWLEDGE DOCS
70	USRD 3135 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3135)	HTTP ERROR 414 REQUEST URL TOO LONG MESSAGE
71	USRD 3142 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3142)	KNOWLEDGE FILTER MAY NOT BE APPLIED CONSISTENTLY
72	USRD 3144 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3144)	UNABLE TO COPY A CHANGE CATEGORY AS A TENANT ADMINISTRATOR
73	USRD 3148 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3148)	LDAP SERVER CONTACTED WHILE LOGGING IN SSO ENVIRONMENT
74	USRD 3152 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3152)	HELP MENUBAR SUPPORT LINKS SHOW PAGE NOT FOUND ERROR
75	USRD 3161 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3161)	DELAYED SERVER RESPONSE WHEN DOING MANUAL NOTIFY
76	USRD 3163 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3163)	UNABLE TO SET PRIVATE SERVICE TYPES FOR A WF TEMPLATE
77	USRD 3167 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3167)	ARCHIVE PURGE RULE PROMPTS CONFUSING CONFIRMATION MESSAGE
78	USRD 3172 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3172)	BUSINESS_CASE COLUMN MISSING IN ISSUE TABLE
79	USRD 3173 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3173)	STORED QUERY MANGLED ON WEB INTERFACE
80	USRD 3194 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3194)	EMAIL ADDRESS CORRUPTED IN KNOWLEDGE NOTIFICATIONS
81	USRD 3200 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3200)	TWO WORKFLOW TASKS STATUS MAY SHOW PENDING
82		

S. No.	Problem No.	Summary
	USRD 3203 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3203)	MACRO SEARCH PAGE FOR EVENTS DISPLAYS BLANK PAGE
83	USRD 3206 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3206)	UNABLE TO UPLOAD FILES USING INTERNET EXPLORER 9
84	USRD 3210 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3210)	WORKFLOW TASK STAYS IN WAIT STATUS
85	USRD 3216 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3216)	INVALID SEARCH COUNT ON KNOWLEDGE SEARCH PAGE
86	USRD 3218 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3218)	KT_DAEMON MAY TERMINATE ON BACKGROUND SERVER
87	USRD 3227 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3227)	HOVERING OVER BUTTONS MAY DISTORT WEB PAGE
88	USRD 3228 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3228)	INCORRECT MESSAGE WHILE CHANGING TICKET STATUS
89	USRD 3229 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3229)	PAGE MAY HANG WHILE TRYING TO EDIT A ROLE
90	USRD 3230 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3230)	GARBLED CHARCTERS IN TICKETS CREATED VIA EMAIL
91	USRD 3231 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3231)	TENANT DROPDOWN LIST IS EMPTY
92	USRD 3233 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3233)	UNVALIDATED REDIRECTS AND FORWARDS
93	USRD 3234 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3234)	SURVEY SENT TO INACTIVE CONTACT
94	USRD 3235 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3235)	INCORRECT PREFERRED DOCUMENT USED IN QUICK PROFILE
95	USRD 3236 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3236)	AHD04796 ERROR WHILE TRYING TO EDIT ACCESS TYPE
96	USRD 3237 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3237)	UNABLE TO CREATE ATTACHMENTS VIA WEB SERVICES
97	USRD 3238 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3238)	GRLOADER FAILS TO CREATE CONFIGURATION ITEM WITH APOSTROPHE
98	USRD 3240 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3240)	HTML EDITOR BOX FOR ANNOUNCEMENTS MAY NOT WORK
99	USRD 3241 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3241)	PDM_LDAP_SYNC AND PDM_LDAP_IMPORT MAY FAIL
100	USRD 3242 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3242)	TENANT DROPDOWN MAY BE INCORRECTLY UPDATED
101	USRD 3243 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3243)	GRLOADER CREATES RELATIONSHIPS WITHOUT MANDATORY OPTIONS
102		

S. No.	Problem No.	Summary
	USRD 3245 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3245)	INCORRECT KNOWLEDGE DOCUMENT SEARCH COUNT
103	USRD 3246 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3246)	ADD LIMITED FEDERATED SEARCH TO KNOWLEDGE TAB
104	USRD 3247 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3247)	VALIDATING INTEGER DATA TYPE IN ARCHIVE PURGE RULE
105	USRD 3249 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3249)	MISSING FOCUS FOR THE FIRST FIELD OF A SUBTAB
106	USRD 3251 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3251)	EXCEPTIONS ON STARTING JAVAW PROCESS
107	USRD 3255 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3255)	USING EDIT IN LIST MAY START WORKFLOW TASKS INCORRECTLY
108	USRD 3256 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3256)	DOMSRVR MEMORY INCREASE
109	USRD 3257 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3257)	FAIL TO SET CATEGORY SYMBOL THROUGH WEB SERVICES
110	USRD 3258 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3258)	UNEXPECTED BEHAVIOUR ON CLICKING CAB CONSOLE BUTTON
111	USRD 3259 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3259)	WEB PAGE HANGS UPON CLICKING NAVIGATION BUTTONS CONTINUOUSLY
112	USRD 3261 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3261)	CONTACTS SEARCH PAGE APPEARS ON WORKFLOW DETAIL PAGE
113	USRD 3263 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3263)	INCORRECT FILES PROVIDED FOR ISSUE ACTIVITY
114	USRD 3264 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3264)	DOCUMENT LINK IS ALWAYS INSERTED IN FIRST LINE
115	USRD 3265 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3265)	ISSUE COPY FAILS WITH ILIMIT ERROR
116	USRD 3267 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3267)	KNOWLEDGE DOCUMENTS LOAD VERY SLOWLY
117	USRD 3268 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3268)	BOPSID VALIDATION FAILS INTERMITTENTLY
118	USRD 3269 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3269)	IMAGES ARE NOT VISIBLE IN KNOWLEDGE DOCUMENTS
119	USRD 3271 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3271)	SLUMP PROCESS MAY TERMINATE INTERMITTENTLY
120	USRD 3272 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3272)	OPTIONS ON RIGHT HAND SIDE OF LREL PAGE NOT SELECTABLE
121	USRD 3273 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3273)	CLEAR FILTER BUTTON DOES NOT WORK WITH INTERNET EXPLORER 9
122		

S. No.	Problem No.	Summary
	USRD 3274 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3274)	PRIORITY WITH SERVICE TYPE IN TICKET MAY DISTORT WEB PAGE
123	USRD 3275 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3275)	DOCUMENTS LOAD VERY SLOWLY IN A MULTI-TENANTED ENVIRONMENT
124	USRD 3278 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3278)	UNCLEARED WEBSESSIONS IN WSP WEBENGINE
125	USRD 3280 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3280)	FILE PUBLISH USING WSP FAILED WITH WEB DIRECTOR
126	USRD 3282 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3282)	WILDCARD SEARCH MAY NOT WORK USING GO BUTTON
127	USRD 3283 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3283)	PERFORMANCE ISSUES WITH SUPPORT AUTOMATION DOMSRVR
128	USRD 3284 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3284)	SCOREBOARD COUNT WRONG WITH STORED QUERIES CONTAINING BREL
129	USRD 3285 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3285)	TOMCAT MAY TERMINATE OR BECOME UNRESPONSIVE
130	USRD 3286 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3286)	PROPERTIES CHECKBOX MAY NOT BE CHECKED USING ENTER KEY
131	USRD 3292 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3292)	CMDB CLASSES WITH SAME NAME
132	USRD 3293 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3293)	INCORRECT CHARACTERS IN URL MAKE WEBENGINE UNRESPONSIVE
133	USRD 3295 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3295)	RESET FILTER ERROR IN KNOWLEDGE TAB OF CI DETAIL PAGE
134	USRD 3296 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3296)	ILIMIT ERROR WHILE CLOSING ALL CHILDREN
135	USRD 3297 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3297)	KNOWLEDGE REPORT CARD FOR ALL DAYS FAILS
136	USRD 3299 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3299)	UNABLE TO UPDATE THE TICKET CATEGORY THROUGH UPDATE URL
137	USRD 3300 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3300)	AUTOMATED POLICIES FOR VERSION 0 DOCUMENTS
138	USRD 3301 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3301)	DNS NAME AND MAC ADDRESS MISSING IN DISCOVERED ASSET LIST
139	USRD 3302 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3302)	SURVEY EMAIL MAY NOT BE RECEIVED
140	USRD 3304 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3304)	ILLEGAL COMPARISON ERROR SELECTING A CHANGE ORDER CATEGORY
141	USRD 3307 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3307)	ISSUE ACTIVITY LOG PREVIEW MAY OUTPUT ERROR
142		

S. No.	Problem No.	Summary
	USRD 3308 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3308)	DISCOVERED ASSET SEARCH RESULT PAGE MAY NOT LOAD
143	USRD 3309 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3309)	COLUMNS DO NOT LINE UP ON USING DTLSTARTROW
144	USRD 3310 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3310)	CANNOT COPY CHANGE CATEGORY WITH WORK FLOW TASKS
145	USRD 3311 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3311)	TICKET LINK IS ALWAYS INSERTED FIRST LINE
146	USRD 3314 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3314)	MANUAL NOTIFY FOR CUSTOM NOTIFICATION METHOD
147	USRD 3315 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3315)	DELETE MENU ITEM FOR NON-DELETABLE WORKFLOW TASK
148	USRD 3316 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3316)	CANNOT ADD CATEGORIES TO KNOWLEDGE SEARCH FILTER
149	USRD 3319 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3319)	GET_ROLES FAILED ERROR SEEN WHILE PROCESSING EMAIL
150	USRD 3320 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3320)	CONFIGURATION MAY NOT USE NX.ENV TEMPLATE FILE
151	USRD 3321 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3321)	BREL ATTRIBUTES CANNOT BE ACCESSED VIA WEB SERVICE CALLS
152	USRD 3325 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3325)	ROLE DETAIL WINDOW CLOSES ON SAVE
153	USRD 3327 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3327)	DIFFERENT ERROR MESSAGES FOR DIFFERENT LOGIN FAILURES
154	USRD 3329 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3329)	UPDATE GO RESOURCES BUTTON DOES NOT WORK
155	USRD 3330 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3330)	INSERT IMAGE WINDOW DOES NOT CLOSE ON COMPLETION
156	USRD 3331 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3331)	ALT+F DISPLAYS BOTH IE AND SDM MENUS
157	USRD 3333 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3333)	USERID CONTAINING COLON MAY OUTPUT ERROR ON LOGIN
158	USRD 3338 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3338)	WEB SERVICE TOMCAT TERMINATES INTERMITTENTLY
159	USRD 3339 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3339)	CUSTOM NOTIFICATION ARE NOT WORKING
160	USRD 3342 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3342)	WRONG ALIGNMENT OF FIELDS UNDER KNOWLEDGE TAB
161	USRD 3362 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3362)	WEBENGINE CONFIGURATION FILES OVERWRITTEN

Issues Fixed in CA Asset Portfolio Management

S. No.	Fix #.	Description
1	T5M7131	During configuration when the object level is set to read-only, the extension is editable.
2	T5GJ148	The data importer job is not using the primary and secondary lookup keys to lookup the values provided in the mappings, instead, it is changing the case-sensitivity of the values.
3	T5M7130	New extensions are unavailable for any configuration in the **Add Existing Fields** section.
4	T5M7130	Unable to create an asset import with simple and reference fields on the cost extensions.
5	T5XU059	When a data importer job fails, the exact record details that caused the failure are not displayed.
6	T5XU059	The following error message is displayed while creating a data importer job on Internet Explorer 11: TypeError: Unable to get property 'Style' of undefined or null reference.
7	T5M7130	During asset registration with CORA, the following error message appears in the registration service log: FATAL CA.Applications.RegistrationService.CORAProcessor - Error updating the usp_owned_resource record for asset XXXXXXXXXXXX."
8	T5M7130	A default configuration option is selected when the **Configuration Mode** is set to **ON**. Any change in the configuration selection returns to default if you navigate to another relationship object.
9	T5GJ146	An exception is triggered in a CA SAM-integrated environment because the query used in Common Asset Viewer (AMS) is incorrect.
10	T5XU058	The CSV file is not created for **Mass Change Jobs** when the contact's first name is listed but the value is set to blank.
11	T5UM105	The following error message is displayed when a tenant user exports the search results and tries to access the link that is mentioned in the export service email: The application cannot retrieve this file for the following reason: system.web.services.protocaols.SoapException. Server was unable to process request.
12	T5E2411	All the date formats are not specified in UTC (Coordinated Universal Time). Created Date and Last Updated Date use the UTC format, whereas Reconciliation Date and Discovery Last Run Date use the local time format.
13	T5E2411	The font of map fields required to create an import is bloated in Internet Explorer 9.
14		

S. No.	Fix #.	Description
	T5E241 1	In data importer during asset creation, the following error message is displayed when the class information is not provided for the model: Class information is required.
15	T5E241 1	Delay in data sync between CA SAM and CA APM as the time formats used in audit table and dx process are different.
16	T5M7 129	The German date format changes to the US date format when exported from an asset search result.
17	T57T002	In a tenant environment the cost page becomes unresponsive when you enter a value in the **Unit Amount** field and press Tab. The **Currency Type** drop-down expands repeatedly and the page becomes unusable.
18	T5GJ143	An environment with CA APM integrated with CA SAM, the following error is displayed on the CA APM configuration screen: FATAL CA.Common.Web - Unhandled Exception: Arithmetic overflow error converting numeric to data type numeric
19	T5M7 127	A data importer job fails when the mapping includes an extended field or a secondary lookup value.
20	T5UM 107	No criteria is defined in the reconciliation process to identify assets with the same serial number and different hostname.
21	T5XU062	Data importer displays the following error message when % is used as the input fields for mapping: No records found for Asset Family - %(Asset Asset Type) Value%
22	T5XU062	After you click **Add Fields** with the **Configure Mode** being set to **ON** for an audit history search, the asset extensions link is not listed on the Add Fields window.
23	T5GJ152	The deleted cost extension is displayed in the **Add Existing Fields** and not in the **Expose Hidden Fields**.
24	T5EM237	The following error message is displayed when you change the asset model class: **The application cannot retrieve this file for following reason - File is not accessible**.
25	T5EM237	Unable to sort the column **Log Details** in descending order in the **Import Jobs** section.
26	T5UM 110	Scroll bar is missing in some drop-down lists (for reference, Mass Change settings, and Data Importer destination field mapping).
27	T5EM238	In data importer, updating location details on an asset fails when the Main Destination Object is set to Asset (All Families).
28		

S. No.	Fix #.	Description
	T5UM109	Irrespective of the actual payment amount, the **Legal Document Payment Due** always displays zero.
29	T5UM108	When a custom relationship is added to a configuration, the relationship count is incorrect in the **Asset** menu.
30	T57T038	The events that are triggered from CA APM took long to sync with CA SAM.
31	T57T012	Unprocessed events are excluded from the **Event Service**.
32	T57T023 T57T029	System faces memory issues when huge number of records are imported on asset and contact objects using data importer.
33	T5EM242	When any user other than the UAPM admin navigates to the **Administration** tab, the following error message is displayed: An unexpected error has occurred. Length cannot be less than zero. Parameter name: length
34	T5EM242	**Hardware Asset Family** subclasses are displayed as classes.
35	T5EM241	The SSL configuration for CA SAM end-point binding is not set-up.
36	T57I127	The last character of the asset name is duplicated when you delete any character except the last character from the asset name and on pressing Tab.
37	T57I126	Unable to enter '#' and '$' symbols in the required fields in Internet Explorer 11.
38	T5EM241	ITAM login credentials are saved in the cache.
39	T5EM241	The application does not validate the permissions while accessing the **System Configuration** page in the **Administration** tab.
40	T57T033	Asset update fails when the asset creator does not exist on the CA contact table.
41		The **Role Contact** pane on the **Role Management** page displays inactive contacts

S. No.	Fix #.	Description
	T57T009	
42	T57T012	Data importer imports the records even when there is no change in the data record.
43	T5E2411	The following error message appears when you save an asset after selecting the last name for a custom legal hold blue box: Another user updated this record after it was loaded.

Issues Fixed in CA Service Catalog

S. No.	Problem No.	Summary
1.	R14.1.02	Form Designer API update: "Note that the Predefined JavaScript Functions for fields and labels will not work if used as table columns".
2.	T52W137	IXUtil is slow when importing services and forms.
3.	T52W133	Slow key events experienced in IE11 for USS catalog user search page.
4.	T52W133	Duplicate items are shown in recent requests page of USS.
5.	T52W129	Users who log in using domain name are unable to add notes (comments) and attachments to any request.
6.	T52W126	Cannot load Catalog Capabilities from Mobile Application.
7.	T52W124	Chrome browser shows an error when a SOG is saved from CA Service Catalog UI.
8.	T52W133	Progress indicator remains on a page even after acknowledgement for any validation error that occurs in a form.
9.	T52W118	When a user tries to approve or fulfill a request, all data in the request information form is lost.
10	T52W116	USS common Admin **Manage users** capability does not set admin role to the users.
11	T52W115	Progress indicator does not disappear for some requests in USS that are using the ca_reportQuery method on OnLoad of the form.
12	T52W109	Radio button is misaligned in USS.
13	T52W104	In system forms like **Request Information**, form values are appended with **-0** and **-1** at the end.
14	T52W117	Unable to submit large forms with long text in USS.

S. No.	Problem No.	Summary
15	T5JH221	Offering description is missing in the USS offering page. Offering name appears as junk character in the USS portal. Unable to expand the Feature offering tree node after two level of folder hierarchy.
16	T5JH230	UUID value appears as a junk character in the form select field. Using the Web Service call UUID appears as a junk character.
17	T5JH231	The **Requested for** field is shown as a plain text box and not as Magnify glass. The $5 character is getting appended in the Overview text. In IE11, page navigation arrow is not working.
18	T5JH235	Submit button is not greyed out upon clicking. As a result, the user can submit the request multiple times.
19	T5JH236	The **Add to cart** button is not greyed out upon clicking. Consequently, a user can add multiple requests to the cart.
20	T5JH237	SDM inactive category is shown in CA Service Catalog plug-in.
21	T5JH241	SDM analysts unable to see attachment from CA Service Catalog.
22	T52W139	USM_Request_Status entries are mixed up and status_old is set to -1 if the service option of a request in pending approval state is edited by the service designer.
23	T52W139	Request submission takes three minutes to complete.
24	T52W139	It is not possible to edit a user profile especially, the phone number field. For example, editing 123ext456.
25	T52W139	Audit Trail history is showing wrong information about the service offering.
26	T52W139	RollBack is deleting new price in invoice.
27	T52W139	Drop-down search field in a form will not display properly when searching users by first name, last name, and user ID.
28	T52W125 T6DR008	The form is not loaded on the request page, when a service offering has only a SOG and an option with form attached to it.
29	T52W133	Lookup fields must not be editable and values must only be selected from the popup window.
30	T5ES163	Unable to change the back ground color of the forms.
31	T5ES161	If a service offering has more than one SOG and if any of the SOG has a single option, there is no way to deselect this option as part of request submission as the corresponding checkbox is removed.
32	R14.1.02	Radio buttons are not aligned properly with the main label for the radio group.
33	T58S083	CA SDM change order does not open seamlessly from CA Service Catalog request using related ticket link.
34	T58S081	CA Service Catalog freezes upon tandem request submission by three or more users.

S. No.	Problem No.	Summary
35	T58S088	Request Manager is unable to approve request in USS.
36	T58S106	CA PAM Processes initiated from CA Service Catalog are not archived.
37	T58S102	CA Service Catalog widget throws a script error when used in USS.
38	T58S107	Form data is lost.
39	T58S108	CA SDM Ticket Link is not displayed for Catalog request.
40	T58S109	USS request item status is not displayed.
41	T58S113	Single-Sign On (SSO) user is stripped off domain attribute.
42	T58S114	Mobile APP fails to login in SSO.
43	R14.1.02	Request gets stuck at approval or fulfillment phase if service definition is edited after request submission.
44	T58S121	Port Form Caching and Performance Improvements.

Known Issues - 14.1.02

The following known issues are specific to the CA Service Management Release 14.1.02:

- CA Service Desk Manager (see page 85)
- CA Asset Portfolio Management (see page 88)
- CA Service Catalog (see page 90)

CA Service Desk Manager

Symptom:

The Description pop-up of Data Export does not automatically close when you log out of CA Service Desk Manager or close the browser.

Solution:

Manually close the pop-up window.

Symptom:

Save a filter with an assignee name that is different from the logged in user name. Now, edit the same filter, the Assignee field appears blank.

Solution:

There is no workaround.

Symptom:

When performing data export you may encounter a MAX DEPTH level error.

For example: Data export reached to MAX DEPTH level 20 for factory lrel_att_ctplist_macro_ntf. Increase the MAX DEPTH value in the *<NX_ROOT>/pdmconf/export.cfg* file to get data for dependent factories.

Solution:

Increase value of the MAX DEPTH parameter in the *export.cfg* file located at *<NX_ROOT>/pdmconf/*.

Symptom:

If you have done a schema change in development and production systems, but have not used the exact names between the systems, for example **zTest** vs **zTEST**. In such a scenario, the *pdm_publish* fails because of a duplicate schema name found. The environment promotion process exits.

Solution:

Ensure that level set is done on the source and target systems.

Symptom:

If the CA SDM Environment Promotion processes for export, import, or dryrun are interrupted unexpectedly, the *<export_import_path>/Promotion* folder retains the footprint of the incomplete process.

Solution:

Manually remove the following folders:

<export_import_path>/Promotion/Export/sdmp_export_yymmdd_hhmmss

<export_import_path>/Promotion/Import/sdmp_import_yymmdd_hhmmss

<export_import_path>/Promotion/Export/DB/sdmp_db_data_export_yymmdd_hhmmss

<export_import_path>/Promotion/Dryrun/Dryrunyymmdd_hhmmss

Symptom:

The BHVTPL value for WFTPL is displayed as CODE (Integer) during the import process.

Solution:

Restart the CA SDM service.

Symptom:

Multiple object selection across pages is not supported.

Solution:

Click View All, to view all the objects on the same page and select the required objects to export.

Symptom:

When you execute the command *pdm_load –r –f tucson_delete.dat* while performing the post installation steps, you may encounter an error based on your system configuration.

For example:

```
ERROR: Error 15 on deleting row.

Problem row:


Error 1 on update, insert or delete done.
```

Solution:

Ignore the errors and proceed with the post installation steps.

Symptom: You may encounter errors or may see missing links between the objects while importing.

For example, you may encounter the following error for missing link between a macro and evt objects:

```
Error: Failed to create LREL for source : [ lrel_true_action_act_t:12409 ],  and
attribute : [ macro='macro:12020' and evt is null ] .  Reason : INVALID
```

The missing link errors may occur due to the following reasons:

- Reason 1: When the link between the objects is missing on the source system.
- Reason 2: When the link between the objects exist on the source system but is missing on the target system.

Solution:

Solution 1: Ignore the error when the link is missing on the source system.

Solution 2: Manually update the link when it is missing on the target system.

Symptom: When you export an object without exporting the dependent objects, you may encounter errors while importing.

Solution: Always export the dependent objects before you export the parent object. Also, when you import, ensure that the dependent objects are imported before you import the parent object.

For example, before exporting the *chgcat* object, export the *tskstat* and *tskty* objects. While importing, ensure that you import *tskstat* and *tskty* objects before importing *chgcat* object.

Symptom: When you import the *risk_level* or *prptpl* object, you may encounter the following error:

For example:

```
Detail message : AHD04116:A duplicate record was encountered. Insert or Update failed.
SDMP10012 : Error while importing record for persistent id : risk_level:100
```

Solution:

- Navigate to the *NX_ROOT\pdmconf* folder and update the following values in these files on the source and target systems:
  - *dbpromote.uniquekey* file:
    - risk_level.uniquekey=enum
    - prptpl.uniquekey=object_type, object_attrname, object_attrval, sequence
  - *DBImport.properties* file:
    - resolve.prptpl.attributes=object_attrval
- Perform export and import again.

Symptom: O n the Non-Windows Advanced Availability server, importing the configuration or customization changes does not automatically start the CA SDM services.

You may see the following message for a while and observe that the services do not start:

Starting the CA SDM service. Please wait until the service starts completely.

Solution:

Follow these steps:

1. Interrupt the import process.
2. Start the CA SDM services manually and perform a failover.

CA Asset Portfolio Management

Symptom: During CA APM Environment Promotion Export, the contact must have a user ID that is associated with it, when the filter value is set to **Last Modified User**. If the condition fails, the search criteria ignores the **Last Modified User** filter and all the records are displayed.

Solution: There is no workaround.

Symptom: Unable to create a new event in CA APM 14.1.02. The follow error appears on the event creation screen: *The type initializer for CA.Common.Workflow.Provider.ProviderManager threw an exception.*

Solution:

Follow these steps:

1. Log in to CA ITAM application server.
2. Stop the CA Asset Portfolio Management - Event Service
3. Navigate to the *Root/Event Service* folder.
4. Open the *CA.Applications.EventService.exe.config* file.
5. Modify the Current Key with the New Key.
   Current Key:

   ```
   defaultProvider="CA IT Process Automation Manager r4.0/r4.1"
   ```

   New Key:

   ```
   defaultProvider="CA IT Process Automation Manager"
   ```

6. Modify the Current Key with the New Key.
   Current Key:

   ```
   name="CA IT Process Automation Manager r4.0/r4.1"
   ```

   New Key:

   ```
   name="CA IT Process Automation Manager"
   ```

7. Start the CA Asset Portfolio Management - Event Service.
8. Log in to the CA ITAM web server.
9. Navigate to the *Root/Web Server* folder
10. Open the *Web.config* file.
11. Modify the Current Key with the New Key.
    Current Key:

    ```
    defaultProvider="CA IT Process Automation Manager r4.0/r4.1"
    ```

    New Key:

    ```
    defaultProvider="CA IT Process Automation Manager"
    ```

12. Modify the Current Key with the New Key.
    Current Key:

    ```
    name="CA IT Process Automation Manager r4.0/r4.1"
    ```

    New Key:

```
name="CA IT Process Automation Manager"
```

13. Execute the following command to stop and restart IIS services on the web server:

```
iisreset
```

Symptom: Environment Promotion Import process fails and the following error message appears when the application server name registered in al_cdb_configurationparameters table is set to FQDN (fully qualified domain name) :

This utility can be executed only on the APM Component server. Exiting the application as the current server is not the component server.

Solution:

Follow these steps:

1. Log in to system database (MDB).
2. Run the following script:

```
UPDATE al_cdb_configurationparameters
SET configvalue = '{Component server machine name}'
WHERE componentkey='Application_Server' AND configkey='ComponentServerName'
```

3. Execute the following command to stop and restart IIS services on the application server:

```
iisreset
```

CA Service Catalog

Symptom: The offering in the **Requests** page on the CA Service Catalog UI are unavailable when the Microsoft SQL Server has a non-default MDB name.

Solution:

Scenario 1: If you are installing 14.1.02 on CA Service Management 14.1:

Follow these steps:

1. Log in to the database as sa user using MS SQL Server Management Studio.
2. Open the *USMHOME/REPLACED/CA_SLCM_r14.1.02.OLD/unconfigureMDB /configureMSSQLMDB-SP1.sql* file.
3. Copy and execute the file content in Microsoft SQL Server.
4. Open the *USMHOME/REPLACED/CA_SLCM_r14.1.02.OLD/unconfigureMDB /configureMSSQLMDB-SP2.sql* file.
5. Copy and execute the file content in Microsoft SQL Server.
6. Restart the CA Service Catalog Windows Service.

Scenario 2: If you are installing 14.1.02 on CA Service Management 14.1.01:

Follow these steps:

1. Log in to the database as sa user using MS SQL Server Management Studio.
2. Open the *USMHOME/REPLACED/CA_SLCM_r14.1.02.OLD/unconfigureMDB /configureMSSQLMDB-SP2.sql* file.
3. Copy and execute the file content in Microsoft SQL Server.
4. Restart the CA Service Catalog Windows Service.

CA Service Management Release 14.1.01 Enhancements

CA Service Management Release 14.1.01 Enhancements

The following new features and enhancements are only available if you apply the patch for CA Service Management Release 14.1.01. Find the patch and the download details from CA Support Online.

CA Service Desk Manager Enhancements

Call Service Desk from Mobile

CA SDM mobile application users can use the Call Service Desk feature to contact the CA Service Management service desk or help desk. Administrators must configure or customize the service desk number using the Options Manager. To enable the options, see Call Service Desk options (see page 1308). For more information about calling service desk, see Call Service Desk from your Mobile Device (see page 3176) topic.

Show To and Cc List Recipients in the Email Notification

You can now view all the recipients of an email notification. For manual email notification, both To and Cc list recipients are displayed and for automatic email notification, only To list recipients are displayed. For this feature to be enabled, install the **mail_show_to_cc_list** option from Options Manager. If you do not install this option, you can only add recipients in the To list **.** For more information, see the Create a Manual Notification (see page 842) topic.

Note: Pager email notification method does not support the listing of all the recipients in To or CC list.

Add Attachments and URLs to a Manual Notification

Attach a local document or URL to a manual notification that is being sent to an end user. For example, the attachment can contain steps to resolve an incident. For audit purposes, the document being sent as part of the manual notification should also be attached to the parent ticket. The

attachment associated with the manual notification will be delivered as an email attachment in the inbox of the recipient. Ensure that the attachment adheres to the email server configuration of the sender and the receiver. For example, size of the file, extension of the file, and so on. If the attachment does not meet these requirements, the manual notification email may get rejected.

For this feature to be enabled, install the **mail_allow_attmnts** option from Options Manager. For more information about the considerations and how to attach the document or URL, see the Create a Manual Notification (see page 842) topic.

Attach Classic Workflow to Each Ticket Type Area

You can attach a classic workflow with each of the request, problem, incident areas. This feature also enables you to attach Request/ Incident/ Problem workflow tasks to events, macros, and notifications as the object type. The procedure to attach the workflow remains the same as attaching it to issue and change order categories. Find more information, see Attach a Classic Workflow on Define a Category or Area (see page 1054) page.

Attach CA Process Automation Workflow to Each Ticket Type Area

You can attach a CA Process Automation workflow with each of the request, problem, incident areas. Find more information, see Attach a CA Process Automation Workflow on Define a Category or Area (see page 1054) page.

Note: For the same ticket area you can attach a Classic workflow or a CA Process Automation workflow for each ticket object (Request/Incident/Problem). For example, for the same area, you can attach a Classic workflow to a request and CA Process Automation workflow to a problem or incident.

Add Attachments to a Configuration Item

Attachment tab support is available for Configuration Item (CI). This feature enables you to attach documents and URLs to a CI. Notifications are sent to the users when an attachment is attached or removed from the CI. For more information, see Attachments (see page 2476).

CA Service Catalog Enhancements

Search Forms

This feature enables user to search for a specific form in Forms Designer page. Form Display name or Folder name can be used to search the form. The search mechanism provides auto suggestion as the user types search terms in the form search text box. The search functionality is case-insensitive and the search results are displayed in hierarchical manner. For more information, see Search Forms (see page 2914).

Form Associations

The **Associations** tab in the Form Designer UI provides the list of service offerings and service option groups that are associated with the selected form. It provides the ability to view where a particular form is used in the current Business Unit and also the capability to assess the impact of modifying or deleting a form. This functionality is also available in the Form Chooser UI when attaching a form to a Service Option. For more information, see Create and Maintain Forms (see page 2986).

Configuration options for displaying or hiding SOG and Form display names

To hide or display the Service Option Group name, a check-box **Hide SOG name** is now provided in the details tab of the offering. This option is enabled only when an offering has a single Service Option Group. In case of multiple service option groups in offering, this option is disabled or greyed out by default. Checking or unchecking this option will not alter the offering preview. An option called **Display Form name** is provided in the Form Chooser UI when attaching a form to a Service Option to show or hide the form name. This option is dependent on System Configuration settings. If the administrator has disabled the form name display option at the System Configuration level, the form name is not displayed, even if the **Display Form name** option is checked. For more information, see Display or hide the Service Option Group Name (see page 2999) and Fields for Form Elements (see page)

New and Flat Icons

The Out of the Box (OOTB) Catalog content, CA Service Management Content Pack & CA Service Management Administration content pack is enhanced to include new and flat icons in the service offering definitions. The patch will re-import the OOTB content implicitly as part of the patch install, however CA Service Management Content Pack & CA Service Management Administration content pack will be imported based on the Administrator choice while installing the patch.

Email Notifications

CA Service Catalog now provides the capability to send email notification to end users and approvers when a note and/or attachment is added or modified for a request or an issue. The capability is provided based on a set of newly added Event-Rule-Actions which can be enabled or disabled as required. For more information, see Add Notes and Attachments (see page). The following are the Event-Rule-Actions:

- Notes Create (see page)
- Notes Change (see page)
- Attachment Create (see page 94)
- Attachment Change (see page)

Notes Create

This event type occurs when a note is created for a CA Service Catalog request. Rules associated with this event type are as follows:

- **When a note is added to a CA Service Catalog request**: When a note is added to a CA Service Catalog request, email notifications are sent.

- **When notes are added to a CA Service Catalog request**: When a note is added to a CA Service Catalog request, it is also synchronized with the corresponding CA Service Desk Manager ticket.
- **When a CA Service Desk note is synchronized to a CA Service Catalog request**: When CA Service Desk Manager (CA SDM) note is synchronized to CA Service Catalog request, email notifications are sent.

Notes Change

These event types occur when a Note is changed or modified for a request. The following rules are associated with this event type:

- **When note with attachment(s) is edited in a CA Service Catalog request**: When a note with attachment(s) is edited in CA Service Catalog request, E-Mail notifications are sent.
- **When note without attachment(s) is edited in a CA Service Catalog request**: When a note without attachment(s) is edited in CA Service Catalog request, E-Mail notifications are sent.

The Notes Create and Notes Change Events have the following parameters:

Event Parameter	Meaning	Example
$source_id$	The request ID of the corresponding note.	10510
$note_text$	Description of the note.	
$ignore_notification$	Value will be true in the following cases: ▪ on submission of a request that has note(s). ▪ when a note event is triggered for a comment with notes and attachments posted in Widgets.	

Attachment Create

This event type occurs when an attachment is created for a request. Rules associated with this event type are as follows:

- **When attachment is added to CA Service Catalog request**: When an attachment is added to a CA Service Catalog request, it is added as a link to the corresponding CA Service Desk Manager ticket.
- **When attachment is added to a CA Service Catalog request**: When an attachment is added to a CA Service Catalog request, email notification is sent.
- **When note and attachment(s) are added to a CA Service Catalog request**: When note (s) and attachment(s) are added to a CA Service Catalog request from Widgets, email notifications are sent.

- **When a CA Service Desk Manager attachment is synchronized to a CA Service Catalog request**: When a CA Service Desk Manager attachment is synchronized to CA Service Catalog request, email notifications are sent.

Attachment Change

This event type occurs when an attachment is changed for a CA Service Catalog request. Following rule is associated with this event type:

- **When attachment associated with a CA Service Catalog request is edited**: When an attachment associated with a CA Service Catalog request is edited, email notifications are sent.

The Attachment Create and Attachment Change events have the following event parameters:

Event Parameter	Meaning	Example
$object_id$	The request ID of the corresponding attachment.	10510
$ignore_notification$	Value will be true in the following cases: ▪ on submission of a request that has attachment(s). ▪ for the first n-1 attachments when a comment with n attachments is posted in Widgets.	Example: If a comment in Widgets has 1 note and 5 attachments, for the first four attachments (n-1=4), the value will be true.
$attachment_url$	Specifies the URL(s) of the uploaded attachment(s).	

Request Details Link for Email Notifications

By default, value for this parameter is not configured. This parameter can be configured in the following format if CA Service Catalog is configured with USS:

http://<USS HostName>:<PortNumber>/web/frontoffice/myrequest-catalog?ServiceCatalogRequestID=

If Unified Self-Service (USS) URL is configured for Request Details Link for E-Mail Notifications, clicking on the request details hyperlinks in the email notification will take to the Unified Self-Service login page instead of CA Service Catalog login page. If this parameter is not configured, clicking on the hyperlinks in email notification with request details takes to the CA Service Catalog Login page.

Edit Completed Requests

A new configuration item Edit Completed requests is added in the **Catalog**, **Configuration**, **Request Configuration UI**. For more information, see Request Management Configuration Parameters (see page 1456). The following values are applicable for this configuration item:

- True – Completed requests can be edited.
- False - Completed requests cannot be edited.

Edit Cancelled Requests

A new configuration item Edit Cancelled requests is added in the **Catalog**, **Configuration**, **Request Configuration UI**. For more information, see Request Management Configuration Parameters (see page 1456).

- True – Cancelled requests can be edited.
- False - Cancelled requests cannot be edited.

Include in Email Notification

In Form Designer, a new attribute is introduced for every form element. This element attribute is used to display a field or component value, including the label in email content. Specify the value as true or false. When the value is set to true, the field or component value is visible in the email. To set or edit this attribute, you must have admin rights. Navigate to Catalog, Forms, select the Form Component and click on the Include in Email attribute. You can use the JavaScript expressions to specify the value as a condition for the Include in Email Notification attribute too. For more information, see Include In Email Notification (see page).

When you set the **Hidden** and **Include in Email Notification element attribute** to true/false in the CA Service Catalog UI, the following is reflected in UI and email notifications:

Hidden	Include in Email Notification	Result
true	true	Form component is not displayed anywhere.
true	false	Form component is not displayed anywhere.
false	true	Form Component and value is displayed in the Form Designer and the Request Form while raising a request, and also in the email notification.
false	false	Form component appears in the Request Form UI and the Form Designer UI, but the component value is not displayed in Email Notifications.

Locale Support for Request Email Action

A new option to choose the locale or language of an Email is added to the standard out of the box Event-Rule-Action set for Request Email. It allows the Request Email Action to choose the language for sending request emails. This capability offers great flexibility as it overcomes the limitation of sending request emails in just one locale. CA Service Catalog Administrators can select the language for sending the Request Email.

- Parameter Name: Choose Email Language
- Type of UI Control: Select Box (Drop down list)
- Options: All supported languages with a special option of Browser Language.
  Browser Language option for email language ensures that the Request Email is sent in the browser language at the time the request is submitted. For example, if a Request Email action is configured with Email language set to Browser Language, the Request Email sent for request submission from a browser supporting French language will be in French.
- English
- French
- German
- Spanish
- Italian
- Chinese
- Japanese
- Brazilian Portuguese
- Dutch
- Finnish
- Danish
- Swedish
- **Browser Language**

How to Specify the Email Subject in a Localized Form

When the **Browser Language** option is chosen as the Email Language, it is apparent that the same Request Email action sends out Email notification in any of the supported locales based on requester' s browser language. This option is very useful in a multi-lingual environment with globally distributed CA Service Catalog users. Since, the same Request Email Action is used to send emails in any of the supported locale, the subject and message of an Email must be given in the locales that you require.

Both the Subject and Message fields accept the following format:

```
<Language code1> :< Language specific subject1>|! <Language code2> :< Language specific subject2>….
```

Note: The character **|!** Is the separator that separates subject line of two different languages.

Standard Language Codes

Language	Code
English	Icusen
French	Icfrfr
German	Icdede
Spanish	Icdede
Italian	Icitit
Chinese	Iccnzh
Japanese	Icjpja
Brazilian Portuguese	Icbrpt
Dutch	Icnlnl
Finnish	Icfifi
Danish	Icdkda
Swedish	Icsesv

An example of Subject Line in Multiple Languages to be used with Browser Language option for Request Email

```
icusen:Approval needed for one or more items in the request ($request_id$) for user
($req_for_user_id$)|!icnlnl:Goedkeuring nodig voor één of meer punten in het verzoek
($request_id$) voor de gebruiker ($req_for_user_id$)|!icbrpt:Aprovação necessária
para um ou mais itens no pedido ($request_id$) para o utilizador ($req_for_user_id$)|!
icdkda:Godkendelse nødvendig for et eller flere emner i anmodningen ($request_id$)
for brugeren ($req_for_user_id$)|!icdede:Zulassung für ein oder mehrere Objekte in
der Anfrage ($request_id$) für Benutzer benötigt ($req_for_user_id$)|!iceses:
Aprobación necesaria para uno o más elementos de la solicitud ($request_id$) para los
usuarios ($req_for_user_id$)|!icfifi:Hyväksyntä tarvitaan yksi tai useampia
kohteitapyynnöstä ($request_id$) käyttäjälle ($req_for_user_id$)|!icfrfr:Approbation
nécessaire pour un ou plusieurs éléments de la demande ($request_id$) pour
l'utilisateur ($req_for_user_id$)|!icitit:Approvazione necessaria per uno o più
elementi nella richiesta ($request_id$) per gli utilizzatori ($req_for_user_id$)
```

The same format is applicable for the Message field as well.

Note: You must use the multi-lingual Subject and Message field only if you use the Browser Language as the Email Language. If you are not using the Browser Language option, you are not required to provide the multi-lingual subject and message.

Note: This feature is complementary with Forms that are localized as the Forms included in the Request Email will also appear in the language of choice.

How to flip over all existing Request Email Actions to send Emails in a language other than English after installing the patch

In order to facilitate an easy flip over to send Request Emails in a language other than English with minimal work, an administrative option is added and included in **Administration**, **Configuration**, **Mail Server**. The new property is Default Request Email Language. The default value of this property is English. By changing this option to some other language, all existing Request Email actions will send out mail in the newly chosen language. This also serves as the default language when you add a new 'Request Email' action.

Limitations

This feature is not available when you are using the web service method of **sendRequestEmail**.

Request Pending Action Change

In cases, where there are multiple approvers and when pending approval actions are assigned, the 'Request Pending Action Change' event sends notifications as many number of times as per the number of approvers. In order, to identify the sequence of such event occurrences for email notification, a new parameter is added: Request Pending Action Change.

- **Parameter Name**: *sequence_id*
- **Values**: Starts with 0 and increments by 1 for every subsequent event that is part of the same Request for which a Pending Action Change has occurred.
- **Application**: This parameter could be used to control action execution based on first occurrence of this event. For e.g. A rule condition that is written by using the following condition would fire only once in spite of the number of approvers on a request *sequence_id=0*.

Addition of New objectSOE to Form Designer Standard Objects Set

This object has been added as there was a requirement to access the Service Option ID to which the form has been attached to. The new object is soe which is available exclusive to Form designer object set. This object has three properties:

- soe.item_id: Specifies the Rate item id of the service option name field
- soe.item_text: Specifies the Service option name
- soe.service_option_id: Specifies the service_option_id of this service option

These new properties could be used to build some useful regular expresssions. For example, to show a form field if the Form is attached to a Service option whose name is New Hire Onboarding:

```
Hidden = $(_.soe.item_text!=' New Hire Onboarding')
```

Pagination Feature to Approval List of Policy Designer

Pagination Feature is added to the assignees Lookup table in the CA Service Catalog Policy Designer Page. It works on the filtered set of approvers (User, Group, and Manager).

New Certifications Included with the Patch

For operating systems, hardware, and software supported by CA Service Catalog 14.1.01 patch, see the certification matrix available at https://wiki.ca.com/display/CASM1401/Supportability+Matrix. For more information, search the CA Service Catalog knowledge base available on http://ca.com/support.

Fixes Specific to the CA Service Catalog 14.1.01 Patch

The following contains the list of fixes that are specific to the CA Service Catalog 14.1.01 patch updates:

- The CA Service Catalog UI crashes when there are two users with identical userids, one active and other inactive.
- The **Requested For** field in the cart is set to default (logged in user) every time a new service offering is added to the cart.
- Built-in event for **Request Transfer** fires multiple times and sends multiple emails to requester when there are multiple approvers.
- When a **requested_for** is selected for a user and there are multiple users with the same userid, one active and others inactive, the **requested_for** is updated to the default user during the request save/submission.
- If a Business Unit (BU) contains some Swedish characters in the ID field, the roles are not populated when the user details are edited for this BU.
- A request can be edited even when it is marked as complete.
- CA Service Catalog search fails as there is an SQL exception at the back end.
- A request can be edited even when it is marked as cancelled.
- When you click the Email button for a request, the request created date is not loaded. This is noticed when there are duplicate spadmin entries, one active and others inactive.
- Folders overlap when there is a huge list of folders and sub folders in the request page.
- Request lookup for a request with 10 Forms and 10 service options takes up to 5 minutes to load.
- Request pending action fires an event each for every approver. An email event written to notify old approver results in multiple emails as that of the number of new approvers.
- LDAP Importer goes into an infinite loop when the user uses TDS (Tivoli directory server) with the **Range Retrieval** option turned off.
- Inheritance relationship of service offering breaks when the names are updated.

- In cases, where there are multiple approvers and when pending approval actions are assigned, the **Request Pending Action Change** event fires as many number of times as the number of approvers. There is a need to identify the sequence of such event occurrences for email notification purposes. In order to facilitate this need, a new parameter has been added to events - **Request Pending Action Change**.

- Clicking the CMDB/SDM test button fails on Internet Explorer (IE) 10. No such issues are noticed with other web browsers.

- Request Email sent from CA Service Catalog contains content in English (for example, General Information, Requested Services, Form Content, and so on.)

- A new object called SOE is made available in the forms designer for expression **evaluation. soe**. It contains the following properties:

  - item_id = rate item id of 'service option' name field soe.

  - item_text = Service option name soe.

  - service_option_id = service_option_id of this service option.

- Copying a service option in the SOG definition throws an error if the form rate item definition uses regular expression to control visibility of the form, and if the expression contains the Exclamation (**!)** mark in it.
  For example: *$(_.service.code != 'noservice')*

- The Email Approval Error Notification Process fails in kicking the Error Notification Process. The Error Notification Process fails triggering the POSTAlert web service method.

- Approve and Reject links in Request Email that are generated from OOTB does not work in SSO as the user is prompted to login again.

- After removing an image from a service offering, white space is seen.

- Setting the **Disable** attribute of a form by providing a JavaScript expression at a Service option level to add a form to it. In widgets, the form can be edited even if the JavaScript validation is valid. However, in the CA Service Catalog UI, it cannot be edited.

- After selecting the Perform Action for a request in which the logged in user is not assigned the pending action, the whole form becomes read only (grayed out) even if the override action is selected.

- On Internet Explorer (IE) 8, clicking the **Ok** button does not save a report to a specific folder in the Set Folder of the Report Builder.

- The **Create Inherited Copy** button does not copy Option in the same language

- There is no synchronization between widgets. Status widget does not update the open requests and cart numbers correctly on other widgets.

- Pagination feature to the approval list (of users and groups) in the policy designer page is introduced.

- For service options associated to an offering that is defined as **One-Click Submit** when the correspondent FORM is loaded, it does not hold the value of ca_fd.formId (returning undefined value). As a result, it is not able to execute the onLoad script of the form which depends on **ca_fd.formId** value in order to pre-populate form values.

  Two new parameters are added to this function:

  ```
  ca_fdFetchSelectData(FormID,DualListID,Validate,KeepExisting)
  ```

  - **Validate**
    The Validate parameter is a boolean value to validate the ToList of dualList on fetching new data into the component.

  - **KeepExisting**
    The KeepExisting parameter is a boolean value to retain the values of ToList on fetching new data into the component.
    For example: ca_fdFetchSelectData('form1','dlist','false','true');
    For details, refer to Test fix: T52W073

    Note: These two parameter values are optional. If the user is not using these values, the component works as per design.

- An image may be shown as the Service option name. Due to this, the HTML tags are displayed in the Service Option name in widgets.

  Note: For more information, refer to Test fix: T52W084

- If any regular expression is given in the pattern attribute of the field, the field is treated as a mandatory field even when it is not mandatory.

- Cross-Site scripting (XSS) vulnerability is noticed with the resetpassword UI node.

- The table data is not populating in the read-only mode when the table mode is set to data instead of selection.

- Policy conditions with external_id (for example, *$(anySoWith('external_id', eq,'111'))*) are not satisfied. This results in the corresponding policy notable to assign the respective action as desired.

- The request is approved after the first or second Overdue notification email is sent. This is noticed even when the status is successfully moved to Pending Fulfillment, and the final Overdue notification as well as the **Not Submitted – Rejected** email is sent.

- When iterating multiple items within the cart, CA Service Catalog makes the same number of calls to the EEM API method. Results are not cached, and unnecessary calls to the EEM API are made which may impact the performance.

- The **getUser** web service method does not return the group details of the user.

- When the logIn() web service is called simultaneously by multiple threads, similar message may randomly get logged in the view.log caused by:

  ```
  com.microsoft.sqlserver.jdbc.SQLServerException: Violation of PRIMARY KEY
  constraint 'XPKusm_webservice_sessions'. Cannot insert duplicate key in object
  'dbo.usm_webservice_sessions'. and the logIn method will not complete successfully.
  ```

- If the Local EEM Group with multi-domain users is made the Approver, the members do not receive email notifications.
- The Domain column of usm_request table is not updated correctly.
- Generating invoice breaks the existing requests by creating several new columns in the request details page.
- If a form contains a field that holds data of size more than 65536 bytes, the Policy based pending action assignment breaks.
- If the Service Options are selected in a quick succession, forms of few service options are not loaded.
- Opening the Service Desk Ticket link from CA Service Catalog may take time to load and open.
- Permissions assigned to a folder or service offering based on multi-domain LDAP group is not honored.
- The change order details page prompts for Authentication.
- Archived Process Status shows up as unknown in Catalog Request Tracking Tab.
- When a Service Offering is exported using the XUTIL, the resultant XML file may not contain few rate items.
- If you select a row on the first page when the **Maximum rows** attributes of a table is set to 1, selecting a row on the second page throws an error instead of deselecting first selection.
- Dual list options that have long labels are truncated and appended with **'...'**. As of now, we do not expose a horizontal scroll bar or allow for mouse over of the options to display the full label as the mouse over is controlled by the **Tool Tip** attribute of the dual list.
- When a select field has multiple options with the same value, the request will always show the first option with the selected value after added to the cart.
- Report data object throws a browser error when you try to edit it.
- In a cart page, additional offerings are shown if the description contains span elements with id value.
- List drop-down details are editable
- The **Submit** button may stop working and show a hang status in the Unified Self-Service Interface. For more information, see *Test fix: T5ES150* posted on http://ca.com/support.

CA IT Asset Manager Enhancements

Search List Items

If you have a larger number if items in your list, you need not navigate across all items to find the item you want. As a CA APM user, you now have the ability to filter your list items. The search criteria depends on the properties of the list.

For more information, see Manage List Items (see page).

Export List Item Search Results

As an Administrator, for a user-defined search, you can now view the user who created the search and when the search was last performed. This information helps you delete user-defined searches if they are not in use for long time.

List Management Access

As an Administrator, you can now define who accesses List Management. You can also determine the list items that different roles can access.

Import List Items

In List Management, you can now export the list of items that you searched for to a CSV file.

Change Cost Details of Specific Assets Using the Lookup

In the Add Asset Cost utility, you can now change cost details of specific assets using the lookup.

CA APM and CA SAM Data Synchronization Changes

CA SAM Import Driver in CA APM 14.1.01 is aligned with the latest change in CA SAM database schema related to operating system values for devices in CA SAM versions 3.6.5 and later.

If CA APM is integrated with CA SAM in your solution deployment, consider the following:

- To install/upgrade to CA SAM 3.6.5 or later, you must install/upgrade to CA APM 14.1.01 or later to be fully compatible with CA SAM.
- For older versions of CA APM (14.1 or older), you must not upgrade CA SAM to version 3.6.5 or later.

CA Service Management Release 14.1.01 Patch Information

The CA Service Management 14.1 cumulative patch #1 (14.1.01) includes a number of defect fixes for the Service Desk component, available for your download (http://www.ca.com/us/support/ca-support-online/product-content/recommended-reading/technical-document-index/ca-service-management-solutions-patches.aspx). For a smooth transition to our published patches, review the Cumulative Incidents (http://www.ca.com//us/support/ca-support-online/product-content/recommended-reading/product-related-technical-information/reported-incidents-with-first-cumulative-patches-of-ca-service-desk-r14_1.aspx).

The following table lists the individual defect fixes resolved in the cumulative patch. For more information on a particular problem, search the knowledge base on support.ca.com (http://support.ca.com) or click on the hyperlinks below.

S. No	Problem #	Summary
1	USRD 801 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=801)	LOCALIZATION CHARACTERS GARBLED IN CONSOLE DISPLAY
2	USRD 1897 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=1897)	EXPORT BUTTON EXPORTS WRONG DATA
3	USRD 1927 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=1927)	TRANSLATION FILE IN GRLOADER CONFIG FILE IS IGNORED
4	USRD 1939 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=1939)	AUTOFILLING OF TICKET SHOW FIELD COMPLETION IN PROGRESS
5	USRD 2113 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2113)	KT_DAEMON MAY TERMINATE WITH STRING TOO BIG ERROR
6	USRD 2133 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2133)	SUPPORT AUTOMATION LOGS ARE EMPTY DUE TO WHISPER LOGS
7	USRD 2765 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2765)	IE9 CRASHES ON OPENING MULTIPLE BROWSERS
8	USRD 2832 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2832)	BOGUS STRING ERROR WHILE PUBLISHING THROUGH WSP
9	USRD 2909 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2909)	PDM_LOAD TERMINATES DURING LOAD WITH MANY TABLE REFERENCES
10	USRD 2915 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2915)	UNABLE TO ACCESS HELP BOOKSHELF AFTER RESTART
11	USRD 2918 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2918)	IMAGE URL GETS ADDED WHEN TOGGLING BETWEEN SOURCE AND DESIGN
12	USRD 2928 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2928)	DEFAULT CHANGE TYPE NOT ASSOCIATED ON CATEGORY CHANGE
13	USRD 2938 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2938)	PRINTING FORM OUTPUTS GARBAGE DATA IN INTERNET EXPLORER
14	USRD 2942 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2942)	PDM_MAILEATER_NXD MAY TAKE A LONG TIME TO PROCESS EMAILS
15	USRD 2943 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2943)	EXISTING TICKET STATUS COPIED OVER TO NEW TICKET
16	USRD 2947 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2947)	CHANGE ORDER COPY FAILS WITH ILIMIT ERROR
17	USRD 2956 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2956)	INTERNAL CHECK BOX IGNORED IN CERTAIN CASES
18	USRD 2957 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2957)	UNNECESSARY VERTICAL SCROLLBAR SHOWS UP ON MAIN SCOREBOARD
19		

S. No	Problem #	Summary
	USRD 2967 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2967)	UNABLE TO ACCEPT DOCUMENT AS SOLUTION
20	USRD 2968 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2968)	DOCUMENT TREE CANNOT BE OPENED VIA LINK IN ANOTHER DOCUMENT
21	USRD 2970 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2970)	PDM_LDAP_SYNC AND PDM_LDAP_IMPORT MAY FAIL
22	USRD 2971 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2971)	SORT FAILS IN DETAIL PAGE FOR ASCENTED CHARACTERS IN ORACLE
23	USRD 2977 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2977)	PDM_LOAD FAILS FOR LARGE DATA
24	USRD 2981 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2981)	WEB DIRECTOR MAY BECOME UNRESPONSIVE
25	USRD 2985 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2985)	MENUBAR MAY BE MISSING ITEMS ON CHANGE ORDER FORMS
26	USRD 2991 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2991)	EXPORTING MORE THAN 5000 CONFIGURATION ITEMS FAILS
27	USRD 2992 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2992)	KD EMAIL NOTIFICATION SENT WITH HIGH URGENCY LEVEL
28	USRD 2993 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2993)	SCREENREADER READS CA LOGO 'CA' INSTEAD OF 'CA TECHNOLOGIES'
29	USRD 2995 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2995)	KNOWLEDGE SEARCH FILTER MAY NOT PICK UP CONTACT FIELDS
30	USRD 2996 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2996)	UNABLE TO ACCEPT DOCUMENT AS SOLUTION FOR ISSUES
31	USRD 2997 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2997)	WORKFLOW TASK STATUS MAY EXECUTE INACTIVE MACRO
32	USRD 2999 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=2999)	CHANGES TO REDIRECTINGURL MAY BE LOST ON CONFIGURE
33	USRD 3001 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3001)	CMDB VISUALIZER SHOWS INCORRECT GRAPH
34	USRD 3003 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3003)	ISSUE SUMMARY REPORT DISPLAYS DESCRIPTION INSTEAD OF SUMMARY
35	USRD 3004 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3004)	AHD03116 TENANCY VIOLATION INVOLVING ORGANIZATIONS
36	USRD 3011 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3011)	ANIMATOR PROCESS MAY EXECUTE INACTIVE MACROS
37	USRD 3019 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3019)	AUTO CLOSE ACTIVITY LOGGED USING WRONG CONTACT
38	USRD 3023 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3023)	RESTRICTED ACCESS TO LEVEL 1 ANALYST TO EDIT A GROUP
39		

S. No	Problem #	Summary
	USRD 3024 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3024)	HEALTHSERVLET MAKES TOMCAT FILE SIZE HUGE
40	USRD 3025 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3025)	UPLOAD ATTACHMENT MAY FAIL THROUGH WEBSERVICES
41	USRD 3027 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3027)	EEM CREDENTIALS EXPIRE WHEN DST IS SHIFTED
42	USRD 3029 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3029)	SQL ERROR MAY OCCUR WHEN OPENING KNOWLEDGE DOCUMENT
43	USRD 3032 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3032)	EXISTING LINKED DOCUMENTS NOT ALLOWED TO BE THE SOLUTION
44	USRD 3033 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3033)	ATTACHMENTS FAIL IN EVENT OF MOMENTARILY NETWORK LOSS
45	USRD 3038 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3038)	INTERNET EXPLORER 8 MAY GROW IN MEMORY USAGE
46	USRD 3041 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3041)	DEPLOY SOAP WEB SERVICES CHECK BOX SHOWN WRONG
47	USRD 3042 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3042)	NOTIFICATION CONTACT NOT ADDED IN KNOWLEDGE DOCUMENT
48	USRD 3044 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3044)	WEB SERVICES CALLS MIGHT HANG
49	USRD 3050 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3050)	JAPANESE TEXT IS GARBLED IN WEB.CFG FILE
50	USRD 3051 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3051)	LOG COMMENT' PAGE MIGHT BE HANGING
51	USRD 3053 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3053)	CATEGORY PROPERTIES MAY NOT BE POPULATED WHEN TABBING OUT
52	USRD 3055 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3055)	ALLOW STRICT SURVEYS TO BE SENT TO MULTIPLE TICKETS
53	USRD 3057 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3057)	BROWSER MIGHT BECOME UNRESPONSIVE WHILE CREATING A TICKET
54	USRD 3059 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3059)	SLUMP PROCESS DOES NOT TERMINATE WHEN SERVER DISCONNECTS
55	USRD 3060 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3060)	UNABLE TO EDIT LOG COMMENT WHEN USING ORACLE
56	USRD 3061 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3061)	QUICK PROFILE MAY NOT DISPLAY CONFIGURATION ITEM
57	USRD 3064 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3064)	IMAGES ARE SHOWING AS RED X IN KNOWLEDGE TREE DOCUMENTS.
58	USRD 3065 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3065)	DUPLICATE VALUES IN KNOWLEDGE EXPORT /IMPORT TEMPLATE
59		

S. No	Problem #	Summary
	USRD 3066 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3066)	INVALID CATEGORY DOES NOT SHOW ANY ALERT MESSAGE
60	USRD 3070 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3070)	ALL CLASSIC WORKFLOW TASKS ARE VIOLATED
61	USRD 3071 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3071)	UPDATEOBJECT METHOD ALLOWS PERSISTENT ID MODIFICATION
62	USRD 3072 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3072)	LOADING CONFIG ITEM FROM TWA UPDATES LAST UPDATE DATE FIELD
63	USRD 3080 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3080)	SPEL_SRVR PROCESS MIGHT NOT RESPOND TO TRIGGERS
64	USRD 3081 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3081)	EACH TOMCAT INSTANCE LEAVES A ZOMBIE PROCESS IN UNIX SYSTEMS
65	USRD 3086 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3086)	SUPPORT FOR DETECTING CIRCLES IN HIERARCHICAL QUERIES
66	USRD 3091 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3091)	TENANT NOT UPDATED FROM LOOKUP FIELDS
67	USRD 3077 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3077)	WIN-UPDATING CI RESULTS IN CARTESIAN PRODUCT ERROR
68	USRD 3089 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3089)	WIN-ERROR MESSAGE IN PAM WORKFLOW PAGE IN MAC OS
69	USRD 3097 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3097)	WIN-UPLOAD ATTACHMENTS FAILS VIA IIS
70	USRD 3094 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3094)	ATTACHING FILES TO THE REPLY OF A KT FORUM DOES NOT WORK
71	USRD 3100 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3100)	CONTACT FROM LDAP DOES NOT WORK WITH WEB WILDCARD SEARCH
72	USRD 3133 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3133)	WIN-SEARCH KNOWLEDGE DOCUMENT PAGE MAY FAIL
73	USRD 3159 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3159)	Wasted ldap_agent
74	USRD 3160 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3160)	WIN-EVENTS NOT GETTING TRIGGERED
75	USRD 3174 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3174)	WIN-ERRORS IN PDM_CONFIGURE WITH DATABASE NAME OTH
76	USRD 3186 (https://support.ca.com/irj/portal/kbproblem?productcd=USRD&problemnbr=3186)	SDM FAILS TO START AFTER ENABLING FIXED SOCKET OPTION

See the procedure (http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec1250834.aspx)to secure CA Service Desk Manager from SSL 3.0 POODLE Vulnerability.

CA Service Management Release 14.1 Enhancements

CA Service Management Release 14.1 Enhancements

The following enhancements provide the solution experience for the CA Service Management users. These features help reduce the time spent on installing, configuring, and administering the solution.

Simplified Install or Upgrade Experience

Single Installer to Install All or Any Combination of the Products in the Solution

You can now install all or any combination of the products in the solution using a single installer, instead of using individual installers for each product. Once you select the products that you want to install, the installer performs the prerequisite check for the selected products and lets you know the status of each prerequisite. It also prompts to install the common components that are required for the products. Common components are CA EEM, CA Process Automation, CA Business Intelligence, and the MDB.

The CA Service Management installer replaces the individual product installers. Therefore, the product-specific installers are no longer available for the products in the solution**.** The common component installers are launched directly from the CA Service Management installer except for CA Process Automation.

With this release, the name of the database (the MDB) is no longer hard-coded to “MDB”. You can now specify another unique name for the MDB, which is used by the entire solution.

Automatic Integration of Products in the Solution

If you have installed more than one product in the solution, the products are automatically integrated to a great extent right after the installation. It requires very few or no manual steps for the integration to work. In addition to the products, the common components are also automatically integrated and requires fewer manual steps after the installation. If one of the products is integrated with a common component, all the other products in the solution are also integrated with that component. This functionality helps you get started with solution faster and minimizes the manual effort and human error that is otherwise caused by manual configuration.

Automatic Upgrade for Products in the Solution

The installer detects any earlier versions of the product that you are trying to install and prompts whether you want to upgrade the same. After you confirm, it automatically upgrades the products to Release 14.1.

Shared Common Components for Products in the Solution

You can now share the common components such as, CA EEM, CA Business Intelligence, CA Process Automation, and MDB across the products in the solution. In addition to sharing a common installation, a common configuration is also now shared across these components. You no longer need to have separate instances of these common components for different products or configure the components for individual products.

Support for CA Business Intelligent 4.1 SP3

With this release, CA Service Management supports only CA Business Intelligence 4.1 SP3. If you have any other earlier version of CA Business Intelligence, you must install 4.1 SP3 and migrate the data from your earlier version for the reports in CA Service Management to work.

Important! If you want to retain any one of the CA Service Management products at an older release level, you must have two instances of CA Business Intelligence. One CA Business Intelligence instance for the older release and one CA Business Intelligence 4.1 instance for 14.1. You can then access the reports for respective releases of CA Service Management products.

Consolidated Documentation Available on a Wiki Platform

You can now access the entire CA Service Management documentation through a dynamic and collaborative Wiki platform. This Wiki space includes documentation for all the products in the solution under one umbrella. You can like, dislike, comment, and share the Wiki pages with your peers. The previous form of delivery through bookshelf has been discontinued with this release and Wiki becomes the primary mode of delivery.

Wiki Links from the Products

You can also access the Wiki from the user interface of the products. Apart from this, some of the context-sensitive links also now redirect to the Wiki. In some cases, the links take you to the CA Service Management Home Page and you can search to find the relevant content using the improved search functionality.

Integrated Administration

Single Interface to Configure and Administer Certain Aspects of the Products in the Solution

You can now manage your tenants, users, roles, and configurations for all the CA Service Management products from a single, common administration interface, as opposed to managing them individually in different products. For example, you can now add or update tenants in the common administration interface and use them in CA Service Desk Manager, CA Service Catalog, and CA IT Asset Manager.

Note: The common administration interface is exposed as a request in CA Service Catalog. So, the interface is available only when you install CA Service Catalog as part of the CA Service Management solution.

Business Value Dashboards

Business Value Dashboards provide decision makers such as, team leads, executives, and managers have additional information into life cycle of the tickets. The reports help the users analyze the following critical information:

- Cost and productivity within the organization
- Cost of service disruptions
- Service demand metrics
- Operation effectiveness of the support groups

For more information, see Business Value Dashboards (see page 783).

CA Service Management Mobile Application Enhancements

As a CA Service Management User, you can now access the CA Service Management Mobile Application. This mobile application is a common interface to access some of the core features of CA Service Desk Manager and CA Service Catalog from your mobile device. The following mobile capabilities are available in CA Service Management Mobile Application:

- Service Desk
- My Tasks
- Unified Self-Service
- Create Ticket
- Catalog

As a CA Service Management Administrator, configure the CA Service Management Mobile Application to ensure that the employees in your organization can access it. For more information, see the Mobility (see page 3156) section.

CA Service Desk Manager Enhancements

The following enhancements are available for CA SDM:

Notification Failures Logged in Ticket Activity Logs

Email notification failure is now logged in the activity log to indicate if any of the notifications were not sent to the users.

Manual Notify Check to Verify Email Address

If you try to send a manual notification to a contact that does not have an associated email address, a message is displayed.

Enhanced Security Options

To prevent a potential Session ID (SID) spoofing attack on CA SDM, you can optionally encrypt the Session ID. You enable this option in CA SDM Options Manager, Security Options. It prevents spoofing attacks by using encrypted cookies along with an encrypted SID. For enhanced security, we recommend that you use an SSL Connection with the encrypted SID option.

Multiple Files Upload Feature

You can now select multiple files simultaneously to upload for tickets, repositories, and knowledge. Maximum files that can be simultaneously uploaded is 10. This limit can configured using max_files_to_upload_simultaneously option from Service Desk Administration. For more information, see the Web Options (see page 1303).

Note: The multiple file selection functionality is not applicable for KT insert images

Cut/Copy/Paste in Context Menu

You can now right-click on a CA SDM web page and select the cut, copy, and paste options.

Note: This feature works on Internet Explorer only. On Chrome and Firefox, you are prompted to use the keyboard shortcuts such as Ctrl+x (cut), Ctrl+c (copy), Ctrl+v (paste).

xMatters and CA SDM Integration

xMatters is used for mass notifications and alerts. When a CA SDM ticket (incident, request, or problem) is created or updated, the integration mechanism sends the notification along with ticket information to the xMatters agent. The notification works only with CA SDM CR objects (incident, request, or problem). The CA SDM notification feature sends notifications to users based on the rules set for notification. CA SDM now automatically sends the Notify Log Reader information along with ticket information to the configured xMatters agent.

CA SDM administrators can enable or disable the integration with xMatters through the Options Manager xMatters options. You must install these options as these options are not installed out of the box. Restart CA SDM services after installing or uninstalling these options. On successful installation of xMatters options, a new daemon the pdm_xmatters_sync is started and can be monitored through the task manager process list. This daemon is a singleton process and runs on the primary or background server.

For more information, see Options Manager-xMatters (see page).

CA SDM and CA Process Automation integration – Retry Mechanism for Failed Events

CA Process Automation Workflows can be attached to CA SDM tickets (for example,Change Orders) through CA SDM Events and Macros. The attached events are triggered by CA SDM at the specified retry interval duration. During retry, if the CA Process Automation is unavailable, the attached event is marked as **Unknown**. CA SDM retry mechanism for failed events automatically re-triggers the attached **Unknown** events when CA Process Automation is available.

CA SDM administrators can enable the retry mechanism for failed events by installing additional options in the CA Process Automation Workflow Options Manager. For more information, see Options Manager, CA Process Automation Workflow Options (see page 1303).

- **caextwf_retry_count**: Default value is 3 and can be set in the range [1 – 20].
- **caextwf_retry_interval**: Default minimum value is set as 10 minutes in the range [10-999].

This feature can be disabled by uninstalling these options. Restart CA SDM services after installing or uninstalling these options. For more information, see CA SDM Retry Mechanism for Failed Events (see page 1250).

CA Service Catalog Enhancements

Usability Enhancements in Form Designer

As a CA Service Catalog administrator, you can now:

- Drag and drop the form elements while creating a form
- Use the Page Layout element, a new form element in this release, to create a form

> **Note:** The _id value for each form element is auto generated.

Related Documentation:

For more information about the page layout and _id value, see Elements of a Form (see page 2916).

Organizing Service Options

As a CA Service Catalog Administrator, use the **Organize Options** button in the Definition tab of the Option Groups for a service offering to arrange the service options.

Support for IN clause in Data Object queries

The IN clause in a Data Object query now supports multiple parameters. You can now choose from a list of values to create a variable.

Mobile Support for Select Plug-in

You can now use the Select Plug-in for mobile users.

LDAP Properties File Modified

You can now import users into the CA Service Catalog application using the LDAPImporter utility which comes with that application only. That is, you can import users into the CA Service Catalog application1 using the LDAPImporter utility which comes with this application only. You cannot import users into CA Service Catalog application2 using the LDAP importer utility of CA Service Catalog application1.

The following properties have been removed from the default ldapimporter_server1.properties file:

- Catalog.Hostname
- Catalog.Port
- Catalog.Context
- Catalog.SSL

Content Pack Enhancements

The following content pack enhancements are available in this release:

My Resources

The business user can perform the following tasks using this offering:

- View all the devices, software, and applications that has been assigned to the user in a single page called My Resources.
- Report an issue on a hardware or software asset from the My Resources page.
- View Warranty expiration dates from the My Resources page.

Reset Password

The business user can perform the following tasks using this offering:

- Reset application password on their own without having to raise an issue.
- Reset domain password of the user.

As a CA Service Catalog administrator, you can update and delete the table entries of the Catalog Content Configuration form of My Resources and Reset Password offerings.

Related Documentation:

The instructions for configuring and using the content packs are explained in a series of videos. To access the playlist, click here (https://www.youtube.com/playlist?list=PLynEdQRJawmxzRAWRffwpXetTc3wtIq4J).

Widgets Enhancements

Unified Self-Service is now available with the CA Service Catalog widgets out-of-the-box. You can also embed the CA Service Catalog widgets in a portal such as Liferay or Microsoft SharePoint.

As a CA Service Catalog user, you can now:

- See a "Featured" folder in the Browse widget. This folder has the featured service offerings that your CA Service Catalog Administrator has configured.
- Use the auto suggest feature when you are browsing the available offerings.

- Add comments or attachments and then view them as a conversation.

  Note: You can also edit or delete the attachments.

- See the status of your request in the Request List widget.

Related Documentation:

For more information about configuring the widgets, see Use Widgets for Request Management (see page 2176).

Change the Business Unit on the fly

As a CA Service Catalog user, you can now change the business unit without having to log out of your CA Service Catalog instance. The business unit that you see depends on your role and access rights.

Change the Locale on the fly

As a CA Service Catalog user, you can change the locale of your CA Service Catalog instance without having to log out of your CA Service Catalog instance. Specify the locale to access the localized Catalog instance as follows:

`http://hostname:port/usm/ (http://hostnameport)&locale=<locale>-<country>`

For example, to see the French UI

`http://hostname:port/usm/&locale=FR-FR (http://hostnameport)`

CA IT Asset Manager Enhancements

Add Costs to Multiple Assets

You can add a cost record to multiple assets at a time. For example, you procured 20 new laptops and want to enter cost records for these laptops.

You can choose to update an individual asset cost record or make changes to all the records at the same time. For example, all the laptops that you procured have the same Unit Amount. You enter the Unit Amount and apply the value to all the asset cost records.

For more information, see Add Costs to Multiple Assets (see page 2373).

Create Copies of Assets

You can now create multiple copies of assets from existing assets. Prior to this release, you could create only one asset copy at a time. For example, you procured 100 new laptops with the same model and same cost. To save time, you create a new asset with model name and cost and then create 99 copies of the same asset. At a later point of time you can specify other details of the assets.

For more information, see Manage Assets (see page 2357).

CA Asset Portfolio Management (CA APM) integration with CA Software Asset Manager (CA SAM) is enhanced and supports Multi-tenancy

If you implemented multi-tenancy, you now have the ability to assign a tenant to instances of SAM. Prior to this release, CA SAM did not support integration with a tenanted Service Management (i.e. CA Service Desk Manager, CA IT Asset Manager, and CA Service Catalog) environment. For more information, see How to Implement Multi-tenancy with CA SAM (see page 390).

Also, integrating CA APM and CA SAM is much simpler with configuring CA SAM Import and Export Service no longer required. For more information, see How to Implement CA SAM with CA APM (see page 382).

Payment Schedules and Recalculation

The Payment Schedule is a list of the payments due, based on the cost information you provide on a cost record. CA Asset Portfolio Management automatically generates the payment schedule in the form of a table when you define and save a cost record. Prior to this release, payments schedules were not created/updated automatically. The schedule generated depends on whether the cost is a one-time cost or a recurring cost.

For more information, see Payment Schedules and Recalculation (see page 2375).

Add Assets from Unreconciled Discovered Records

You can configure CA APM to automatically add new/un-reconciled discovered assets to your ownership repository. Prior to this release, the user was required to run a report and run an import to create newly discovered assets. This enhancement automates the process based upon the rules the user defines.

For more information, see Add Asssets from Unreconciled Discovered Records (see page 2425).

Contact Details in CA APM are Added to CA SDM Contact Quick Profile

After CA APM and CA SDM are integrated, the contacts list in CA APM is added to the CA SDM contact quick profile window. When you create asset records, the contact details are automatically reflected in CA SDM contact quick profile window. For more information, see Verify Single Sign-On (see page 3254).

Enable Single-Sign On Login for CA IT Asset Manager and CA SDM Integration

CA Service Management provides the following mechanisms to enable SSO from CA IT Asset Manager to CA Service Desk Manager.

- Web Service Access Policy File
- CA Service Desk Manager Administrator Credentials

Both the mechanisms internally use the CA Service Desk Manager SOAP Web Services to achieve the SSO from CA IT Asset Manager to CA SDM. You can configure either one or both the mechanisms to achieve SSO from CA IT Asset Manager to CA SDM.

Note: Ensure that CA IT Asset Manager and CA Service Desk Manager are installed on the same MDB.

For more information, see Enable Single Sign-On (SSO) from CA APM to CA Service Desk Manager (see page 3251) and Verify Single Sign-On (see page 3254). (https://wiki.ca.com/display/CASM/Verify+Single+Sign-On)

Unified Self-Service Enhancements

Unified Self-Service (formerly known as CA Open Space) has a new and improved user interface. There are two self-service interfaces available; one for business users and the other for administrators. You can install Unified Self-Service as part of CA SDM or CA Service Catalog products.

CA Service Desk Manager Connector Enhancements

CA Service Desk Manager Connector Enhancements

- CA Catalyst Container r3.4.1 is supported by CA SDM connector.
- CA SDM connector supports all CA SDM localized languages.
- Following new CMDB classes and families are introduced:

Family Name	Class Name
Software.WebSite	WebSite
Hardware.StorageVolume	StorageVolume
Hardware.VMDataStore	NetworkFileSystem, LocalStore, LocalStore-VMwareFileSystem
Hardware.StoragePool	StoragePool
Software.HyperVHypervisor	HyperVHypervisor
Software.ESXHypervisor	ESXHypervisor
Software.VirtualManager	VirtualManager
Enterprise.TransactionContext	TransactionContext
Hardware.EnvironmentalSensor	Intrusion, Vibration, Humidity, AirFlow, Pressure, Temperature, GasDetection, Unknown

Family Name	Class Name
Hardware.File	Volume, Directory, File, File-Exe, File-Data, File-Log, File-Cabinet, VirtualImage, VirtualImage-CDDVD, VirtualImage-Floppy
Hardware. Memory	Physical, Physical-Processor, Physical-IO, Physical-PCI, Physical-Fast, Physical-Multibus, Physical-Video, Paging, Cache
Software. NetworkServer	NetworkServer
Hardware. Processor	680x0, 80x87, x86, x86-32, x86-64, x86-64-IA64, x86-64-AMD64, s390x, MIPS, MIPS-BigEndian, MIPS-LittleEndian, Alpha, PA-RISC, PowerPC, SPARC, ARM
Hardware. DiskPartition	BFS, Xenix, Linux.EFI, FAT, FAT12, FAT16, FAT32, FAT64, IBM-Extended, AIX, HFS, HPFS, JFS, NTFS, NTFS1-3, NTFS4, NTFS5, TransactionalNTFS, OPUS, VMware, Unformatted
Software. ResourceServer	ResourceServer, SecurityServer, TransactionServer, MessageServer
Software.COTS	BackgroundProcess

For more information about the attribute mapping of these new classes, see under Type Mapping (see page 4737).

Supported Operating Environments and Languages

Supported Operating Environments

Supported operating environments include the platforms, databases, browsers, integrations, and mobile platforms that are supported by CA Service Management. For the complete list of supported operating environments, see the Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix).

Languages Supported

Documentation Wiki is available in the following languages:

- French
- Italian
- German
- Spanish
- Japanese
- Simplified Chinese

- Brazilian Portuguese

For the list of languages supported by the products in the solution, see the Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix).

Note: Some of the products in the solution support additional languages such as Canadian French, Traditional Chinese, Danish, and so on, which are not supported by the Wiki. Refer to the English wiki for such languages.

Supportability Matrix

The CA Service Management Supportability Matrix is a unique reference to the solution level compatibility of service management capabilities, which includes the following products:

- CA Service Catalog
- CA IT Asset Manager (CA Asset Portfolio Management and CA Software Asset Manager)
- Unified Self-Service
- Mobility

CA Service Management supports the followin g common components:

- CA EEM
- CA Process Automation
- CA Business Intelligence

Note: CA Software Asset Manager version is not specified in the supportability matrix as the information below is generic to every version of the CA SAM that is supported. The certified version of CA Software Asset Manager with CA Service Management 14.1 is 3.6.3 and we continue to support the versions above 3.6.3 .

Tip! CA Software Asset Manager version 4.0.1 is not compatible with CA Service Management MDB running on Oracle database. We recommend that you use CA SAM 3.6.7 until this incompatibility is resolved.

The CA Service Management supportability matrix encompasses the information that is related to the following:

Operating Systems Support

Consider the following points**:**

- CA Service Management will support all service packs and point releases of the following mentioned operating systems. The certified editions of above Microsoft Windows Server platforms are Standard, Enterprise, and Data Center Editions.
- If the customer configuration involves a need for Linux/UNIX server platforms, CA recommends installing the database of service management products on Linux/Unix platforms and access the web client interfaces on Windows platforms. This is applicable for all the Service Management products and can be supported by CA.
- Please refer the instructions in Operating Systems for additional details on deployment of **CA Service Desk Manager** on Linux platforms.

LEGEND : **V** - Certified (Tested and Verified); **O** - Supported (Not Tested, expected to work) ; **x** - Not Supported

Microsoft Windows Server Operating Systems	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1	CA EEM 12.51 CR02	CA Process Automation 4.3	CA Business Intelligence 4.1 SP3
Microsoft Windows Server 2012 R2 (64-bit only)	V	V	V	V	V	V	V	V
Microsoft Windows Server 2012 (64-bit only)	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V

Microsoft Windows Server Operating Systems	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1	CA EEM 12.51 CR02	CA Process Automation 4.3	CA Business Intelligence 4.1 SP3
Microsoft Windows Server 2008 (64-bit only)								
Microsoft Windows Server 2008 R2 (64-bit only)	V	V	V	V	V	V	V	V

Linux Server Operating Systems	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1	CA EEM 12.5 CR02	CA Process Automation 4.3	CA Business Intelligence 4.1 SP3
Red Hat Enterprise Linux 6 (x86; 64-bit only)	V	x	x	x	V	x	O	x
Red Hat Enterprise Linux 5.5 (x86; 64-bit only)	V	x	x	x	V	x	O	x
SUSE Linux Enterprise Server 11 SP1 (x86; 64-bit only)	V	x	x	x	V	x	x	x

UNIX Server Operating Systems	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1	CA EEM 12.5 CR02	CA Process Automation 4.3	CA Business Intelligence 4.1 SP3
Oracle Solaris 11 (SPARC; 64-bit only)	V	x	x	x	x	V	O	x
Oracle Solaris 10 (SPARC; 64-bit only)	V	x	x	x	x	V	O	x
IBM AIX 7.1 (Power; 64-bit only)	V	x	x	x	x	x	O	x

UNIX Server Operating Systems	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1	CA EEM 12.5 CR02	CA Process Automation 4.3	CA Business Intelligence 4.1 SP3
IBM AIX 6.1 (Power; 64-bit only)	V	x	x	x	x	x	O	x

Database Support

All databases are certified for both 32-bit and 64-bit, unless specifically noted, and service packs of all the above databases are supported. For information about a remote Oracle 11g R2 MDB database installation on HP-UX 11i (PA-RISC) for CA Service Desk Manager, download the package from the CA SDM Product Download page on http://support.ca.com/. Refer the instructions in the Implementing section on how to deploy CA Service Management in Oracle RAC environment successfully. To know more about CA Process Automation components like Orchestrator, agent, web based UI, see the CA Process Automation compatibility matrix at http://support.ca.com (http://support.ca.com/).

LEGEND : V - Certified (Tested and Verified); **O** - Supported (Not Tested, expected to work) ; **x** - Not Supported

Database	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1	CA Process Automation 4.3	CA Business Intelligence 4.1 SP3
Microsoft SQL Server 2014	V	V	V	x	V	V	V
Microsoft SQL Server 2012	V	V	V	V	V	V	O
Microsoft SQL Server 2008	V	V	V	V	V	V	O
Microsoft SQL Server 2008 R2	V	V	V	V	V	V	O
Oracle 12c	V	V	V	x	V	O	O
Oracle 11g R2	V	V	V	V	V	V	O
Oracle 11g R2 RAC	V	V	V	x	V	V	O
MY SQL 5.5	x	x	x	O	x	x	O

Web Browser Support

Consider the following points:

- Web chat is the only feature of Support Automation that is available on Apple MAC OS 10.8.4 for desktops/laptops.
- Support Automation feature for analyst are not supported on Microsoft Edge.
- For more information about ESR releases, see https://www.mozilla.org/en-US/firefox/organizations/faq/. (https://www.mozilla.org/en-US/firefox/organizations/faq/)
- The certified versions of the browsers include Microsoft Internet Explorer 11, Microsoft Edge on Windows 10, Firefox ESR 24.0, Firefox 31.0, Chrome 34.0, and Safari 7.1.

  Note: Microsoft does not support Internet Explorer 9 and 10. We will provide limited support around the usage of these versions with CA Service Management.

- Apple Safari 7.1 support is only on MAC OS. Apple Safari is no more supported on Windows operating systems.
- CA Business Intelligence Dashboards are rendered optimally when Compatibility View display mode is enabled. Graphical glitches may appear in Dashboards if Compatibility View display mode is not enabled.
- If you use Internet Explorer 10 or 11 to view CA Business Intelligence pages, enable the Compatibility View mode to display the pages accurately.

LEGEND : **V** - Certified (Tested and Verified); **O** - Supported (Not Tested, expected to work) ; **x** - Not Supported

Browser	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1	CA EEM 12.5 CR02	CA Process Automation 4.3	CA Business Intelligence 4.1 SP3
Microsoft Internet Explorer	V	V	V	V	V	V	V	V
Microsoft Edge on Windows 10	V	V	x	x	V	Not Applicable	x	x
Mozilla Firefox ESR	V	V	V	O	V	x	V	V
Mozilla Firefox	O	O	O	V	O	x	V	x

Browser	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1	CA EEM 12.5 CR02	CA Process Automation 4.3	CA Business Intelligence 4.1 SP3
Google Chrome	V	V	V	x	V		V	x
Apple Safari	V	V	V	x	V	x	V	V

Mobile and Tablet Support

CA Service Management mobile app is available in Apple App Store and Google Play Store. This app replaces the earlier CA Service Desk Manager mobile app. The app enables access to Unified Self-Service through mobile devices running Apple iOS or Google Android OS. The following capabilities of Unified Self-Service are most commonly used and these are made available through the mobile app including:

- Reporting an issue by users
- Browsing Service Catalog for available services
- Requesting services
- Viewing/updating/approving service requests
- Viewing My Resources (hardware and software)
- Viewing the ticket queue by analysts
- Performing basic activities on tickets like escalate, reassign, update, and so on
- Viewing My Tasks (Approve/respond/act on assigned work items created by a workflow engine)
- Posting or answering questions on communities; if the community cannot answer your questions, reporting an issue

Note: For other UI interfaces, Apple Safari browser on the Apple iPad has limited and known support boundaries. The capabilities and experience of Apple Safari browser on the Apple iPad are not fully equivalent to using Apple Safari on an Apple MAC OS X desktop /laptop.

LEGEND : V - Certified (Tested and Verified); **O** - Supported (Not Tested, expected to work) ; **x** - Not Supported

Supported Platforms	Mobile App
iOS 8.0	V

Supported Platforms	Mobile App
Android 4.x	V

Unified Self-Service on Tablet

Supported Browsers	iOS 8.0	Android 4.x
Apple Safari	V	**NA**
Google Chrome	x	x
Mozilla Firefox	**NA**	x

Common Components Support

LEGEND : V - Certified (Tested and Verified); **O** - Supported (Not Tested, expected to work) ; **x** - Not Supported

CA Service Management includes common components CA EEM, CA Business Intelligence, and CA Process Automation. The supported versions of these components are as follows:

Note: CA Service Desk Manager, CA Service Catalog, and CA Asset Portfolio Management includes a limited entitlement to CA Process Automation and CA Business Intelligence. This entitlement is restricted to use within the context of Workflows associated with these products **.**

Common Components	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1
CA EEM (Embedded Entitlement Manager) 12.51 CR02	V	V	V	x	V
CA Process Automation 4.2 SP2, 4.3	V	V	V	x	x
CA Business Intelligence (CA BI) 4.1 SP3, SP5 (Patch)	V	V	V	x	x

Other Components Support

LEGEND : V - Certified (Tested and Verified); **O** - Supported (Not Tested, expected to work) ; **x** - Not Supported

CA Service management products include a few additional components like JRE, Apache Tomcat, .Net Framework, IIS, and PHP.

Other Components	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1
.Net Framework 4.0	x	x	V	x	x
Internet Information Server 8.0	V	V	V	V	V
Internet Information Server 7.0	V	V	V	V	V
Apache Tomcat	V	V	V	x	V
Java Runtime Environment (JRE)	V	V	V	V	V
PHP 5.4	x	x	x	V	x
Liferay Portal 6.1.2 GA3 (CE)	x	x	x	x	V

Following table lists specific versions of the common components that are used by CA Service Management products:

CA Service Management 14.1	Apache Tomcat	Java Runtime Environment (JRE)
CA Service Desk Manager 14.1	7.0.59	1.8.0_45 (32-bit)
CA Service Catalog 14.1	7.0.47	1.8.0_45 (32-bit or 64-bit)
CA Asset Portfolio Management 14.1	8.0.21 and 5.5.25	1.8.0_45 (32-bit)
Unified Self-service 14.1	7.0.40 and 7.0.59	1.8.0_45 (64-bit)

Integration and Interoperability Support

We recommend you to upgrade all CA Service Management capabilities in a customer environment using the common installer and common administration capabilities that are available with CA Service Management 14.1 solution. If you plan to upgrade product by product in a phased manner, use information in the tables below as a guideline to see the interoperability among the CA Service Management capabilities.

Unified Self-Service is an interface that is available with CA Service Desk Manager or CA Service Catalog, therefore, we recommend the following upgrades to leverage the enhanced usability improvements that are available in Unified Self-Service 14.1.

- If you are using 12.x versions of CA Service Desk Manager/CA Asset Portfolio Management and CA Service Catalog, you need to upgrade the CA Service Catalog to at least 14.1.
- If you are using 12.x version of CA Service Desk Manager/CA Asset Portfolio Management, you need to upgrade the CA Service Desk Manager to at least 14.1.

- If you are at 12.x version of CA Asset Portfolio Management and CA Service Catalog, you need to upgrade the CA Service Catalog to at least 14.1.

LEGEND : V - Certified (Tested and Verified); **O** - Supported (Not Tested, expected to work) ; **x** - Not Supported

CA Service Desk Manager interoperability/compatibility within CA Service Management capabilities are as follows:

Compatibility	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	Unified Self-Service 14.1
CA Service Desk Manager 12.9	V (Upgrade)	O	O	O
CA Service Desk Manager 12.7	V (Upgrade)	V	V	V
CA Service Desk Manager 12.6	V (Upgrade)	O	O	O
CA Service Desk Manager 12.5	V (Upgrade)	O	O	x

CA Service Catalog interoperability/compatibility within CA Service Management capabilities are as follows:

Compatibility	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	Unified Self-Service 14.1
CA Service Catalog 12.9	O	V (Upgrade)	O	x
CA Service Catalog 12.8	V	V (Upgrade)	V	x
CA Service Catalog 12.7	O	V (Upgrade)	O	x
CA Service Catalog 12.6	V	V (Upgrade)	V	x

CA Asset Portfolio Management (CA APM) interoperability/compatibility within CA Service Management capabilities are as follows:

Note: As Unified Self-Service requires either CA Service Desk Manager or CA Service Catalog, it is assumed that one of these products is available in the customer deployment along with CA Asset Portfolio Management.

Compatibility	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	Unified Self-Service 14.1
CA APM 12.9	O	O	V (Upgrade)	O

Compatibility	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	Unified Self-Service 14.1
CA APM12.8	O	O	V (Uninstall 12.8 and Upgrade)	O
CA APM 12.6	V	V	V (Uninstall 12.6 and Upgrade)	V
CA APM 11.3.4	V	V	V (Uninstall 11.3.4 and Upgrade)	O

CA Service Management integrations with other CA products is as follows:

Compatibility	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	Unified Self-Service 14.1
CA Workflow 1.1.5 SP6 Build 132	O	V	x	x
CA IT Client Automation 12.8 Fix Pack 1	V	V	V	x
CA Spectrum Automation 9.4	V	x	x	x
CA Configuration Automation 12.8 SP1, 12.8.3	V	x	x	x
CA Software Change Manager 12.5	O	x	x	x
CA Site Minder 12.5 CR01	V	V	V	V
CA Workload Automation AE 11.3.6	V	x	x	x
CA Clarity 13.3.0.286	V	x	x	x
CA Application Performance Management 9600	O	x	x	x
CA Identity Manager 12.6 SP4	V	x	x	x
CA Catalyst Connector 3.2	V	x	x	x
CA Services Operation Insight 3.0	O	x	x	x
CA Unicenter Network and Systems Management 11.2 SP2 CUM1	V	x	x	x

CA Business Intelligence compatibility with CA Service Management capabilities is as follows:

CA Service Management 14.1 requires a separate instance of CA Business Intelligence 4.1 SP3 before you upgrade or install CA Service Management capabilities. CA Service Management 14.1 is ***not*** compatible with earlier versions of CA Business Intelligence 3.3 SP1 and there is no direct upgrade from CA Business Intelligence 3.x to 4.x. For more information, see CA Business Intelligence Platform Installation. (https://docops.ca.com/display/CABI41SP3/CA+Business+Intelligence+Platform+Installation)

Compatibility with 14.1	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1
CA Business Intelligence 4.1 SP5 (Patch)	V	V	V
	V	V	V

Compatibility with 14.1	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1
CA Business Intelligence 4.1 SP3			
CA Business Intelligence 3.3 SP1	x	x	x

Internationalization and Localization Support

An Internationalized product (also referred to as a language-certified product) is an English-language product that runs on local language versions of the supported operating system and required third-party products. Internationalized products support local language data for input and output, and also support the ability to specify local language conventions for date, time, currency, and number formats.

The following list indicates the localized versions of the products that are supported depending on the operating system:

Note: IBM AIX supports English only.

Language	Operating System
German	Windows, Linux, Solaris
French	Windows, Linux, Solaris
French Canadian	Windows
Brazilian Portuguese	Windows
Italian	Windows
Spanish	Windows
Japanese	Windows, Linux, Solaris
Simplified Chinese	Windows

LEGEND : **V** - Certified (Tested and Verified); **O** - Supported (Not Tested, expected to work) ; **x** - Not Supported

Consider the following points:

- The installation of CA Business Intelligence 4.1 SP3 is supported only on English. For additional languages support, it is required to apply the language pack based on the locale as described in Full Installation (https://docops.ca.com/display/CABI41SP3/Full+Installation).
- CA Service Desk Manager 14.1 reports are localized in French, German, Italian, Japanese, Simplified Chinese, Spanish, and Brazilian Portuguese.

- CA Asset Portfolio Manager 14.1 reports are localized in French, Italian, German ,Spanish, Japanese, and Brazilian Portuguese.

- CA Service Catalog 14.1 reports are ***not*** localized.

Internationalization Support	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1	CA Business Intelligence 4.1 SP3
English	V	V	V	V	V	V
French	V	V	V	V	V	V
German	V	V	V	V	V	V
Japanese	V	V	V	V	V	V
Italian	V	V	V	V	V	V
Spanish	V	V	V	V	V	V
Brazilian Portuguese	V	V	V	V	V	V
Simplified Chinese	V	V	x	V	V	V
Korean	x	x	x	x	x	x
Traditional Chinese	x	x	x	x	x	x
French Canadian	V	x	x	x	x	x
Finnish	x	V	x	x	V	x
Dutch	x	V	x	x	V	x
Danish	x	V	x	x	V	x
Swedish	x	V	x	x	V	x

A translated product (also referred to as a Localized product) is an Internationalized product that includes local language support for the user interface, online help, and other documentation, as well as local language default settings for date, time, currency, and number formats.

LEGEND : V - Certified (Tested and Verified); **O** - Supported (Not Tested, expected to work) ; **x** - Not Supported

Localization Support	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1	CA Business Intelligence 4.1 SP3
English	V	V	V	V	V	V
French	V	V	V	V	V	V
German	V	V	V	V	V	V
Japanese	V	V	V	V	V	V
Italian	V	V	V	V	V	V

Localization Support	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1	CA Business Intelligence 4.1 SP3
Spanish	V	V	V	V	V	V
Brazilian Portuguese	V	V	V	V	V	V
Simplified Chinese	V	V	x	V	V	V
Korean	x	x	x	x	x	x
Traditional Chinese	x	x	x	x	x	x
French Canadian	V	x	x	x	x	x
Finnish	x	V	x	x	V	x
Dutch	x	V	x	x	V	x
Danish	x	V	x	x	V	x
Swedish	x	V	x	x	V	x

Accessibility Support

LEGEND : V - Certified (Tested and Verified); **O** - Supported (Not Tested, expected to work) ; **x** - Not Supported

Accessibility	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	CA Software Asset Manager	Unified Self-Service 14.1
Section 508 compliance	V	**O** (Only widgets are supported)	V	x	V
Web Content Accessibility Guidelines (WCAG) 2.0	V	**O** (Only widgets are supported)	V	x	V

Load Balancing Support

CA Service Management 14.1 supports the following load balancing techniques across the capabilities:

LEGEND : V - Certified (Tested and Verified); **O** - Supported (Not Tested, expected to work) ; **x** - Not Supported

Load Balancers	CA Service Desk Manager 14.1	CA Service Catalog 14.1	CA Asset Portfolio Management 14.1	Unified Self-Service 14.1	CA Software Asset Manager
Apache Tomcat	V	O	V	x	x
F5 Networks	V	O	V	x	x
Microsoft NLB	x	x	O	x	x

Supported Products for CA SDM Connector July 2015

		Catalyst Connector Version	
		r3.2	r3.4.1
	r12.9 CUM1	Certified with CA Configuration Automation r12.8 SP1, r12.8 SP2 Certified with CA Service Operations Insight r3.1, r3.2, r3.2 CUM3	Not certified with CA Configuration Automation Certified with CA Service Operations Insight r3.2 CUM2, r3.2 CUM3, r3.3, r3.3 CUM1
CA SDM Version	r14.1.01	Certified with CA Configuration Automation r12.8 SP1, r12.8 SP2 Certified with CA Service Operations Insight r3.1, r3.2 cum3.	Not certified with CA Configuration Automation Certified with CA Service Operations Insight r3.2 CUM2, r3.2 CUM3, r3.3, r3.3 CUM1

*The IFW Proxy is required for CA SOI integration that uses 3.2 container.

LEGEND : V - Certified (Tested and Verified); **O** - Supported (Not Tested, expected to work) ; **x** - Not Supported

Accessibility Features

CA Technologies is committed to helping all customers, regardless of their ability, to use its products and supporting documentation to accomplish vital business tasks. This section outlines the accessibility features that are part of CA Service Management.

This section contains the following topics:

- "Skip to Main Content" Navigation (see page 136)

Product Enhancements

CA Service Management offers accessibility enhancements in the following areas:

- Display
- Sound
- Keyboard
- Mouse

Note: The following information applies to Windows-based and Macintosh-based applications. Java applications processed on many host operating systems, some of which already have assistive technologies available to them. For these existing assistive technologies to provide access to programs written in JPL, they need a bridge between themselves in their native environments and the Java Accessibility support that is available from within the Java virtual machine (or Java VM). This bridge has one end in the Java VM and the other on the native operating environment, so it will be slightly different for each operating environment it bridges to. Sun is currently developing both the JPL and the Win32 sides of this bridge.

Display

To increase visibility on your computer display, you can adjust the following options:

Font style, color, and size of items

Lets you select font color, size, and other visual combinations.

Screen resolution

Lets you change the pixel count to enlarge objects on the screen.

Cursor width and blink rate

Lets you make the cursor easier to find or minimize blinking.

Icon size

Lets you make icons larger for visibility or smaller for increased screen space.

High contrast schemes

Lets you select color combinations that are easier to see.

Sound

Use sound as a visual alternative or to make computer sounds easier to hear or distinguish by adjusting the following options:

Volume

Lets you turn the computer sound up or down.

Text-to-Speech

Lets you hear command options and text read aloud.

Warnings

Lets you display visual warnings.

Notices

Gives you aural or visual cues when accessibility features are turned on or off.

Schemes

Lets you associate computer sounds with specific system events.

Captions

Lets you display captions for speech and sounds.

Keyboard

You can make the following keyboard adjustments:

Repeat Rate

Lets you set how quickly a character repeats when a key is struck.

Tones

Lets you hear tones when pressing certain keys.

Sticky Keys

Lets those who type with one hand or finger select alternative keyboard layouts.

Mouse

You can use the following options to make your mouse faster and easier to use:

Click Speed

Lets you select how fast to click the mouse button to make a selection.

Click Lock

Lets you highlight or drag without holding down the mouse button.

Reverse Action

Lets you reverse the functions controlled by the left and right mouse keys.

Blink Rate

Lets you select how fast the cursor blinks or if it blinks at all.

Pointer Options

Lets you complete the following tasks:

- Hide the pointer while typing
- Show the location of the pointer
- Set the speed that the pointer moves on the screen
- Select the pointer's size and color for increased visibility
- Move the pointer to a default location in a dialog box

Keyboard Shortcuts

The following table lists the supported keyboard shortcuts:

Keyboard	Description
Ctrl+X	Cut
Ctrl+C	Copy
Ctrl+K	Find Next
Ctrl+F	Find and Replace
Ctrl+V	Paste
Ctrl+S	Save
Ctrl+Shift+S	Save All
Ctrl+D	Delete Line
Ctrl+Right	Next Word
Ctrl+Down	Scroll Line Down
End	Line End
CA Service Desk Manager Keyboard Shortcuts	

Keyboard	Description
CA Service Catalog Keyboard Shortcuts	
Ctrl+Shift+Z	Reach the first service offering from the category tree in the browse widget.
v (small letter)	Open the popup window when you click the links in the list widget.
Ctrl+Shift+O	Reach the first button in button area when a request form is loaded and the focus is at any place in between the form.
CA Asset Portfolio Management Keyboard Shortcuts	
Alt+Shift+Ctrl+D	Resize a Dialog Box in the Downward direction
Alt+Shift+Ctrl+U	Resize a Dialog Box in the Upward direction
Alt+Shift+Ctrl+R	Resize a Dialog Box to the Right
Alt+Shift+Ctrl+L	Resize a Dialog Box to the Left
ESC	Close a Dailog Box
Ctrl+Shift+Down	View the Contents of a Drop-Down List
Unified Self-Service Keyboard Shortcuts	
Ctrl+1	Go to Home page
Ctrl+2	Go to Communities
Ctrl+3	Ask a Question
Ctrl+4	Go to User Profile
Ctrl+5	Reply to a Question **Note:** To use the keyboard shortcut to reply to a question (CTRL+5), you must be viewing the entire conversation.
Ctrl+6	Go to Questions
F1	Display Help

"Skip to Main Content" Navigation

The user interface has a **Skip to Main Content** link that allows users to quickly navigate to the the first data field in the user interface without having to tab multiple times to get to the main content on the page.

In CA SDM, this link exists as **Skip Navigation**. This link allows the Screen Reader users to skip the in-between links and navigate to the main content page. This link is available by default for the Customer and Employee roles. For the Analyst role, the link is available only when the Screen Reader mode is enabled.

Deprecated Features

CA Service Catalog - Reservation Manager Integration Deprecated

The point-to-point integration between CA Service Catalog and Reservation Manager is deprecated.

Instead of using the point-to-point methodology, consider setting up this integration by exchanging data through web service calls from custom CA Process Automation processes. This methodology lets you set up services so that users can modify, extend, or return early their existing reservations of physical or virtual resources.

For information about how to integrate CA Service Catalog with Reservation Manager, see this section (https://support.ca.com/cadocs/0/CA%20Service%20Catalog%2012%209-ENU/Bookshelf_Files/HTML/CA_Svc_Cat_Integration_ENU/index.htm?toc.htm?IntegratingwithReservationManager.html) on the CA Service Catalog 12.9 bookshelf.

CA Workflow Deprecated

CA Process Automation is the recommended process automation tool. If you are using CA Workflow process definitions, we recommend that you create and use CA Process Automation processes instead.

Note: For more information about installing and using CA Process Automation, see the CA Process Automation documentation.

CA Workflow integrations are not documented in this Wiki.

MYSQL - Unified Self-Service Integration Deprecated

Unified Self-Service (formerly known as, CA Open Space) no longer supports MYSQL databases. You can use Oracle and SQL Server databases for installing Unified Self-Service.

Known Issues

This section contains the following articles:

CA Service Management

Note: The CA Service Management 14.1 installation media includes the following legacy documents:

- CASM r12.5 Install Guide.docx
- CASM r12.5 Readme.txt

The installation media also includes the 12.9 bookshelves.

Ignore the legacy documents because they are not required for CA Service Management 14.1 installation.

All the deliverables for CA Service Management have been completely migrated to this Wiki. Access this Wiki for 14.1 documentation.

The following known issues can also affect how you manage the CA Service Management solution:

CA Service Management Known Localization Issues

Following are the localization known issues that are applicable for CA Service Management:

Chinese and Japanese Characters Do Not Appear Correctly in the Common Administration User Interface

When you create a user or a tenant through the common administration user interface and specify the details in Chinese or Japanese characters, the details are not displayed properly.

You may experience this behavior even when the details contain upper case non-English characters like Æ, Å, Ø, Ñ, É.

Help Calls from Some of the Localized Product User Interfaces Fail

When you launch the help or the link to the wiki from the localized product user interfaces, on some pages you get an error message "Unable to render {include} The included page could not be found". We are trying to resolve this issue as soon as possible.

Note: Some of the localized product user interfaces will launch the English Wiki space, which means that the documentation Wiki will not be available in those languages. For more information, see the Languages Supported (see page 118) section.

CA Service Desk Manager

This section contains the following known issues:

CA Service Desk Manager Known CA Products Issues

This article contains the following known issues:

CA Process Automation and SSL Integration Generates Errors

Symptom:

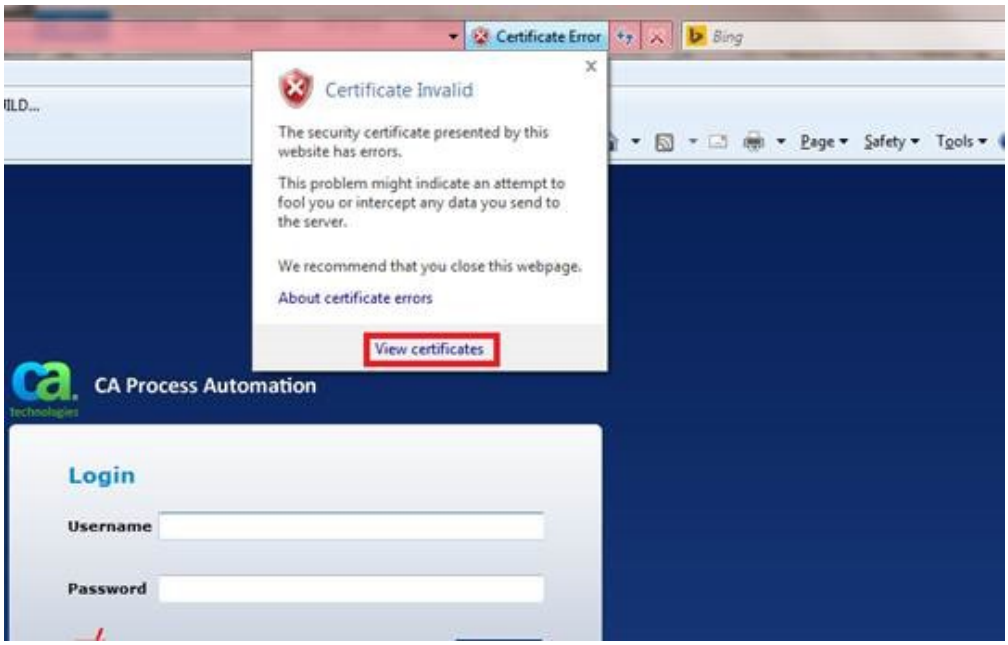
When trying to integrate CA Process Automation with SSL, the following SSL validation errors are seen during the installation:

```
2014/11/11 19.04.39.728 DEBUG [AWT-EventQueue-0] [PAMWebserviceManager] Get ITPAM
version
2014/11/11 19.04.39.752 ERROR [AWT-EventQueue-0] [PAMValidator] CA PAM validation
failed
com.ca.smsi.installcore.webservices.WebserviceException: ; nested exception is:
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX
path building failed: sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested target
at com.ca.smsi.installcore.webservices.PAMWebserviceManager.getITPAMVersion
(PAMWebserviceManager.java:265)
```

Solution:

This issue may occur because the Java Runtime Environment (JRE), under which the installer is running, is not able to connect to the CA Process Automation SSL URL. The needed SSL Certificates may be missing in the JRE. JRE obtains such SSL certificates from a keystore. Complete the following steps to add a CA Process Automation SSL certificate to the JRE keystore:

1. Download the SSL Certificate by accessing the CA Process Automation URL.



2. Copy this certificate file to some location. For example, *c:\ItpamCert.cer*

3. Extract the CA SDM DVD to a local drive. For example, C:\CASMDVD14\< >

4. Import the CA Process Automation SSL Certificate to a keystore file using the following command:

   ```
   c:\CASMDVD14\java\jre\bin\keytool -importcert -file c:\ItpamCert.cer -alias
   somealias -keystore c:/keystore_file -storepass somepass
   ```

5. To enter the keystore and password values to the JRE, open the C:\CASMDVD14\setup.lax file in Wordpad or a similar text editor.

   Note: It is recommended NOT to use Notepad so as to avoid any formatting issues.

6. Identify the "lax.nl (http://lax.nl).java.option.additional" property.

7. Append the reference to the JAVA keystore and keystorepass entries as follows:

   ```
   -Djavax.net (http://Djavax.net).ssl.trustStore=c:/keystore_file -Djavax.net (http:
   //Djavax.net).ssl.trustStorePassword=somepass
   ```

   After the modification, the line would look like:

   ```
   lax.nl (http://lax.nl).java.option.additional=-Djava.library.path=".\\java\\bin;
   -DGET_SD_PRESETS=true -Djavax.net (http://Djavax.net).ssl.trustStore=c:
   /keystore_file -Djavax.net (http://Djavax.net).ssl.trustStorePassword=somepass
   ```

8. Save the file and restart the setup by executing C:\CASMDVD14\setup.exe command.

GRLoader Compatibility

The General Resource Loader (GRLoader) for CA Service Desk Manager is distributed at level r14.1 and is backward compatible with all previous releases of CMDB.

Important! We recommend that you use GRLoader distributed with CA Service Desk Manager r14.1.

The following considerations apply to GRLoader:

- The GRLoader utility that is distributed with CMDB r11.x is not compatible with CA Service Desk Manager r14.1. Upgrade the utility to the version that is distributed with CA Service Desk Manager r14.1.
- For any third-party product that uses GRLoader, reinstall all the files and directories in the java\lib directory.
- Earlier releases of GRLoader, for example, GRLoader distributed with CA Cohesion ACM, may require an upgrade. Apply the appropriate patch.
- (Solaris only) When running GRLoader using pdm_task, the environment variable $NX_ROOT must not be exported from pdm_task. Prevent exporting $NX_ROOT, by doing one of the following:
  – Temporarily comment out the line where $NX_ROOT is exported.
  – Add a small script so that $NX_ROOT is not exported when pdm_task runs GRLoader.

  Note: In non-Windows operating environments, it can be useful to invoke GRLoader using pdm_task GRLoader <arguments>.

Unable to Access the Customized Tables Created from Web Screen Painter

Symptom:
I created a table using the Web Screen Painter but could not access the list page of this table from the CA Service Desk Manager Web UI.
Solution:
Customized table names must not contain the JavaScript keywords, such as alert, prompt, and confirm. For example, the customized table with the name, z_global_alert, is rejected by the CA Service Desk Manager webengine. Create the table with some other names and try again.

How to Review the Log Files

If a CA Business Intelligence installation fails, review the log files for further information. The log files contain error codes, presented as return values from certain functions. Until the installation directory is created completely, the installer dumps the installation logs in Windows temp (%TEMP%) folder.

After the installer directory is created, the installation logs are copied to <INSTALLDIR>\InstallData\logs directory with the timestamp. For more information about the CA Business Intelligence 4.1 SP3 installation,see the CABI Installation on Windows (https://docops.ca.com/display/CABI41SP3/CABI+Installation+on+Windows) topic.

CA Service Desk Manager Fails to Start after Previous Versions of eTPKI are installed after CA Service Desk Manager

Valid on Windows systems with other CA products installed after CA Service Desk Manager
Symptom:
The following message occurs while CA Service Desk Manager is starting:
Unable to connect to DB
CA Service Desk Manager fails to start when CA products with earlier versions of eTPKI are installed after CA Service Desk Manager.
Solution:
To avoid this issue, do the following:

1. Edit the system path: Move the PROGRA~1\CA\SC\CAPKI\Windows\x86\32\lib directory to the beginning of the path.

2. Start CA Service Desk Manager.

Error Adding Scoreboard to a Multi-Frame Form

Valid on all operating systems
Symptom:
When you add the Scoreboard to a multiframe form, the following error occurs:

```
Error: window.parent.scoreboard has no properties
```

For example, this problem occurs when you do the following:

1. Create a multiframe form.

2. Add the Scoreboard to one of the frames.

3. Publish the form.

4. Add the form to a tab, and the tab to a role.

5. Log in to CA Service Desk Manager using the role to which you added the tab or form. The following error message appears:

   ```
   Error: window.parent.scoreboard has no properties
   ```

   Note: For information about these steps, see the Online Help.

Solution:
Do not use the Scoreboard with multiframe forms.

Error While Launching the CA Process Automation Process Viewer

Valid on all operating systems
Symptom:
When a user tries to launch the CA Process Automation Process Viewer from CA Service Desk Manager, the following error message appears:

```
Unable to launch the application. [Client name][Publisher][From]
```

Solution:
The CA Process Automation installer uses the host name of the computer where it is installed to populate the information in the CA Process Automation configuration files. For CA Process Automation to operate properly, the host name has to be a reachable name from all computers that access CA Process Automation from CA Service Desk Manager. If there is an issue with the hostname value that is set during installation, the Administrator can change a CA Process Automation configuration file to resolve the problem.

1. On the CA Process Automation server open the %InstallationDir%\server\c2o\. config\OasisConfig.properties file.

2. Change the oasis.local.hostname to a value that is reachable from both the CA Process Automation server and from CA Service Desk Manager workstations.

   Note: Verify that the new hostname matches the CA Service Desk Manager Options Manager value set in the caextwf_processdisplay_url option.

3. Restart the CA Process Automation server.
   The user can launch the Process Viewer from CA Service Desk Manager. The host name is reachable from every computer that accesses CA Process Automation from CA Service Desk Manager.

CA Process Automation Client Launches with the Previous User Credentials

Symptom:
When I launch the CA Process Automation client, the client opens with the previous user credentials.
Solution:
CA Process Automation caches data such as for user names and passwords in the browser. This caching causes the client to open with the previous user credentials when a user clicks View Process or any process instance log under the Workflow Tasks tab of any ticket detail page.
Clear your browser cache before you log in to CA Service Desk Manager or open CA Service Desk Manager in a new browser.

404 Error is Displayed on Clicking the View Process Button

Symptom:

CA Service Desk Manager is integrated with CA Process Automation r3.1 SP1. When I click on the View Process button from CA Service Desk Manager, a 404 error is displayed.
Solution:

1. Select Options Manager, CA IT PAM Workflow.
2. Set the value of the caextwf_processdisplay_url option to the following:

   ```
   http://<wf_hostname>:<wf_tomcat_port>/itpam/JNLPRequestProcessor?
   processType=startUI&roid
   ```

3. Restart CA Service Desk Manager services.

Dependent CIs Belonging to Service Family Do Not Display on the Change Scheduler

Symptom:
Dependent CIs that belong to the CI families: Enterprise Service and Service do not display on the Change Scheduler if the Service family in the table ci_resource_family has an table_extension_name different from "serx."
Solution:
Change the table_extension_name for the Service family to "serx."

Configuration Item Reconciliation Attributes Are Not Tenant Aware

Valid on all systems with a multi-tenancy installation
Symptom:
The user cannot create a configuration item because it conflicts with another configuration item owned by a different tenant. The following reconciliation attributes are not tenant aware:

- Name
- Serial Number
- Hostname
- DNS Name
- Asset Tag

Solution:
To prevent this conflict, append the name of the tenant to one or more of the reconciliation attributes.

Support Automation Creates a Temporary Folder Named CA-SupportBridge

Symptom:
When end users and analysts use Support Automation, they cannot locate the temporary Support Automation folder. The temporary folder stores files, such as executables, from the end-user client and Support Automation Analyst Interface.
Solution:
The temporary folder created by the applications is named CA-SupportBridge, such as in the C:\Documents and Settings\All Users\Application Data\CA-SupportBridge directory.

Purge on a CA Support Automation r6.0 SR1 eFix5 Database Does Not Export Inactive Users

After running the historical data purge script on the CA Support Automation r6.0 SR1 eFix5 database, inactive users (those that have not been involved in an assistance session during the retained history time period) are not exported to the CA Service Desk Manager database.

CA BSI Metric Data Does Not Display Properly

When you integrate CA Service Desk Manager with CA BSI, users can display Metric data for Contract CIs that are associated with a CA BSI MDR. Users must specify a Contract Party (CA BSI Entity) before they submit the request. A CA BSI limitation prevents metric data from being properly displayed for Contract Parties that have certain non-alphanumeric characters within the name. We recommend that you use alphanumeric Contract Party names and avoid using any of the following characters:
reserved = gen-delims / sub-delims
gen-delims = : / ? # [ ] @
sub-delims = ! $ & ' ( ) * + , ; =

CA NSM Integration

CA Service Desk Manager customers that plan to integrate with CA NSM must apply a CA NSM patch that enables the integration using the CA Service Desk Manager r14.1 WSDL. You can download the CA NSM patch from CA Support Online (https://support.ca.com/irj/portal/newhome).

No Restriction in Multiple Selection of Same File for Upload

Applicable for tickets, repositories, and knowledge.

Example:

1. Log in to CA Service Desk Manager and choose a file to attach to a ticket.
   The file name appears in the list.

2. Again choose the same file.
   The same file appears twice in the list.

Solution:

Ensure that you do not choose the same file more than once for upload. Delete all duplicate files and then upload.

Federated Search Does not Work After CA SDM Upgrade

Symptom:

1. I installed CA SDM 12.9 and configured Federated Search.

2. I upgraded CA SDM and tried to perform the Federated Search.
   Federated search did not work ad the following error message is displayed in the jfscrawler. log file.

```
09/17 15:12:38.031 [http-bio-8040-exec-2] ERROR SearchService 181 Source name
(google) not found in configured list of search adapters


09/17 15:12:38.032 [http-bio-8040-exec-2] ERROR SearchService 303 Exception
error occurred for adapters([]) on uri(http://lodiibmsdm7:8040/cafedsearch/sdm
/search?q=testing&source=google&userid=srvcdesk&index=1&size=10&_type=json)
```

Solution:

Regenerate the following files:

- adapters-config.xml
- google.xml
- sharepoint.xml
- OpenSpace.xml
- Customized adapters xmls

Unable to Launch Support Automation Script Editor Application

Valid for Windows 8.1

Solution:

Currently no solution exists.

CIs created using the Copy (Including all Relationships) function are not displayed in the CA SOI service graph

Symptom:

You created a CI in CA SDM which is updated in the CA SOI graph. Now, you create another CI in CA SDM using File, Copy (Including all Relationships) and check the graph in CA SOI. The new CI is not updated in the graph.

Solution:

To view the added CIs, import the service graph on CA SOI again.

Incorrect TWA Update Transaction for a blank Configuration Status

Symptom:

You changed the Configuration Status of a CI in CA SOI console to production, but the Configured Status attribute is missing in TWA.

Solution:

Manually reset the service status in CMDB for the CI.

Services without alerts are not loaded in CA SOI

Symptom:

For a service, you remove the Alert option from the Exclude CI Type list of the Configuration settings. You import the service on CA SOI. The service is not loaded on CA SOI.

Solution:

Disable the alert for the service.

Follow these steps:

1. Add Alert to the Exclude_USM_CI_type property during the CA SDM Connector configuration.
2. Restart the CA SDM Connector.

Unable to rename a service CI in CA SOI

Symptom:

You edit the name of a CI on the CA SOI console. The CI is not renamed and a new service CI is created with the edited name.

Solution:

CA SOI does not handle decorrelation of some type of CIs, for example, USM:Service. When such CIs are renamed, CA SOI sends a new CI to be created in CA CMDB, while the old one still exists.

CA Service Desk Manager Known Client Issues

This article contains the following known issues:

Unable to Launch the Support Automation Web Chat Client Session

Symptom:
The web chat client session can only be launched after closing the existing browser and opening a new browser. You encounter the following problems when you configure the supportautomation_url with an IP address:

- The web client end user does not launch after the first web client end-user session is closed. The Post Logout page displays the following message: Your Live Assistance Session is complete.

- Different web client end-user consoles are merged with the existing web client session when you try to launch a different web client end-user console on the same computer in the same browser window.

Solution:
If the supportautomation_url configuration uses an IP address which has an existing host name mapping, the HTTP request processing resolves to this host name. You can change the configuration of supportautomation_url to the host name or you can remove the mapping of the IP address to host name to resolve the issue.

Unable to Run the Support Automation Agent Installer Silently

Valid on Windows 8 with UAC enabled or disabled, Windows 7 with UAC enabled. Vista with UAC enabled
Symptom:
I am unable to perform silent install or silent uninstall on the Support Automation Agent installer.
Solution:
To run the installer silently, user must be using a built-in administrator account. If the user is a created administrator (non-built-in administrator), complete the following steps to install or uninstall silently:

1. Open the command prompt, as the administrator.
   The UAC window is displayed.

2. Click Yes on the UAC window, go to file location of silent installation bat file and run the batch program.

Unable to Perform Some Support Automation Tasks (Chat, Automation, File Transfer, Remote Registry, and so on)

Valid on Windows XP 64 bit machine with pre-installed Support Automation agent.
Symptom:
Remote control and screenshot functionalities are working, while the remaining functionalities (for example, Chat, Automation, File Transfer and Remote Registry, and so on) are not working.
Solution:
Currently no solution exists.

Unable to Use the Remote Control Functionality

Valid on Windows 8 machine with pre-installed agent
Solution:
Make the following registry changes on the end-user machine:

- Hive: HKLM
- Path: SYSTEM\CurrentControlSet\Control\Windows
- DWORD: NoInteractiveServices
- Change value "1" to "0"

We also recommended that when an analyst tries to do Remote Control with the end user, the end-user machine must be accessed as a console session and not by any other remote desktop protocols.

Unable to Create Registry keys Under HKEY_LOCAL_MACHINE, Software

Valid on Windows 7, 8 and Vista with UAC enabled
Symptom:
SA analyst has initiated a Live chat session with a SA end user. Both SA analyst and SA end user are on different machines and the SA end user has logged in to Support Automation as a created administrator. SA analyst tries to create a registry key under HKEY_LOCAL_MACHINE, Software on the SA end user machine (Windows 7, 8 and Vista with UAC enabled). An error message is displayed.
Solution:
Use the impersonate feature, and impersonate as the built-in administrator to work with registry keys.

Support Automation Analyst Cannot Use Remote Control During the Assistance Session

Valid on Windows Vista, Windows 7, Windows 8, and Windows 8.1

Symptom:
When I use Remote Control during an assistance session, I try to run an application as Administrator and I use the provided Administrator credentials in the User Account Control window. I do not have control on an opened application in the Remote Control session on the end-user computer.
Solution:
Windows Vista, Windows 7, and Windows 8 do not display the User Account Control (UAC) window or any Secure Desktop window for the Support Automation Analyst during the web launch. You can only switch between the Desktops to display the secure Windows window when the end-user computer runs the CA Support Automation Agent Service.

Unable to View the HKEY_LOCAL_MACHINE\SOFTWARE Sub Registry Keys

Valid on Windows 64-bit computers
Symptom:
When the end user uses a 64-bit client computer, the registry key behaves as the following cases:

- During an assistance session, a user creates, modifies, or deletes registry keys under HKEY_LOCAL_MACHINE\SOFTWARE on the end-user computer from the Support Automation Analyst Interface. These keys display under the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node on the end-user computer.

- A user creates, modifies, or deletes registry keys under HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node on the end-user computer and starts the assistance session. The keys display under the HKEY_LOCAL_MACHINE\SOFTWARE in the analyst session.

- A user creates, modifies, or deletes registry keys under HKEY_LOCAL_MACHINE\SOFTWARE on the end-user computer and starts the assistance session. The keys do not display under the HKEY_LOCAL_MACHINE\SOFTWARE in the Analyst assistance session.

Note: The HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node key is transparently presented to 32-bit applications by WoW64 as HKEY_LOCAL_MACHINE\SOFTWARE. For more information, see the MSDN article titled Registry Keys Affected by WOW64.

Error Message Appears When Launching the Support Automation Analyst or End-User Clients

Valid on Internet Explorer 9, 10, and 11
Symptom:
For the Support Automation end-user client, if your CA Service Desk Manager site is in an Internet zone (or any other zone) with a security level higher than Medium-Low, Internet Explorer blocks pop-up windows and the end user is not able to launch the Support Automation client.
For the Support Automation analyst client, if your CA Service Desk Manager site is in an Internet zone (or any other zone) with a security level higher than Medium-Low, Internet Explorer blocks downloads and launches from IFRAME, and the analyst is unable to launch Live Assistance.
Solution:
For the Support Automation end-user client, move the CA Service Desk Manager site to the Trusted Sites Zone and set the security level to Medium-Low, or allow pop-up windows from the CA Service Desk Manager site.
For the Support Automation analyst client, move the CA Service Desk Manager site to the Trusted Sites Zone and set the security level to Medium-Low. You can also set a Custom security level by setting the Enable for Downloads and Automatic prompting for file downloads options.

Submenu Does Not Disappear from the Page in iOS

Valid on the Apple iPad
Symptom:
When I click the File Menu on the Service Desk tab, the submenu does not disappear until I select any links from the submenu or any other tab. If I click a different link on the form, the submenu does not disappear.
Solution:
The iOS has a limitation that causes this behavior because the iPad does not use a mouse.

Cygwin Environment Causes Application Problem

Symptom:
I can launch CA Service Desk Manager Java applications from a Cygwin environment using an AIX server, but the application buttons are not operable.
Solution:
This behavior is a problem with the Cygwin environment. Use a different emulator.

Functionalities in Change Calendar Are Not Accessible

In the Change Calendar tab, if you click the back button in Internet Explorer, you cannot access the functionalities of the change calendar. The object that does not support the error displays. Log out from CA Service Desk Manager to access the Change Calendar tab again.

iOS Crashes when Selecting a Contact During Ticket Creation

Valid on iOS
Symptom:
When I create a ticket and want to add a contact, the browser crashes. The auto-correction feature of iOS and the search-as-you-type feature of CA Service Desk Manager retrieve results and the user selects the contact that CA Service Desk Manager retrieves.
Solution:
Disable the auto-correction feature on iOS.

Child Windows Do Not Close After Logging Out on the iPad

Valid on iPad iOS 5
Symptom:
After I log out of CA Service Desk Manager on the iPad, the child windows do not close. For example, I click File, New Change Order. I log out of CA Service Desk Manager and the New Change Order window remains open and I can still enter data.
Solution:
The iOS 5 operating system has an issue when you close the window using the handle (close() API). For more information, use an internet search engine to look for "iPad Safari IOS 5 window.close()."

PDA Interface Displays Error Message when Creating a Ticket

Valid on the PDA interface
Symptom:
If two or more contacts have the same first name, last name, and middle name combination and I add the user to the End User, Requester, or Assignee fields, I cannot create tickets from the PDA interface.
The PDA interface displays one of the following error messages:

- Multiple Matches - Affected End User: XXXX
- Multiple Matches - Requester: XXXX
- Multiple Matches - Assignee: XXXX

Solution:
Use the regular CA Service Desk Manager user interface which does not display these errors.

CA Service Desk Manager Known Knowledge Management Issues

This article contains the following known issues:

Unable to Batch Import Knowledge Documents Using the keit_daemon Command

Valid on Linux

Solution:

The problem may occur while importing SampleData by using ImportSampleData script. Import the packages individually using pdm_kit command.

Comma Not Supported in Name Fields

Valid on all operating systems
Symptom:
A comma in a name field can cause unexpected results in the display of the combined user name. For example, entering a name such as the following while creating or updating a contact record causes the combined name to display incorrectly:

- Last Name: Smith, Jr
- First Name: John
- Middle Name: <blank>

The comma causes "Jr" to appear in the first name position and "John" not to appear.
Solution:
Avoid using the comma character in a name field.

Searching for a Document That Has White Spaces in the Title Causes Failure

Valid on all operating systems
Symptom:
You create a Recommended Document from Knowledge, Search, Recommended Documents, Create New. The Title text (as displayed in Edit mode) contains a leading space or double spaces between title words.
When I type the title words and use the auto-completion feature in the Knowledge Document text field, the Knowledge Document Lookup page opens with no results found.
Solution:
You must invoke the Knowledge Document Lookup Form by clicking the link on the Create New Recommended Document page. From the Knowledge Document Lookup Form, do the following:

1. Enter the title text.
2. Search for the document.
3. Select the correct record.

Note: If you fail to do this solution and enter the title words into the text field (without observing correct white-space), auto-completion is invoked, and the Knowledge Document Lookup page opens with no results found. If no results occur, clear the search filter on the Knowledge Document Lookup page, manually enter keywords in the title into the Keywords for Advanced Search field, and click Search.

Wrong Number of Documents Are Returned in Search Results

Symptom:
The incorrect number of knowledge documents are returned in search results.
Solution:
To resolve this issue, run pdm_k_reindex +f from the command line. The correct number of documents appears in the search results.

Unable to Export Documents from Templates

Symptom:
I am unable to export a document using the export or import template. I click the Export button from Documents, Export/Import Templates, but the action does not initiate the exporting function.
Solution:
Incorrect handling of embedded links that reference CA Service Desk Manager objects instead of files in a repository cause this error. A warning message displays when you click the Export button, similar to the following example:
02/17 15:55:05.30 hostname keit_daemon 4088 WARNING export.c 645 The link 'New Request from a template - 400002'' which references a Service Desk object was encountered. The target object will not be exported. As a consequence, if the link is invalid or incorrect on the server where the document is re-imported the document will need to be altered to reference the correct object.
Using Insert, New Ticket Link lets you automate part of the request or automate another ticket type creation process for users. However, during export while the text in the resolution field exports as is, the linked ticket template cannot export with it.

1. Reimporting the document to the same CA Service Desk Manager cluster (as defined by a shared backing data store) that it was exported from works correctly.
   The reimport works if the referenced ticket still exists.

2. If you want to export the document to a different CA Service Desk Manager cluster, modify the resolution to verify that the linked ticket template actually references a ticket template.

3. Verify that the template references the correct ticket template.
   This issue affects all links to CA Service Desk Manager objects within Knowledge Documents.

CA Service Desk Manager Known Localization Issues

This article contains the following known issues:

Installer and Component Installers Translated Incorrectly

Valid in all localized versions
Symptom:
The installer and some of the component installers display strings that are not translated correctly. For example, minor spelling or grammar problems can occur in the title bar, on buttons, or in dialogs.
Solution:
The errors have no impact on the functionality of the product.

Unable to View the CA Service Desk Manager Reports in Localized Languages

Solution:
CA Service Desk Manager reports support all CA Service Desk Manager supported languages, except Brazilian Portuguese, and French Canadian, with the following exceptions:

- CA Service Desk Manager reports content will be in Brazilian Portuguese and CABI will be in English when Brazilian Portuguese is integrated with CABI multilingual installation.

- CA Service Desk Manager reports content will be in French Canadian and CABI will be in French when French Canadian is integrated with CABI multilingual installation.

To view the CA Service Desk Manager reports in the required languages (for example, Japanese, French, German, and so on), complete the following steps:

1. While installing BO, install required language packs to get the localized strings that are part of BO.

2. Install Arial Unicode MS (True Type) font on the server where BIAR file will be imported.

3. The font files have to be copied to the Fonts folder of windows.

4. Add the following code to fontalias.xml and i18n.xml files:

Note: Find the fontalias.xml file in the <BO Installation Path>\BusinessObjects Enterprise 12.0\win32_x86\fonts directory.

Find the i18n.xml file in the <BO Installation Path>\BusinessObjects Enterprise 12.0 \win32_x86\scripts directory.

```
<FONT NAME="Arial Unicode MS">
<FONTFAMILY PLATFORM="ttf" NAME="Arial Unicode MS">
<FONTATTRIBUTE BOLD="false" ITALIC="false" LOGICAL="Arial Unicode MS"
PHYSICAL="ARIALUNI.TTF"/>
</FONTFAMILY>
<FONTFAMILY PLATFORM="win" NAME="Arial Unicode MS"/>
<FONTFAMILY PLATFORM="java" NAME=" 'Arial Unicode MS', 'Arial Unicode MS'"/>
<FONTFAMILY PLATFORM="html" NAME=" 'Arial Unicode MS', 'Arial Unicode MS'"/>
</FONT>
```

When the user opens the reports document, Business Intelligence Launch Pad tries to display content in the user's Preferred Viewing Locale (PVL).
If no visible translation is available in the PVL, Business Intelligence Launch Pad tries to display the translation in the Substitution language.
If no visible translation is available in the substitution language, Business Intelligence Launch Pad tries to display the translation in the Dominant locale of the user's PVL.
If no visible translation is available in the dominant locale, Business Intelligence Launch Pad displays the Original content language.

Note: Following are the localization limitations:

- Localization of crystal reports prompts are not supported.
- Localization of chart labels are not supported.
- Localization of reports folder structure (tree control), report titles, and descriptions in the List view of Business Intelligence Launch Pad are not supported.

- Group Tree labels cannot be localized in Crystal Reports when a Group Name is based on a conditional Formula.
- Y-Axis chart labels in Crystal Reports are shown horizontally in Firefox browser, while they are shown vertically in IE browser.
- Dashboards are partially localized. Tabs within the Dashboards and charts are not localized.
- Timestamp is not displayed by default in new Webi Reports.
- Date format does not change based on the browser locale because all the date formats are hard coded in CA Service Desk Universe as "mm/dd/yyyy hh:mm:ss AM/PM". By removing the date format, there is an Impact on Webi Reports. By default, only date part will be displayed in new Webi Reports.You can change the date format in Webi Report to display the correct timestamp.

CA EEM Install Fails on Windows 2008 SP2

Valid on all languages
Symptom:
The CA EEM install fails on Windows 2008 SP2 with the following message:
Windows 2008 sanity testing failed.

Note: The message appears in English for all languages.

Solution:
Before you install the CA EEM Server on Windows 2008, do the following:

1. Run the netsh-> interface-> ipv6-> show-> address command from the command prompt.
   All the interfaces in the computer that use the IPv6 link-local addresses starting with fe80 are listed.
2. Delete the link-local address starting with fe80.
   The link-local address is removed.

Note: For more information about how to remove the interface, see the Microsoft Support website and refer to KB article 929852.

Two Windows Menu Shortcuts for the CA EEM Documentation and UI Items

Valid on all localized versions
Symptom:
After upgrading CA EEM for a Non-English language OS environment, two Windows menu shortcuts for the CA EEM Documentation and UI items can appear. One item displays in the local language, and

the other item in English.
Solution:
Delete the unwanted duplicate menu item.

Hot Keys Not Working in Context Menus

Valid on Japanese and Chinese localized versions
In the Japanese and Chinese localized versions, most right-click context menus do not include a hotkey character that works for each menu item. Typically, the hotkey character is placed between parentheses after the translated characters of the menu item; (_) is placed instead. In some cases, where the menu text includes English, the hot key is designated with an underscore and it works.

Some Values in the Option List Are Not Translated

Valid in all localized versions
Symptom:
The string "Auto Issue Event" is not translated in the "Value" Column of the Option List.
Solution:
Most of the fields on the Option List and Options Detail Web form with the exception of the Description field, certain Value fields such as Yes/No, and drop-down lists are not localized and appear in English. The Option List is found by navigating the left pane menu on the Service Desk Manager Administration tab to the Options Manager node and select any child node.

Language Valid Character Range Does Not Display Correctly

Symptom:
When I try to view kt_admin_parse_settings.htmpl, the Language Valid Character Range does not display correctly.

Solution:
No solution is available.

Localized Noise Words

Valid in all localized versions
Symptom:
Noise words for your language do not display.
Solution:
Each language has its own set of noise words that are delivered with the product.
To see the noise words for your language, run pdm_k_reindex in the same manner as when you want to add a noise word.
The noise words for your language appear.

Alias Name is not Localized

The alias name data that appears on the Attributes Alias List and the Attributes Alias Detail pages is not localized. For example, when you select Service Desk, Application Data, Codes, Attribute Aliases and click Search, the data that appears in the Alias Name column appears only in English.

8.3 File Name Creation and Extended Character Support

Valid in Japanese and Chinese localized versions
Symptom:
8.3 file name creation and extended character support are not supported.
Solution:
Perform the following steps:

1. Modify the NtfsAllowExtendedCharacterIn8dot3Name registry key to "0".

   Note: The value is set to "1" as default; manually change this setting.

2. Restart your computer.

3. Start the install.

Command-Line Utilities Cannot Display Special Characters

Valid in all localized versions
Symptom:
All CA Service Desk Manager command-line utilities that run from a DOS command prompt do not correctly display data that is returned. In particular, Japanese characters, Chinese characters, and special Latin characters with accents such as a German umlaut or a French accent grave are not displayed correctly.
Solution:
The output of command-line utilities, for example, pdm_extract can be redirected to a file, and then successfully read using any tool that supports UTF-8 encoded characters, for example, Microsoft Notepad.

Command-Line Tools Output Strings Incorrectly on Windows

Valid in all localized versions on Windows
Symptom:
Command line utilities display incorrect characters in output.
Solution:
Use the pdm_cmd.exe program to run all command line tools. The pdm_cmd utility converts output strings of the command line tool from UTF8 to UNICODE, so it can display the output strings in a foreign language. For example, to display output characters for pdm_webcache correctly, run the pdm_cmd pdm_webcache command. If the command line file name does not end with .exe, use the full file name on the command line.
For example, use the pdm_cmd pdm_publish.cmd command to publish Web Screen Painter schema changes. Use the pdm_cmd pdm_odbc_start.bat command to start the ODBC driver.

Note: Any command line tool that displays incorrect characters must run pdm_cmd.

Spell Check Not Working as Expected

Valid in all localized versions
Spell Check is not supported in the Japanese and Chinese localized versions.
Symptom:
Spell Check suggests almost every word in Latin localized versions.
Solution:
Perform the following steps:

1. Set the lex_lang option to the correct language in the Options Manager.
2. Restart the Service Desk Service.

Only U.S. States and Canadian Provinces Display for All Localized Versions

Valid in all localized versions
Symptom:
The State list selection in the CA Service Desk Manager web client only displays U.S. states or Canadian provinces regardless of the country selected.
Solution:
CA Service Desk Manager includes a database table for states and provinces. The product delivers data for this table consisting of only U.S. states and Canadian provinces. States or provinces for other countries are not included in the data provided, but you can modify the ca_state_province table to include additional states for other countries.

Characters Not Displayed in Linux SuSE Installation and Configuration

Valid in Japanese and Chinese localized versions on Linux SuSE
The CA Service Desk Manager installer and configuration program (pdm_configure) cannot display Japanese and Chinese Korean characters.

Hot Keys Defined as Dollar Signs

Valid in Japanese and Chinese localized versions
The dollar sign ($) is used as the hotkey in all forms when there is no other hotkey character available. In previous versions, the hotkey was picked from a list in the alphabet. In this release, CA Service Desk Manager determines the hotkey character from the corresponding English label.

Characters Not Translated During Upgrade

Valid in all localized versions on Linux and Solaris
All characters are displayed in English during the Migration step of an upgrade from Unicenter Service Desk r11.2.

CA CMDB Visualizer Date Helper Does Not Translate the Month and the Day

Valid in all localized versions
The name of the month and days of the week are not translated in the Date Helper in the Maintenance section of the scoreboard in the CA CMDB Visualizer.

CMDB Visualizer Date Format Cannot Be Localized in Japanese and Chinese

Valid in Japanese and Chinese localized versions
Symptom:
The date format in Maintenance section of the CMDB Visualizer Web Client cannot be localized.
Solution:
The CMDB Visualizer Web Client displays dates in the format dd/mm/yyyy. The preferred format for Japanese and Chinese is yyyy/mm/dd.

CMDB Visualizer Date Helper Does Not Translate the Month and the Day

Valid in all localized versions
The name of the month and days of the week are not translated in the Date Helper in the Maintenance section of the scoreboard in the CMDB Visualizer.

CA CMDB Visualizer Date Format Cannot Be Localized in Japanese and Chinese

Valid in Japanese and Chinese localized versions
Symptom:
The date format in Maintenance section of the CMDB Visualizer Web Client cannot be localized.
Solution:
The CMDB Visualizer Web Client displays dates in the format dd/mm/yyyy. The preferred format for Japanese and Chinese is yyyy/mm/dd.

CA CMDB Visualizer Does Not Support Login with Non-English User Credentials

Valid in all localized versions
CA CMDB Visualizer does not support login with Non-English User credentials.

Process Definitions in the CA Workflow IDE Appear in English

Valid in all localized versions
CA Workflow IDE process definitions are not localized and appear in English.

Support Automation End-User Assistance Session Pages Display in English

Valid in all localized versions
Symptom:
Support Automation Live Support: Assistance Session Web Page displays in English.
Solution:
All default Support Automation end user interface pages are not localized, such as the On Hold, In Session, Post-Launch, and Post-Logout pages. You can customize these pages and configure custom localizations from the Support Automation node on the Administration tab.

The Support Automation Adaptations Page Does Not Show the Localized Language Name

Valid in all localized versions
Symptom:
When I migrate a non-English CA Service Desk Manager from a previous release (r11.2, r12, or r12.1), the following areas display in English:

- Administration tab: Support Automation, Branding, Adaptations list page, shows the English row (in the respective localized language) instead of showing the actual localized language name.
- Click Live Chat on the Employee Home page, and the Localization list box shows English (in the respective localized language) instead of showing the actual localized language name.
- Support Automation Tab: From View Preferences, Support Automation Analyst UI, the Localization list box shows English (in the respective localized language) instead of showing the actual localized language name.

For example, in the Brazilian Portuguese localized SDM, after migration displays "Inglês" instead of "Português do Brasil."
Solution:
On the Administration tab, Support Automation, Adaptations, Localization Admin, enable the installed localized language name so that it is available with English.

Note: You cannot disable the English language when you migrate a non-English localized CA Service Desk Manager from r11.2, r12.0, r12.1.

Knowledge Search Parse Settings Set to English in Localized Versions

Valid on all localized versions
Symptom:
From the Search node in Knowledge Administration, the Language Type setting on the Parse Settings page is set to English by default in localized versions of CA Service Desk Manager. The product parses search text according to the language specified.

Web Screen Painter Shows English Strings While in Design Mode

Symptom:
When Web Screen Painter is in design mode, notebook tabs, buttons, menus, and the menu items appear only in English.
Solution:
To view a form in another language, do the following:

1. Open the form in Web Screen Painter.
2. If you are creating a form or updating an existing form, add the new localized strings to the $NX_ROOT/sdk/scripts/msg_cat.js file.
3. Click Preview.

Positions of Month and Day Options are Not Switched

Symptom:
I select the Yearly option when creating a Change Window for a Change Order. The Month and Day options appear in a different order.
Solution:
Customize the form in WSP to modify the positions of the Month and Day options.

Workshift Schedule Data Can Only Be Entered in English

Valid on all localized versions
Symptom:
If I use localized Workshift data, an error message appears when scheduling the Workshift.
Solution:
CA Service Desk Manager only supports English text for workshift schedule data, including days of the week, dates, and morning (am) and afternoon (pm).
The following examples display Workshift data in the correct formatting:

- Mon - Fri {8:00 am - 5:00 pm}
- Sun {9:00 - 12:00 2:00 pm - 4:00 pm}
- Sat 12/24/08 - 1/1/05 {8:00 - 12:00 14:00 - 4:00 pm}
- 7/4/09

Note: This restriction only applies to the Workshift schedule data. You can specify the Workshift display name in any localized language.

CA Process Automation Does Not Process Japanese Character Values Correctly

Valid on Japanese localized versions
Symptom:
I am able to install and run CA Process Automation and display characters correctly, until I run a CA Process Automation process that requires Japanese values being sent to CA Service Desk Manager. This action causes the process monitor to display question marks (??) in the values and CA Service Desk Manager rejects input by displaying ?? errors in stdlog.

Solution:

Important! This information supersedes the instructions in the CA Process Automation documentation.

For SQL Server

Your SQL Server database uses an incorrect collation, such as SQL_Latin1_General_CP1_CI_AS. You cannot change the collation after creating the SQL Server database.

1. Install SQL Server with the ability to create databases with Japanese codepages.
2. During the CA Process Automation installation, complete one of the following tasks:
   - Create the database with Japanese codepages manually.

- Select the Japanese codepage within the CA Process Automation installer and create the database.

Note: If you manually create the database, match the codepages from the CA Process Automation installer drop-down list with the database codepages. The installer does not detect this option or change the default codepage from Latin. CA Process Automation does not warn you about incorrect settings.

For Oracle

1. Verify that you created and started the CA Service Desk Manager database instance with the locale set correctly. For Japanese, set the locale set to ja_JP.UTF-8.

2. Verify that CA Process Automation database also started in the Japanese locale.

CMDB r11.2 German and Japanese Upgrade Detects French Locale

Valid on German and Japanese Versions
Symptom:
When upgrading CA CMDB r11.2 German or Japanese versions, the Installer upgrade program automatically detects the French locale instead of the German or Japanese locale. When the French version is detected an error message appears and the installation fails. The user cannot switch to the German or Japanese locale from the Installer.

Solution:
To resolve this issue, do the following:

1. On the CA Service Desk Manager server, navigate to the NX_ROOT directory.

2. Open the .GENLEVEL file for editing.

3. Replace 12611053G900 with 11209045R4

4. Navigate to the NX_ROOT/Site directory.

5. Open the install.properties file for editing.

6. Replace locale.current=en-US with one of the following:
   locale.current=ja-JP (Japanese)
   locale.current=de-DE (German)

7. Save your changes and run the upgrade.

The correct locale is detected.

GRLoader Does Not Identify Non-English Spreadsheet Sheet Names

Valid on all English Operating Systems

Symptom:

GRLoader does not identify non-English spreadsheet sheet names when I use the -sss option on an English OS.

Solution:

Specify the non-English spreadsheet sheet names in a configuration (.cfg) file with the grloader. spreadsheet.sheetname=name option if you run GRLoader on an English OS.

Installer Does Not Auto-Detect Local Languages

Valid on Windows 2008

Symptom:

The Setup Language screen in the CA Service Desk Manager Installer does not automatically detect the local language on Windows 2008. To proceed with the installation, the end user must select a language in this screen. The problem occurs when the format, system locale, and location options are not specified correctly in Regional and Language Options. Additionally, the product displays misplaced special characters (commas and periods) when the Format tab in Regional and Language Options is not set to the correct language.

Solution:

Set the format, language, and system locale for your environment as follows:

1. From the Control Panel, select Regional and Language Options.
2. Specify a language in the Format and Location tabs.
3. On the Administrative tab, select the Change system locale button, and specify your current system locale.
4. Click OK.

The format, location, and system locale are set.

Error Message May Appear After Installing or Migrating on a Non-English Windows Computer

Valid on all non-English Windows computers

Symptom:

The installation or migration displays an error message such as "Can not find the install directory." When I click OK, the migration or configuration window does not appear.

Solution:

This error can display on non-English Windows computers during installation or migration. Open the C:\Windows\paradigm.ini file and update the CA Service Desk Manager installation directory in the NX_ROOT and NX_LOCAL variables, such as in the following example:

```
[PARADIGM]
NX_ROOT=C:/PROGRA~2/CA/SERVIC~1
NX_LOCAL=C:/PROGRA~2/CA/SERVIC~1
```

Spelling Errors Appear in Translated CMDB Data Values

Valid on Spanish, Italian, Japanese, Brazilian, Portuguese, Simplified Chinese language systems

Symptom:

After data is loaded into CMDB, unexpected spelling and grammatical errors appear in the translated values for class names, family names, and relationship types.

Solution:

In CA Service Desk Manager, the GRLoader utility provides a set of .rul files with the new translation values for CMDB. GRLoader .rul files appear by default in the following directory:

$NX_ROOT\java\lib\GRloader

If you moved the GRLoader .rul files to a different directory (or server) in a previous release, then modify the .rul files to reflect the new translation values.

CA Service Desk Manager provides the following new translation values for CMDB:

Object Type	English Strings	Language	Previous Translation Values	New Translation Values
class	Pager	Spanish	Localizador	Buscapersonas
class	Portfolio Asset	Spanish	Activo de cartera	Activo de la cartera
family	Cluster.Resource Group	Spanish	Clúster.grupo de recursos	Clúster.grupo de recursos
family	Cluster.Resource	Spanish	Clúster.recurso	Clúster.Recurso
relationship	is monitored by	Spanish	está controlado por	está monitorizado por
relationship	is served by	Spanish	está proporcionado por	está servido por
relationship	authors	Spanish	autores	es autor de
relationship	monitors	Spanish	controla	monitoriza
family	Facilities.Furnishings	Italian	Attrezzature.Mobili	Attrezzature.Mobilio
relationship	is governed by	Italian	è regolato da	dipende da
relationship	runs on	Italian	esegue su	viene eseguito su
relationship	is serviced by	Italian	è fornito da	è servito da

Object Type	English Strings	Language	Previous Translation Values	New Translation Values
relationship	is served by	Italian	è servito da	è assistito da
relationship	governs	Italian	regola	governa
relationship	is administered by	Japanese	管理される	処理される
relationship	administers	Japanese	管理する	処理する
class	Portfolio Idea	Brazilian Portuguese	Idéia do Portfolio	Ideia do Portfolio
family	Investment.Idea	Brazilian Portuguese	Investimento.Idéia	Investimento.Ideia
relationship	is administered by	Simplified Chinese	的管理方是	的控制者是
relationship	is governed by	Simplified Chinese	的管理方是	的治理方是
relationship	is regulated by	Simplified Chinese	的管理方是	的调整方是
relationship	administers	Simplified Chinese	管理	管控
relationship	governs	Simplified Chinese	管理	治理
relationship	serves	Simplified Chinese	服务	提供服务
relationship	regulates	Simplified Chinese	管理	调整

Note: All data values must be encoded using UTF-8 encoding.

Missing Exclamation and Colon Characters from the Final Installation Page

Valid on French, Brazilian, Portuguese, and German versions
Symptom:
The final installation page displays text that is missing a colon (:) or exclamation point (!).
Solution:
This behavior relates to a third-party software issue and does not affect the product functionality.

Japanese Version of Online Help Does Not Open in Internet Explorer

Valid on Japanese versions
Symptom:
When a Japanese Internet Explorer is used with the Japanese version of CA Service Desk Manager, the role-based Online Help does not display in the web interface as expected. This problem occurs for the following reasons:

- The order of statements in the SDHelp_index.htm file is incorrect.
- The Japanese IE browser defaults to the native JIS encoding instead of the Unicode (UTF-8) signature.

Solution:
To resolve this issue, update the SDHelp_index.htm file as follows:

1. Navigate to the SDHelp_index.htm file in the $NX_ROOT/bopcfg/www/wwwroot/help/web directory.
2. Create a backup copy of this file.
3. Create a new SDHelp_index.html file (named tmp.htm in this example) by running the pdm_uconv --add-signature -f utf8 -t utf8 -i SDHelp_index.htm -o tmp.htm command at the command prompt.
4. Replace the original SDHelp_index.htm with the new file.
   The SD_Help_index.htm file with the UTF-8 signature is updated.
5. Launch the web-based Online Help.

xMatter Integration is Supported on CA SDM English Language Only

Currently no solution exists.

CA Service Desk Manager Known Reporting Issues

This topic contains the following known issues:

Unable to Run the Crystal Reports

Symptom:

I integrated CA Business Intelligence Release 4.1 SP3 with CA SDM. Sometimes, I cannot launch the crystal reports (CA SDM reports) and the following error message is displayed:

The viewer could not process an event. Your request could not be completed because a failure occurred while the report was being processed. Please contact your system administrator. [RCIRAS0546]
---- Error code:0 [CRWEB00000119]

Solution:

Follow these steps:

1. Locate and find the following lines in the ivoa25.ini (32 bit Client ODBC) file located at C:\Program Files (x86)\CA\Service Desk Manager\add-ons\oaodbc72.

   Note: If CABI is installed on different machine from CA SDM find the file at C:\Program Files (x86)\CA\SC\CASD_ODBC.

   ```
   ;[WorkArounds]
   ;UnloadICUMessagesDLL=0
   ```

2. Remove the semicolon (;) from both the lines. For example,

   ```
   [WorkArounds]
   UnloadICUMessagesDLL=0
   ```

3. Save the file and test your report.

Symptom:

The following error occurs when the 64bit ODBC client did not install correctly when CABI was running and the DLL file was already in use.

Failed to open Connection and a driver architecture mismatch error on WEBI reports.

Solution II:

Follow these steps:

1. Stop the CABI server.
2. Close the Universe Design Tool.
3. Start the CABI server.
4. Execute the CABI configuration for SDM routine to install the 64 and 32bit ODBC drivers again.
5. Update the .ini file with the changes in Solution I (see page).

Unable to Generate Reports for the CIs that contain dot (.) in the CI names

Valid on MS SQL
The following reports (to find the relationship between the CIs) are not generated for the CIs containing dot (.) in the CI name:

- All Change Impact Report
- CIs Relationship Report
- CIs Root Cause Analysis Report
- Direct Change Impact Report

CA Business Intelligence Web Report Options

In Options Manager, the following options listed on the Web Reports List page are no longer relevant when configuring CA Business Intelligence to work with CA Service Desk Manager and can be safely ignored.

- bo_server_auth
- sec Enterprise
- secLDAP
- secWinAD
- secExternal

Progress OpenEdge DSN and ODBC Driver are Not Visible in ODBC Data Source Administrator

Valid on Windows 2008 R2
Symptom:
When configuring the OA server, I create a Project OpenEdge DSN named casd_servername. I use this DSN with pdm_isql and CA Business Intelligence. After I create the DSN, I cannot view it in the 64-bit ODBC Data Source Administrator.
I cannot edit the DSN or create a DSN using the ODBC Data Source Administrator. I am unable to point CA Business Intelligence to a different server. The 64-bit ODBC Data Source Administrator control panel does not show 32-bit drivers and configurations.
Solution:
Use the 32-bit ODBC Data Source Administrator to view the ODBC drivers by executing the %windir% \SysWOW64\odbcad32.exe file.

CA Service Desk Manager with CA Business Intelligence Upgrade

If you configured CA Service Desk Manager as a data source for CA Business Intelligence, shut down all CA Business Intelligence services before upgrading.

CA Business Intelligence ODBC Server Fails to Start on Non-Windows

For CA Business Intelligence reporting, if you experience problems with the startup of your ODBC server, uninstall, and then reinstall the ODBC server.

Follow these steps:

1. Export the library path as follows:
   - (For AIX) Export LIBPATH=$LIBPATH:<CA_SharedComponent>/lib:<NX_ROOT>/lib
     Example: Export LIBPATH=$LIBPATH:/opt/CA/SC/lib:/opt/CAisd/lib
1. - (For Solaris/Linux) Export LD_LIBRARARY_PATH=$ LD_LIBRARARY_PATH:/opt/CA/SC/lib:<NX_ROOT>/lib
     Example: Export LD_LIBRARARY_PATH=$ LD_LIBRARARY_PATH:/opt/CA/SC/lib:/opt/CAisd/lib
2. To uninstall the ODBC server, run the oa72_server_uninstall command from the command prompt.
3. To reinstall the ODBC server, run the oa72_server_setup command from the command prompt.

CA Business Intelligence ODBC Server Fails to Start on Windows

For CA Business Intelligence reporting, if you experience problems with the startup of your ODBC server, uninstall, and then reinstall the ODBC client and server.

Follow these steps:

1. To uninstall the ODBC client and server, run the following commands from the command prompt:
   - oa72_client_uninstall
   - oa72_server_uninstall
2. To reinstall the ODBC client and server, run the following commands from the command prompt
   - oa72_server_setup
   - oa72_client_setup

CA Business Intelligence Integration Fails after Upgrade

Symptom:

I upgraded CA Business Intelligence and downloaded the TrustedPrincipal.conf file from the Central Management Console. But the integration between CA SDM and CA Business Intelligence failed.

Solution:

After the CA Business Intelligence upgrade, copy the downloaded TrustedPrincipal.conf file at $NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd directory.

Report Details are not Displayed Correctly After Export to CSV

Symptom:
When I export reports to CSV, the data does not display correctly. For example, the header displays multiple times in the CSV without showing the appropriate content.

Solution:

Export the report in Excel format, which is available in Crystal Reports 2013 and save the file as a CSV.

Configure Business Intelligence Launch Pad Log On Page

Valid on Windows
Symptom:
The Business Intelligence Launch Pad Log On page is not configured to prompt users for their authentication type or CMS name.
Solution:

1. Copy the properties file from C:\Program Files (x86)\SAP BusinessObjects\tomcat\webapps\BOE\WEB-INF\config\default directory to C:\Program Files (x86)\SAP BusinessObjects\tomcat\webapps\BOE\WEB-INF\config\custom directory for modification.

2. Specify the default authentication types (secEnterprise, secLDAP, secWinAD, secSAPR3) here. For example, authentication.default=secEnterprise.

3. To prompt users for their CMS name, locate the cms.visible parameter and change its <param-value> from false to true. For example, <param-value>true</param-value>.

   Important! To ensure that your changes are preserved and not lost the next time the WAR files are deployed (typically during patch upgrades), follow SAP Note 1615492 (http://service.sap.com/sap/support/notes/1615492) and copy the custom files to the <BOE_HOME>\SAP BusinessObjects Enterprise XI 4.0 \warfiles\webapps\BOE\WEB-INF\config directory.

4. Save and close the file.

5. Restart Tomcat.

CA Service Desk Manager Known Security Issues

This articles contains the following known issues:

Antivirus Software Can Delay CA Service Desk Manager Startup

Valid on Windows
Symptom:
In some situations, antivirus software running on the same computer as CA Service Desk Manager can delay CA Service Desk Manager startup by 2 minutes or more. Typically, after a few minutes, the startup continues.
Symptoms include messages in the stdlog indicating a network connection cannot be made and CA Service Desk Manager appears suspended for several minutes.
If the delay occurs during migration, the migration can fail as the migration process times out waiting for services to start.

Solution:
Disable the antivirus software before you start CA Service Desk Manager. If the problem resolves, try configuring the antivirus software to relax restrictions on opening network ports, upgrade the antivirus software, and contact the vendor.
To complete migration, temporarily disable the antivirus software during the entire migration process.

LDAP Using TLS on a Windows AD Server Stalls or Fails

Valid on Windows
Symptom:
A Microsoft bug causes LDAP client applications that use more than one connection to stall or fail while using TLS encryption. When the server uses TLS encryption with LDAP groups enabled, CA Service Desk Manager can use a second connection in each LDAP Agent process. CA Service Desk Manager encounters one or more of the following symptoms:

- LDAP queries, synchronizations, or imports stall. A time-out can also occur with one or more ldap_agent.exe processes running continuously at or near 100 percent usage of one CPU core.
- LDAP queries, synchronizations, or imports fail with Server Down errors.
- LDAP queries, synchronizations, or imports return no errors and no results.

Solution:
If you use TLS encryption for LDAP, we do not recommend using LDAP groups with Windows Active Directory servers. You can either disable TLS or LDAP groups.
To disable TLS encryption or LDAP groups, do the following:

1. Terminate all ldap_agent.exe processes that are continuously using a large portion of CPU time
2. If you are unable to log in to CA Service Desk Manager to access the Options Manager, stop the CA Service Desk Manager service. In the $NX_ROOT/NX.env file, set one of the following options to No, and then stop and restart the CA Service Desk Manager service:
   - NX_LDAP_ENABLE_GROUPS (LDAP Groups)
   - NX_LDAP_ENABLE_TLS (TLS Encryption)
3. In Options Manager, disable either the ldap_enable_groups (LDAP Groups) option or the ldap_enable_tls (TLS Encryption) option.
4. If the CA Service Desk Manager service is running, stop the service.
5. Restart the CA Service Desk Manager service.

Automatic Login to Business Intelligence Launch Pad Fails

Valid on all operating systems with a CA Business Intelligence installation
Symptom:
During the CA Business Intelligence installation, a CA Technologies web cookie is installed by default that lets you automatically access Business Intelligence Launch Pad from the CA Service Desk Manager Reports tab without logging in. If access is restricted through your web browser privacy settings, the application fails to execute, and a login prompt appears on the Reports tab.
Solution:
If you encounter this issue, adjust your web browser Internet Options, Privacy settings so that CA Technologies web cookies are allowed on your system.

Warning Messages Appear When Generating Stub Classes

Valid on all operating systems
Symptom:
When using the AXIS tool WSDL2JAVA to compile stub files, warning messages appear.
Solution:
These warning messages are common when using AXIS 1.4 and cannot be avoided. The stub files are still created successfully.

Online Help Error Messages

Symptom:
Some context-sensitive online help pages produce a script error, although the online help topic displays correctly.

Solution:
The script errors can occur when script error notification is enabled in your browser. You can ignore these error messages, or you can disable script error notification on the Tools, Internet Options, Advanced tab.

CA Workflow Process Definitions Are Not Imported Automatically

Symptom:
The CA Workflow process definitions and actors are not imported automatically when starting CA Workflow due to incorrect locale variable settings on UNIX/Linux.
Solution:
After installing CA Workflow, use one of the following methods to resolve this issue:
To import CA Workflow process definitions and actors

1. Set the environment variables of LANG and LC_ALL to UTF-8 in a prompt for your operating system environment. For example, on Oracle Solaris the environment variable appears as: LANG=en_US.UTF-8.

2. Stop and then restart the CA Workflow Tomcat server as follows:

   - Run pdm_tomcat_nxd -d STOP -t CAWF.

   - Run pdm_tomcat_nxd -d START -t CAWF.
     The CA Workflow process definitions are imported.

To import the CA Workflow process definitions and actors manually

1. Use the IDE client to open CA Workflow.

2. Note: The IDE client is only available on Windows and Linux operating systems.

3. Locate the process definition and actor xml files, for example: $NX_ROOT/site/Workflow/data /actors and $NX_ROOT/site/Workflow/data/process directories.

4. Select File, Import, Process Definition, select all the XML files for import, and click Open.

5. Select all the definitions and click Import.
   The process definitions are imported.

6. Select File, Import, Actors, select all the XML files for import, and click Open.
   The actor xml files are imported.

7. Select all the actor files and click Import.
   The CA Workflow process definitions are imported.

CA Workflow IDE Login as User Other than Root Sets Incorrect URL

Valid on Linux

Symptom:

When a nonprivileged user launches CA Workflow IDE on Linux, the URL is set incorrectly to https://servername:8443/pm. Java errors appear on screen, and the login to CA Workflow is unsuccessful.

Solution:

1. Launch the CA Workflow IDE client.
2. Change the URL to: http://servername:8090/pm.
   Login is successful.

Duplicate Definition Messages

Symptom:

Because CMDB automatically creates the attributes and triggers for your customized extension tables, the stdlog can include the following harmless message for extension tables that were created in previous releases:

Ignoring duplicate definition

Solution:

To eliminate these messages, remove the following attributes from your custom extension tables:

- id SREL nr;
- version_number INTEGER { ON_CI INCREMENT 1; };
- creation_date DATE { ON_NEW SET NOW ; };
- creation_user STRING { UI_INFO "AUDITLOG"; ON_NEW DEFAULT USER ; } ;
- last_mod_dt last_update_date DATE { ON_NEW SET NOW ; ON_CI SET NOW; } ;
- last_mod_by last_update_user STRING { UI_INFO "AUDITLOG"; ON_NEW DEFAULT USER ; ON_CI SET USER ; } ;
- delete_flag del SREL actbool { ON_CI DEFAULT 0; };
- mdr_name LOCAL STRING;
- mdr_class LOCAL STRING;

Errors Occur When CA Wily Data is Loaded into CA CMDB

Symptom:

The GRLoader.log file produces errors when CA Wily data is loaded into CA CMDB as CIs.

The following is an example of the log entry:

```
11/07 00:44:52.662 ERROR grCI 504 Error trying to insert CI. Error setting at
```

Solution:

CA Wily integration includes an older version of GRLoader. Use the version of GRLoader that ships with CA Service Desk Manager to import the data successfully.

Multi-Tenancy and Visualizer

The Visualizer uses the Administrator role for impersonation purposes. A user with this role must have rights to see *ALL TENANTS*. If this user does not have ALL TENANTS rights, then Visualizer launch (stand-alone or in context) can fail.

Example: Visualizer Session Error

When Visualizer is launched in context for a CI, the following Visualizer session error appears:

Authentication failed for user

Symptom:

Tenant Access for the impersonation role is set to *Single Tenant*.

Solution:

To launch Visualizer in context without this error, set the Administrator role to *Tenant Access to All Tenants*.

Visualizer Relationship Performance

CMDB Visualizer can process approximately 2500 relationships on its graphical canvas. If a Visualizer request contains more than 2500 relationships, then Visualizer performance can degrade.

Set Browser Locale for Visualizer

CMDB Visualizer adapts itself to the client-browser locale, which can display a different language from your localized CA Service Desk Manager. To view the same language in Visualizer, set the browser locale to the CA Service Desk Manager language.

To set the browser locale in Internet Explorer

1. Select Tools, Internet Options, General tab, Languages.
2. Add the language you want and move it to the top.
3. Open the new IE browser window (or refresh the browser).

   Visualizer displays the language of the localized CA Service Desk Manager.

To set the browser locale in Firefox

1. Select Tools, Options, Content tab, Languages section.
2. Add the language you want and move it to the top.

3. Open the new Firefox browser window (or refresh the browser).

   Visualizer displays the language of the localized CA Service Desk Manager.

CA Service Desk Manager Known Miscellaneous Issues

This article contains the following known issues:

Upgrade to JRE 1.8 Causes PDM_CONFIGURE to Throw an Error

Valid on AIX

Symptom:

Running pdm_configure after upgrading CA SDM JRE to version 1.8 throws the following error in the AIX operating system:

```
"ERROR: xawt path is not a valid directory: [$XAWTPATH]"
"Please export proper JAVA_HOME/lib/ppc/xawt into LIBPATH"
```

Solution:

Follow these steps:

1. Take a backup copy of the $NX_ROOT/local/pdm_configure file.

2. Open the file $NX_ROOT/local/pdm_configure and search for the following information:

   ```
   echo "ERROR: xawt path is not a valid directory: [$XAWTPATH]"
   echo "Please export proper JAVA_HOME/lib/ppc/xawt into LIBPATH"
   exit 1
   ```

3. Comment those lines (Add # to start of each line).

4. Save the file and exit.

Auto Refresh Does not Work When an Existing Attachment or URL is Deleted or Detached From a Configuration Item

> **Note:** This known issue is only applicable for CA SDM Release 14.1.01

Valid on all browsers
Solution:
Manually refresh the Activities Tab of the Configuration Item to view the updated activities.

Values in Money Fields Truncated at Decimal Point

Valid on all operating environments
Symptom:
Including a decimal point in a money amount causes truncation of the value. This behavior applies to all fields intended to hold currency values, such as Purchase Amount and Maintenance Fee. For example, if you enter 265.50 in the Purchase Amount field, the value is saved as 265.
Solution:s
Although the name of some fields implies that they are money fields, they are implemented as integers. To avoid truncation, do not use a decimal point in integer fields.

pdm_ident command Returns an Empty Output

Valid on Linux
Running the pdm_ident command on any CA Service Desk Manager executable, returns an empty output.

Xlib Error Messages Appear While Uninstalling CA Service Desk Manager

Valid on Linux and UNIX
Symptom:
I am using third part remote management tool to uninstall CA Service Desk Manager. Xlib error messages appear during the uninstallation.
Solution:
CA Service Desk Manager will be uninstalled successfully, even though the error messages appear. To stop these error messages from coming, export DISPLAY variable and execute xhost + command before you begin the uninstallation.

Unsuccessful Failover on Standby Server

Valid on AIX
Symptom:
Both standby server and background server are installed on AIX. You want to perform failover and promote the standby server as the new background server. You used the pdm_server_control -b command on the standby server. You get the following error message:
This server is not a STANDBY server and cannot use the -b option.
Solution:
This issue occurs when you use XManager. Export CASHCOMP=/opt/CA/SC on Xmanger and try to run the command on the standby server again.

Pop-up Windows on CA Service Desk Manager web UI Shows Blank Page

Valid on Internet Explorer 10
Symptom:
You opened a pop-up window (for example, Create New Incident page) from the CA Service Desk Manager web UI. The page is blank or has only few control with blank sections. If you resize the window, then the contents appear properly.
Solution:

1. On your IE browser, go to Internet Options, Security, Local intranet.
2. Click Sites.
3. Add the CA Service Desk Manager URL to the intranet zone.
4. Close the browser and try to launch the CA Service Desk Manager web UI on a new IE browser.

Library Errors Occur When Running Command-Line Utilities

Valid on AIX, Linux, and Solaris
Symptom:
The following library errors similar to the following occur when I run command-line utilities:

```
ld.so (http://ld.so).1: pdm_pki: fatal: libetpki2.so (http://libetpki2.so): open failed:
No such file or directory
Killed
```

Solution:
Add the etpki library directory to your library path. The etpki library path is typically located at /opt /CA/SC/ETPKI/lib.

CA Spectrum Infrastructure Manager Integration with CA Service Desk Manager

Valid on all platforms
Symptom:
Integrating CA Spectrum Infrastructure Manager 9.2 (hotfix H03 applied) with CA Service Desk Manager produces the following issues:

- When an alarm is triggered through CA Spectrum, the associated service desk ticket is not automatically created in CA Service Desk Manager as expected. A solution has not been found.
- (Solaris only) When a user closes or transfers a service desk ticket in CA Service Desk Manager, the ticket is not propagated to CA Spectrum as expected.

Solution:
To resolve the ticket closure issue on Solaris, do the following:

1. Navigate to the $NX_ROOT/bin directory.
2. Open the OCNotify.jar file for editing.
3. Change the permission value to 777.
   The value is set.

4. Update a service desk ticket (Incident, for example) in CA Service Desk Manager.

5. Save your changes.
   The ticket is propagated to CA Spectrum.

SiteMinder Integration with CA Service Desk Manager

Symptom:
Single Sign-on (SSO) with the CA Service Desk Manager and SiteMinder integration is not working.
Solution:
Due to known issue with SiteMinder, SiteMinder is not able to send REMOTE_USER in HTTP Header which is required for default SSO for CA Service Desk Manager. Complete the following workaround steps to enable SSO until there is a fix from SiteMinder:

1. Set RemoteUserVar as REMOTE_USER under Agent Configuration in SiteMinder Policy Server.

2. Create a response with Attribute “WebAgent-HTTP-Header-Variable” and Variable Name as “REMOTE_USER” on SiteMinder.

3. Add @NX_ACCEPT_HTTP_REMOTE_USER=1 in the Service Desk Manager NX.env file.

4. Restart CA Service Desk Manager Services.

Exported Excel File Contains Errors and Does Not Open

Symptom:
When I click Export on a CA Service Desk Manager form, the exported Excel file displays XML PARSE ERROR and does not open correctly. I used the character 0xB (0013 base 8 and 11 base 10).
Solution:
The export utility does not support certain characters. According to the World Wide Web Consortium (W3C), XML does not permit all characters below 0x20, except 0x9, 0xA, and 0xD.

Wild Character Search Does Not Work for Federated Search

Symptom:
Wild character search such as %, ?, _, [], [^] does not work for Federated Search.
Solution:
CA Service Desk Manager wild character search is applicable only to EBR search.

CA Service Desk Manager Known Browser Issue

This section contains the following known issues:

IE 9 Browser Does not Support Multiple File Selection

Valid for IE 9 browser

Applicable for tickets, repositories, and knowledge.

Example:

1. Log in to CA Service Desk Manager with the administrator access type.
2. Open any existing ticket and try to attach multiple files using the Ctrl button.
   Unable to select multiple files using Ctrl button.

Solution:

Currently no solution exists.

Firefox Limitations in Knowledge Management

Valid on Windows and Linux
When using Firefox browsers, you can experience the following limitations in Knowledge Management:
Symptom:
From the Design Tab in the HTML Editor, you cannot delete previously saved text entered in the Resolution field of a knowledge document.
Solution:
You can delete previously saved text from the Source tab in the HTML Editor.
Symptom:
In Knowledge Management, a Firefox security setting can prevent you from using Cut, Copy, and Paste functions.
Solution:
To enable Cut, Copy, and Paste functions, modify your browser security preferences.

Note: For more information about configuring browser preferences, see mozilla.org (http://mozilla.org/).

Chrome Does Not Display Page Titles Correctly

Valid on Windows Server 2008
Symptom:
When I use Google Chrome, some title pages do not display correctly. For example, the detail_in. htmpl contains the title as untitled.
Solution:
Upgrade to the latest version of the browser.

Unable to Navigate to the Main Page of CA Service Desk Manager

Valid on Internet Explorer 9, 10, and 11.
Symptom:
I am unable to go back to the main page of CA Service Desk Manager when I click List All Windows from the menu driven option and then click Main Page.
Solution:
The problem occurs when you open multiple tabs on the Internet Explorer. You must close all the other tabs and then click Main page option. This behavior is a known issue in Internet Explorer 9, 10, and 11.

JAWS Does Not Read Header Associated with a Link on Read-Only Detail Forms

Symptom:
JAWS does not read the header associated with a link on a read-only detail form.
Solution:
Complete the following steps:

1. Open IE.
2. Press the Insert key + V to open the JAWS options.
3. Click Link Options, Text Link show Using - Screen text.
4. Press the spacebar until the option changes to Text Link Show Using - Title.
5. Close the options dialog.

Search-As-You-Type Works Differently for Japanese Language with Firefox

When Firefox is used with the Japanese version, the analyst must commit characters (such as exiting the IME process) to see matching results with Search-As-You-Type. Japanese characters in Firefox are not processed until the characters are released (no longer underlined or highlighted) by the Japanese Input Method Editor (IME).

Web Interface Renders Incorrectly in Internet Explorer

Valid on Windows
Symptom:
I experience any of the following problems:

- The web interface does not render correctly when I log in to the Analyst interface
- I cannot log on as a customer or employee.
- The guest login link is not on the page or the button is incorrect.
- Internet Explorer is using the Enhanced Security Configuration and the Internet zone does not allow you to run any script.

Solution:
Complete one of the following tasks:

- Create a custom security level in IE to enable most entries or add the server hostname to the Local Intranet zone.
- Log on as Administrator and disable the Enhanced Security Configuration in Internet Explorer.

Unable to Export Schedule on Internet Explorer

Valid on Windows
Symptom:
Exporting the Change Order Schedule does not function correctly when Enhanced Security is enabled in Internet Explorer (IE). The Enhanced Security option prevents IE from displaying the download prompt that the Export button creates for the user. The Enhanced Security option is only available on server installations of Windows.
Solution:
Disable the Enhanced Security option in IE.

Support Automation Clients Do Not Open on Chrome, Safari, or Firefox

Symptom:
When I open the Support Automation Analyst Interface or end-user client from Chrome, Safari, or Firefox, the Support Automation client opens in IE. The client only opens in IE, even if I set Chrome, Safari, or Firefox as the default browser. For example, you click on any link on the Support Automation Analyst Interface, such as an Incident. The Incident opens in Internet Explorer, instead of opening in Chrome, Safari, or Firefox. If I disable IE, the links do not work.
Solution:
No solution exists.

JavaScript Updates Cause Pages to Appear Incorrectly in Internet Explorer

Valid on Internet Explorer 9, 10, and 11.
Symptom:
I upgraded CA Service Desk Manager or modified CA Service Desk Manager by updating the JavaScript files. The updates do not display in the web interface correctly. JavaScript errors may also appear.
Solution:
A setting in Internet Explorer prevents the deletion of Temporary Internet Files from favorite sites and you must clear the browser cache.
Follow these steps:

1. Click Tools, Internet Options.
2. Click Delete in Delete Browsing History.
3. Disable the Preserve Favorites website data option and verify that the Temporary Internet files check box is selected.
4. Click Delete.
   The browser deletes the files.
5. Click OK on the Internet Options dialog.

CA Service Desk Manager Known Database Issues

This article contains the following known issues:

Oracle and CI Name Search

On Oracle 11g r1, if you search for an existing CI Name that is longer than 67 characters, the search fails. This problem does not occur on Oracle 11g r2.

Oracle RAC Failover

Few delay response pages are not converted to proper CA SDM pages during the failover of Oracle 11g r2 RAC Node. Errors are logged in the std log file.

For more information, see Deploy Oracle RAC with CA Service Management (see page 745).

Search Operations Do not Fetch any Results

Symptom:

I tried to perform search in CA Service Desk Manager based on data partitions. No search results are displayed and I get a DB error in the stdlog file.

Solution:

Upgrade your Oracle server version to release 11.2.0.3.0 and try again.

pdm_isql Utility is not Working on the Background Server

Symptom:

I logged in to the background server and executed the pdm_isql command. I am getting the following error message:

```
Unable to connect to the database.Since ODBC Services are not running on BG S
```

Solution:

The pdm_isql utility works only on the application server and you cannot run it on the background server.

Oracle 11g Release 1: Enable Case-Sensitive Search Capabilities within CA Service Desk Manager

Valid on all operating systems

Symptom:

When using CA Service Desk Manager with Oracle 11g Release 1, unexpected results can occur due to a case-sensitivity issue. For example, the following problems can occur:

- Documents can be associated with the wrong categories.
- Data partitioning may not work as intended.
- The Web UI may become unresponsive when a list of relationships is displayed.

Solution:

To *resolve* this issue, use Oracle 11g, Release 2. You can download Oracle 11g Release 2 from the Oracle Metalink Support page.

To *avoid* this issue, enable case-sensitive search capabilities within CA Service Desk Manager. In the NX.env file, set the NX_ORACLE_CASE_INSENSITIVE=variable to 0 instead of the default, 1, and restart services.

Note: For problem resolution, BUG ID No. 7335665 has been assigned to the Oracle development group.

CA Service Desk Manager Services Do Not Run After Configuration

Valid on Oracle on UNIX/Linux

Symptom:

After I complete the CA Service Desk Manager configuration, the CA Service Desk Manager services do not run by default.

Solution:

For configuring a 64-bit Oracle 11g database on a 64-bit computer, you *must* also install the Oracle 32-Bit Client on the server. Complete the following steps when you configure the database:

- The system library path (LD_LIBRARY_PATH on Oracle Solaris and Linux, and LIBPATH on AIX) must point to the 32-bit Oracle libraries.
- The ORACLE_HOME variable *must* point to the 32-bit Oracle libraries.
- The system PATH variable should include the 32-bit client bin folder: $ORACLE_HOME/bin.
- Create a net service name on the Oracle client to point to the Oracle database server instance. Use Administrator as the Oracle 32-bit client installation type.

Incorrect Search Results When Using Wildcards on Oracle

Valid on Oracle 11g R2

Symptom:

I use the underscore (_) and question mark (?) wildcards in a search and an incorrect number of results appear.

Solution:

Avoid using an underscore or question mark when you want the number of returned records to be accurate. These wildcards work on SQL Server searches.

SQL Server Limitation When Using Required Fields Which Do Not Allow Duplicate Values

SQL Server may not accept more than 900 bytes when you update the required fields which does not allow duplicate values. These fields can contain unique indexes and SQL Server has a known limitation. When you click Save, this limitation causes CA Service Desk Manager to display an error message such as the following example:

Operation failed. The index entry of length %d bytes for the index '%.*ls' exceeds the maximum length of %d bytes.

CA Service Desk Manager Known Documentation Issues

This article contains the following known issues:

Help On CA Service Catalog Options Opens the Online Help Home Page

Solution:

For more information about the CA Service Catalog options, navigate to Options Manager, CA Service Catalog from the Online Help Home Page or you can also see Options Manager (see page 1303) topic.

Help On This Window Option Does Not Work on the iPad

Valid on the Apple iPad

Some online help forms display the main CA SDM *Online Help* home page instead of specific topics. If this topic appears, use the search in the *Online Help* to find the appropriate content.

If the Help On This Window option does not work on the iPad, use the following actions:

- If you have an open help page and click Help On This Window on the other form, the new help form does not appear. Instead, the form updates to the already opened help form. The focus does not go to the help form and you have to click the form.
- If you open the help from another form, for example the Incident or Problem detail form, a prompt appears on the CA SDM home page. Click Accept from th home page to view the required help form.

Help on Server Configuration Wizard Shows Incomplete or Incorrect Information

- The following fields are not added in the help documentation of MS SQL Database Config wizard:
  - Database Admin User
  - Database Admin Password
- The following fields are stated as Read-only in the help documentation of Oracle Database Config wizard:
  - Data Tablespace Name
  - Index Tablespace Name
- Tablespace Path in DB server is written as Tablespace Path in the help documentation of Oracle Database Config wizard.

For correct information about these fields, see Server Configuration Utility (see page 869) topic.

Online Help Does Not Include the Documentation of Newly Introduced Options

The following options are not explained in the CA SDM online help:

- caextwf_retry_count
- caextwf_retry_interval
- force_browser_to_send_cookie_only_in_ssl_connection
- use_encrypted_sid_and_cookie
- max_files_to_upload_simultaneously
- xmatters_cr_attr
- xmatters_retry_count
- xmatters_retry_interval
- xmatters_url

For more information about these options, see the Options Manager (see page 1303) topic.

CA Service Desk Manager Known Sharepoint Issues

This article contains the following known issues:

Incident Modified Date is not Correct in the SharePoint 2010 Search Result

Valid on all operating systems

Symptom:

I created and modified an incident. Then I created the content source and crawler rule for CA Service Desk Manager. When I do Federated Search for the incident in SharePoint 2010, I find that the modified date of the incident is displaying the crawling time and not the modified date.

Solution:

There is no solution for this problem.

SharePoint 2010 does not Index PDF Files

Valid on all operating systems

Symptom:

When I perform the knowledge search through the Federated Search crawler, the PDF files that the crawler sends to the SharePoint 2010 does not get indexed.

Solution:

SharePoint 2010 does not have a PDF filter and cannot process the PDF files. So, you do not get the content of these PDF files in the search results. Install the fix that is mentioned in the KB_Article (http://support.microsoft.com/kb/2293357).

Total Search Count Varies When I Navigate Through Search Result Pages

Valid on all operating systems

Symptom:

I searched the knowledge database using the Federated Search mechanism (SharePoint 2010). As I navigated through the results pages, the total search count varies from one page to the other page. Though the total count must be consistent through out the pages.

Solution:

This is a known behavior in SharePoint 2010. For more information, use the following URL:

`http://social.technet.microsoft.com/Forums/sharepoint/en-US/10638572-9240-44f`

CA Service Desk Manager Known Migration Issues

This article contains the following known issues:

Errors are Displayed in the ITIL Content After the Migrating

Symptom:

I migrated from CA SDM Release 12.9. After the migration, the ITIL content schema files are missing and errors are displayed in the std log file.

Solution:

Install the ITIL Content for CA Service Desk Manager (see page 4819) to rectify this issue.

Migration Failure on Oracle 10g

Valid on Oracle 10g

Symptom:

The migration fails with the following error messages in the log file:

```
"STDERR: Error in dbcallback. event:4 err:15"
"STDERR: Error fetching data:15"
"ERROR: (54 of 54) Tables Failed Schema Validation!"
```

Solution:

Before starting the migration on Oracle 10g, verify that SQLPlus and Oracle DB are able to communicate. If communication fails, verify that Oracle is configured with the loopback adaptor using Oracle-supplied utilities and diagnostic techniques.

Migration Failure on SUSE 10 Machine

Valid on SUSE 10 machine

Symptom:

I click on Migrate to upgrade CA SDM. An error message is displayed.

Solution:

You are required to apply a patch to fix this problem. Contact CA Support Online (http://support.ca.com/) and find out the patch details.

Migration Does Not Back Up xlate Files

Symptom:

When you migrate from CA SDM r12.1, the GRLoader translation "xlate" files located in <nxroot>/java /lib/GRLoader are not backed up.

Solution:

If you made edits or created GRLoader translation "xlate" files located in <nxroot>/java/lib/GRLoader for any user-defined class, family, or relationship, back them up before migration.

Inactive Support Automation Users Set to Employee Access Type After Migration

Symptom:

Inactive Support Automation users, such as deleted Technicians, appear as Employees after migration.

Solution:

If you deleted users in CA Support Automation 6.0 SR1 eFix5, login and role associations were deleted, and the users were set to inactive. After migration, these inactive users have the Employee access type. You can delete these inactive users.

Data in Support Automation Reports Cannot Be Grouped by CA SDM Ticket Category After Migration

Symptom:

After I migrate Support Automation data, I cannot group or filter CA Business Intelligence reports by using the CA SDM ticket category. The Support Automation Assistance Sessions, Support Automation Assistance Sessions Metrics, and Support Automation Tool Usage Summary reports are impacted.

Solution:

The Support Automation migration script does not migrate relationships between Support Automation assistance sessions and CA SDM ticket categories. After migration, the Support Automation assistance session associates with the CA SDM ticket reference number. Additionally, you *must* manually associate the assistance session to the CA SDM ticket category.

Migration Does Not Remove WorldView Class Options

Symptom:

If the installation of a previous release of CA SDM included the Change Impact Analyzer integration, the WorldView context menu includes the ManageObject and UBMClass WorldView Class options.

Solution:

Because Change Impact Analyzer is deprecated in this release, delete theses menu options manually.

To delete the menu options

1. Start WorldView.
2. Right-click any object on the WorldView map and select Edit Class.

The Unicenter Class Wizard opens.

3. On the Class tab, select Modify Existing Class, and select the ManagedObject class.
4. On the Menu tab, select ManagedObject from the Menu Name drop-down list.
5. Scroll down in the middle field, select Impact Analyzer Sep, and click Delete.
6. Select Read Impact Analyzer in the middle field.
7. Click Delete.
8. Save and close the dialogs by clicking OK and Yes as appropriate.

   The ManagedObject class is removed from the WorldView context menu.
9. Repeat Steps 1 through 8 for the UBM Class and delete the same entries for the UBMClass Menu.

   The UBMClass is removed from the WorldView context menu.

Incorrect Path Causes Migration Failure on UNIX/Linux

Valid on UNIX/Linux

Symptom:

When I try to migrate from CA SDM r12.1 migration fails with missing file or directory errors in configure.log:

```
ERROR InstallTomcatTask.java 150 catalina.policy: /opt/CA/ServiceDesk/bopcfg/www
/CATALINA_BASE/conf: A file or directory in the path name does not exist.
ERROR InstallTomcatTask.java 150 context.xml: /opt/CA/ServiceDesk/bopcfg/www
/CATALINA_BASE/conf: A file or directory in the path name does not exist.
```

Solution:

The CATALINA_BASE path begins with the /opt/CA/ServiceDesk directory incorrectly. This path was replaced in CA SDM r12.5 with /opt/CA/ServiceDeskManager.

Execute the following command to fix the link to the required path:

```
ln -s /opt/CAisd /opt/CA/ServiceDesk
```

Tenant Cache Error Appears When Migrating from CA SDM r12.1

Symptom:

After I migrate from CA SDM r12.1 with multi-tenancy enabled, I try to create a Request/Incident /Issue and assign a tenanted user as a contact. When I tab out of the contact field, the following error message appears:

getCandidateTenants(cr:83274874,3986928649836438928346) failed - tenant cache is not correctly initialized

Solution:

Complete the following steps after you migrate:

1. Open web.cfg in the $NX_ROOT\bopcfg\www\ directory.
2. Go to the line that defines SelListCachePreload.
3. Add the following factory and attribute at the end of the line:

   ```
   tenant(name subtenant_group supertenant_group) tenant_group_member(tenai
   ```

4. Restart CA SDM services.

CA Service Desk Manager Known Upgrade Issues

This article contains the following known issues:

Modify Tomcat Delivered with Unicenter Service Desk r11.2

If you are upgrading from Unicenter Service Desk r11.2 and are using a version of Tomcat other than the default (4.1.31), follow these instructions before upgrading.

For Windows:

1. Modify the following line in the NX_ROOT\NX.env file to specify the path of the version you are using:

   ```
   @NX_TOMCAT_INSTALL_DIR= C:\Program Files\CA\SharedComponents\Tomcat\4.1.31
   ```

2. Modify the following lines in the NX_ROOT\site\config.properties file:

   ```
   web.tomcat_home= C:\Program Files\CA\SharedComponents\tomcat\4.1.31
   web.tomcat.service_name=Apache Tomcat 4.1
   web.tomcat.version=4.1.31
   ```

3. Install CA SDM.

Note: Any customizations made to the NX_ROOT\bopcfg\www\CATALINA_BASE\conf server.xml have to be manually updated to the server.xml (5.5.25) after configuration is run. An example would be SSL setup for Tomcat.

For UNIX:

1. Modify the following line in the NX_ROOT/NX.env file to specify the path of the version you are using:

```
@NX_TOMCAT_INSTALL_DIR=/opt/CA/SharedComponents/tomcat/4.1.31
```

2. Modify the following lines in the NX_ROOT/site/config.properties file:

```
web.tomcat_home=/opt/CA/SharedComponents/tomcat/4.1.31
web.tomcat.service_name=Apache Tomcat 4.1
web.tomcat.version=4.1.31
```

3. Install CA SDM.

Note: Any customizations made to the NX_ROOT/bopcfg/www/CATALINA_BASE/conf server.xml have to be manually updated to the server.xml (5.5.25) after configuration is run. An example would be SSL setup for Tomcat.

MDB Patch 17261861 Oracle for Windows

Symptom:

MDB patch 17261861 Oracle for Windows has an error that prevents an upgrade to MDB r1.5.

Solution:

MDB patch 17615776 includes the fix for this problem. Install patch 17615776 before upgrading to MDB r1.5 (CA CMDB r12.0 and CA CMDB r12.1 use this MDB version).

Note: CMDB-UAP Integration Patches RO2252 and RO02288 both include MDB patch 17261861 Oracle for Windows. If you have installed RO2252 or RO02288, and you are using an Oracle database, contact CA Technical Support for information about how to obtain the MDB patch and how to install it.

Upgrade Fails from Unicenter Service Desk, CA CMDB r11.2, and Visualizer

Valid in all languages

Symptom:

The following error message displays when you upgrade your Unicenter Service Desk, CA CMDB r11. 2, and Visualizer installations.

The environment variable CMDBVISUALIZER_HOME has been detected. This system appears to have CMDB Visualizer installed. This installation cannot continue. Cancel this installer. Remove CMDB Visualizer by 1) executing the Uninstaller separately; 2) Reboot the Operating System; 3) then run this installer again.

Solution:

Manually uninstall CA CMDB Visualizer before you perform the upgrade.

Live Assistance, Live Chat, and Join Analyst Now Links Are Missing

Symptom:

After upgrading from Unicenter Service Desk r11.2 with CA Support Automation r6.0 SR1 eFix5, the Support Automation Live Chat and Join Analyst Now links on the Employee page do not appear.

Solution:

After you upgrade CA SDM, remove the home.htmpl file from the NX_ROOT\site\mods\www\htmpl\web\employee\Employee directory so that the folder does not contain any files

Symptom:

After upgrading from Unicenter Service Desk r11.2, CA Service Desk r12, or r12.1 without CA Support Automation r6.0 SR1 eFix5, the following Support Automation options do not appear:

- The Live Assistance button on the Assigned Queue list page.
- The Live Chat and Join Analyst Now links on the Employee or Customer home pages.

Solution:

Support Automation uses the Analyst and End User default access levels. Because you upgraded from a CA SDM release that did not include Support Automation, assign the access level manually after upgrading.

CA SDM Upgrade Fails if the UTF-8 Locale is Not Installed

Valid on UNIX and Linux

Symptom:

The CA SDM upgrade fails when the UTF-8 locale is not installed before upgrading.

Solution:

CA SDM must run on the UTF-8 locale on UNIX and Linux operating systems. Before upgrading CA SDM, verify that you have installed the UTF-8 locale.

Printed Knowledge Documents Contain Large Spaces After Migration

Valid on all operating systems

Symptom:

Customers upgrading from Unicenter Service Desk r11.2 experience a printing problem for Knowledge Documents. Printed documents display a large space after the Resolution section when the documents contain embedded images.

Solution:

Complete the following steps:

1. On the Administration tab, navigate to Knowledge, Documents, Document Templates.
2. Open a Knowledge Document template.
3. Locate the <TD> tag in the HTML section and add the following code:

   ```
   <TD vAlign=top><SPAN class="clsTextBlackXXsmall"><SPAN>{TAG_RESOLUTION}
   ```

4. Repeat this change for all default Document Templates.

CA Service Desk Manager Known Configuration Issues

This article contains the following known issues:

pdm_configure Fails When MDB is Copied From Another Environment

Symptom:

1. Copied MDB from one machine to another machine and run pdm_configure.
2. During the configuration, entered the database information, and clicked Next.
   The following message is displayed.

   ```
   Database was previously configured by the server name of application server in
   the environment in which
   MDB was copied from.
   ```

3. Clicked OK and the dlgsrv table is automatically updated.
   The following message is displayed

   ```
   Already following servers are using the same database:<server name>. Make
   these servers as Inactive
   to proceed.
   ```

4. Clicked OK.
   pdm_configure fails to continue.

Solution:

To resolve this issue, add the @NX_SWING_BOX_MIGRATE variable. If this variable is set to Yes, the active server checks are ignored.

Note: For each CA SDM advanced availability server, manually add or update the NX variable in the $NX_ROOT/NX.env file and recycle CA SDM.

1. Run the following command from the command prompt on the primary server:

   ```
   pdm_options_mgr -c -s SWING_BOX_MIGRATE  -v Yes -a pdm_option.inst
   ```

2. Set the value of NX_SWING_BOX_MIGRATE to **No** after pdm_configure is successfully completed using the following command:

   ```
   pdm_options_mgr -c -s SWING_BOX_MIGRATE  -v No -a pdm_option.inst
   ```

3. To retain the changes made when you run pdm_configure, run the following command:

   ```
   pdm_options_mgr -c -s SWING_BOX_MIGRATE  -v No -a pdm_option.inst -t
   ```

Note: You may need to make additional changes to the database and/or CA SDM configuration to prevent duplicate notifications, and so on. For more information, see TEC578669 (https://support.ca.com/irj/portal/anonymous/kbtech?searchID=TEC578669&docid=578669&bypass=yes&fromscreen=kbresults).

Functionality Failures After Configuring the CA SDM Secondary Server with a Different Tomcat Port

Valid on all operating environments

Symptom:

I configured the CA SDM Secondary server with a different Tomcat port than the Primary server port. This configuration causes some functionality to fail when accessed from the Secondary server web URL. For example, GRLoader, and Process Viewer.

Solution:

Access the functionality from the primary server URL because they do not work on the secondary server. Use the –s parameter to specify host name and port number while running GRLoader from the secondary server.

Configuration Failure on 64-bit Oracle

Valid on 64-bit Oracle 11g R1 and 11g R2

Symptom:

The configuration fails and the following error messages appear on 64-bit Oracle:

- In the stdlog: "Unable to connect to Oracle database mdbadmin on server"
- In the checkdb.0 log: “Unable to load the OCI library or DLL. Cannot continue!”

Solution:

Install the latest 32-bit Oracle client, and do the following:

- On Windows, verify that the path includes the directory for the 32-bit Oracle libraries.
- On UNIX, set the library path variable so it points to the 32-bit Oracle library.

> **Note**: The problem can also occur when migrating from a previous release of CA SDM. If the error occurs during migration, install the client and run the migration.

bopauth_nxd Does not Run When Moved from Background Server

Symptom:

I have setup advanced availability configuration for the CA SDM environment. I logged in to the background server and navigated to Options Manager , Security from the Administration tab. I changed the bopauth_host value from default to point to an application server. I restarted all the CA SDM servers. bopauth_nxd is not running on the application server.

Solution:

When bopauth_nxd is moved from background server to any other server (such as the application server) complete the following steps:

1. Restart the background server after changing the default value of bopauth_host.
2. Start version control as a client on the application server using the following command:

   ```
   pdm_ver_nxd -c
   ```

3. Restart the application server.

Configuration Fails After CA SDM Installation

Valid on Windows 2008 SP2 and Windows 2008 R2

Symptom:

I logged in as an Administrator on Windows 2008 with enabled User Access Control (UAC) settings and installed the CA SDM application. When I try to configure CA SDM from the Start menu, the configuration fails either during the launch of the Configuration window or in the Database Configuration screen of the Configuration window.

Solution:

To configure CA SDM successfully, click Start, All Programs, CA, Service Desk Manager, then right-click Configure and select Run As Administrator.

Warning Message Appears When Implementing CA SDM

Valid on SuSE 11 only

Symptom:

During the CA SDM installation, configuration, or uninstallation procedures, the following warning message appears:

libxcb: WARNING! Program tries to unlock a connection without having acquired a lock first, which indicates a programming error. There will be no further warnings about this issue.

Solution:

Disregard the warning; it has no impact on the installation, configuration, or uninstallation procedures.

Error Messages Appear in pdm_tomcat_REST.log During REST Web Services Deployment

Symptom:

On rare occasions, the following error message may appear in the REST Tomcat logs (pdm_tomcat_REST.log) during REST Web Services application deployment.

```
SEVERE: Exception fixing docBase for context [/caisd-rest]
java.util.zip.ZipException: error in opening zip file
Feb 27, 2012 3:44:57 PM org.apache.catalina.core.StandardContext resourcesSta

SEVERE: Error starting static Resources
java.lang.IllegalArgumentException: Invalid or unreadable WAR file : error in

Feb 27, 2012 3:44:57 PM org.apache.catalina.core.StandardContext startInterna

SEVERE: Error in resourceStart()
Feb 27, 2012 3:44:57 PM org.apache.catalina.core.StandardContext startInterna

SEVERE: Error getConfigured
Feb 27, 2012 3:44:57 PM org.apache.catalina.core.StandardContext startInterna

SEVERE: Context [/caisd-rest] startup failed due to previous errors
Feb 27, 2012 3:45:07 PM org.apache.catalina.startup.HostConfig checkResources

INFO: Undeploying context [/caisd-rest]
```

Solution:

Sometimes the WAR file for the REST Web Services application is not accessible at the time Tomcat tries to deploy the application. You can ignore this error message because Tomcat fixes the error automatically. Tomcat retries the deployment which succeeds usually.

IPV6 Address Fails to Connect

Valid on all operating systems

Symptom:

A primary or secondary server is configured for either mixed mode or IPV6-only mode and the browser or standard logs show connection failure messages.

Solution:

Verify that the primary server, secondary server, or client can resolve the IPV6 address by name. Verify that the CA SDM address is a valid IPV6 address. For example, the IPV6 address is a routable IPV6 global address instead of an unrouted FE80 address.

To resolve IPV6 address connection issues on the servers or clients, do the following:

1. On the primary or secondary server, run the following CA SDM Java 1.7 command-line utility:

   ```
   java -cp $NX_ROOT/java/lib/checkprotocols.jar com.ca.ServicePlus.ipv6.t
   ```

   ```
   For example, to obtain IPV4 addresses for the Sd16 node, enter java –cp
   ```

   address/nodeSpecifies the named address/node name of the primary or secondary server (either local or remote).slump portSpecifies the TCP slump port number. For example, 2100. protocol(Optional) Specifies the IPV4 or IPV6 protocol. When you omit the protocol, the default supplies both IPV4 and IPV6 addresses.

   The utility lists information for the specified server node.

2. Use the data from the command line utility to verify that the routable CA SDM addresses are correct and are the same addresses that are on the DNS or name resolving servers entries.

3. If the addresses still do not resolve, specify the local and remote addresses for the CA SDM servers in one of the following files:

   - (Windows) <system drive>:\windows\system32\drivers\etc\hosts
   - (UNIX/Linux) /etc/hosts

   > **Note:** Use the server information from the command line utility to update the *hosts* file. Follow the instructions in the hosts file to add the CA SDM server node names.

4. If remote clients cannot connect to CA SDM, do one or more of the following:

   - Verify that the DNS name servers have the correct addresses.
   - Enter the IPV6 address directly into the browser.

PKI Login Fails with CA Workflow Configuration on AIX

Valid on IBM AIX

Symptom:

When I configure CA Workflow on AIX, the PKI login fails.

Solution:

After you install CA Workflow on AIX, you can configure CA Workflow for PKI login if necessary. IBM AIX requires additional security policy files for this login to work successfully.

Follow these steps:

1. Verify that you configured CA Workflow successfully.
2. Go to the IBM website and download the *Unrestricted Policy Files* (version 1.4.2 or later) from the Unrestricted JCE policy files page.

   Note: Register on the IBM website to download the policy files.

3. Replace the local_policy.jar and US_export_policy.jar files in your Shared Components JRE directory with the policy files that you downloaded from the IBM website.

   By default, these files are located in the /opt/CA/SC/JRE/1.7.0_04/lib/security directory.

4. Stop and start CA Workflow using the following commands:

```
pdm_tomcat_nxd -c STOP -t CAWF
pdm_tomcat_nxd -c START -t CAWF
```

LDAP Virtual Database Does not Run When Moved from Background Server

Symptom:

I have setup advanced availability configuration for the CA SDM environment. I logged in to the background server and navigated to Options Manager , Security from the Administration tab. I changed the ldap_virtdb_host value from default to point to an application server. I restarted all the CA SDM servers. LDAP Virtual Database is not running on the application server.

Solution:

When LDAP Virtual Database is moved from background server to any other server (such as the application server) complete the following steps:

1. Restart the background server after changing the default value of ldap_virtdb_host.
2. Start version control as a client on the application server using the pdm_ver_nxd -c command.
3. Restart the application server.

Uninstall CA SDM Manually

Symptom:

During uninstall, a message informs me to refer to the *Release Notes* for manual uninstall instructions.

Solution:

The installvariables.properties file is missing from the NX_ROOT/SDUninstall folder, however, the file is required to uninstall CA SDM. Perform the following procedures to resolve this problem.

To uninstall CA SDM manually on Windows operating environments

1. Shut down CA SDM.
2. Execute the following instructions:

   ```
   oa60_client_uninstall
   oa60_server_uninstall
   ```

3. Remove the file %WINDIR%\paradigm.ini.
4. Remove the CA SDM installation folder. For example, the default folder location is C:\Program Files\CA\Service Desk Manager.

   Important! Verify if both the ODBC services (CA SDM ODBC Data Access and CA SDM ODBC Agent) are removed or shut down before deleting the installation directory.

5. Remove the CA\Service Desk Manager folder from % ALLUSERSPROFILE%\ Start Menu\Programs.

   The product is uninstalled.

   Note: To uninstall the CA SDM Server service, run the instruction pdm_d_mgr -u.

To uninstall CA SDM manually on UNIX operating environments

1. Shut down CA SDM.
2. Remove the symbolic link /opt/CAisd.
3. Remove the CA SDM installation folder. For example, the default folder location is /opt/CA /ServiceDeskManager.

   The product is uninstalled.

CA CMDB Visualizer Fails to Start on Secondary Server

Valid on all operating systems

Symptom:

When CA CMDB Visualizer is configured on a secondary server, the following error message appears on the Visualizer login screen:

```
Loading application configuration data. Application is not ready to use. Plea
```

Solution:

Stop and then restart CA CMDB Visualizer tomcat on the secondary server as follows:

1. Run the following commands at the command prompt:
   - pdm_tomcat_nxd -d STOP -t VIZ
   - pdm_tomcat_nxd -d START -t VIZ
2. Log on to Visualizer.

   The Visualizer application opens.

CA Service Desk Manager Known Installation Issues

This article contains the following known issues:

Installation Issue in a non-Windows Environment

Valid on Non-Windows (RH Linux, AIX, and Solaris)

Symptom:

I cannot install CA Service Desk Manager in a non-Windows environment if root directory '/' has less than 10 GB.

Solution:

The CA Service Management installer checks the ‘/’ drive always for the required free space. When the disk space is less than 10 GB in the root directory, the installation fails because the threshold for the disk space is set to 10 GB in the installer.

Follow these steps to disable the disk-space validation:

1. Copy Non-windows DVD to a folder.
   For example, /DATA/CASM_DVD

2. Edit the common_config.properties under <DVD>/config/
   For example, the file is at DATA/CASM_DVD/config/common_config.properties path.

3. Set the following properties values to 0 to disable validation:

   - diskspace.sdm=0
   - diskspace.osop=0
   - diskspace.error.limit=0
   - diskspace.warning.limit=0

4. Save this config file and relaunch setup.

Supported Characters in Installation Path

Valid on operating systems with a CA Business Intelligence installation

Symptom:

The installation fails with an error regarding the characters specified in the installation path.

Solution:

The CA Business Intelligence installation supports only alphanumeric, spaces, dashes, and underline characters in the installation path. Modify the installation path to include these character types only.

Unable to Enter Credentials for the Privileged User During the CA SDM Installation

Valid on Non-Windows (RH Linux, AIX, and Solaris)

Solution:

Type the password on a notepad on your computer or any terminal, and then copy and paste it using the mouse.

Unable to Install or Configure CA SDM When the Install Directory Contains Spaces

Valid on UNIX/Linux

Symptom:

The install directory name contains spaces and you are unable to install or configure CA SDM properly on UNIX/Linux.

Solution:

Do not specify spaces in the installation media path and folder name.

CA EEM Installation Fails on Solaris or Linux

Valid on Solaris and Linux

Symptom:

The CA EEM installation fails with the following errors if you did not configure IPV6 correctly:

- CA iGateway installation failed
- Error message: Performing sanity test for system ip configuration for localhost: fail is displayed in igwinstall.log.

Solution:

Execute the following commands:

```
ifconfig lo0 inet6 plumb ifconfig lo0 inet6 up Add ::1 in /etc/hosts
```

CA Service Desk Installation Fails on a Pure IPV6 Environment

Symptom:

The **Installation Progress** screen reports an issue during **Integrating the Products** and an error message is displayed.

Solution:

1. Exit from the CA Service Management installer.
2. Open NX.env file from $NX_ROOT directory.
3. Ensure that the NX_PROTOCOL_ONLY variable is set to IPV6.
4. Restart CA SDM services.
5. Re-launch the CA Service Management installer.
6. On the **Select the required Installer** screen, select **Integrate pre-installed solution components** option (last in the list) and complete the installation.

CA Service Catalog

This section contains the following known issues:

CA Service Catalog Installation Known Issues

This section contains the following CA Service Catalog installation known issues:

Installation, Upgrade, and Migration Issues

After JRE1.8.0 is Upgraded, JRE Version is not Updated

Post JRE upgrade, while mentioning JRE version in the ANT upgrade-jre command, build failed error message is shown. This happens because the build.xml file is not getting updated with the correct JRE version after an upgrade is performed. To resolve this, you must locate the following lines in the build. xml file and manually change the JRE version to the upgraded JRE version:

```
<condition property="new.jre.is (http://new.jre.is).supported">
 <matches pattern="^(1.8.0_)([1][2-9]|[2-9][0-9])$" string="${new.jre.version}" />
 </condition>
```

Upgrade Requires Several Hours for Oracle

If you are using Oracle, the upgrade can require several hours. For example, the upgrade can run for five hours for all CA Service Catalog components.

Restart Computer After Migration

After migrating to CA Service Catalog from an earlier release, restart your computer and verify that all installed CA Service Catalog Windows services are started. The services are CA Service Accounting and CA Service Catalog.

Issue with Yearly Fiscal Periods After Migration

After migrating to CA Service Catalog from an earlier release, if you are using yearly fiscal periods, recreate them after migration. You do not need to recreate monthly fiscal periods after migration.

Actions Disabled After Upgrade

If an action whose type is JAVA, Command Line, or HTTP Post has a status of Disabled before you upgrade CA Service Catalog, the type of the action changes to Unknown during the upgrade. If you enable the action after the upgrade, CA Service Catalog prompts you to specify the type again.

Uninstall not Clean

When you uninstall CA Service Catalog, some folders and files can remain. For example, the USM_HOME\catalog folder can remain after you uninstall. Typically, the cause is that files in the USM_HOME folder were modified or new files were added.

To work around this issue, if any folders or files are left over after the uninstall, delete them manually.

Database Issues

Case Sensitivity for Searches

In CA Service Catalog, you can search for requests, users (including attributes), accounts, and other items. The case sensitivity of all searches in the product depends on the case sensitivity or collation settings in the database used for MDB, as follows:

- Microsoft SQL Server is typically set up using case-insensitive collation. Therefore, searches are typically case-insensitive.
- Oracle is typically set up using case-sensitive collation. Therefore, searches are typically case-sensitive.

If necessary, verify the case sensitivity settings for your database by testing or by consulting your database administrator.

Case Sensitivity for Assigning Actions to Groups

You can assign requests pending action to an CA EEM group that corresponds to a group with the same name in CA Process Automation. In such cases, the group names in CA EEM and CA Process Automation must match exactly, including case, if either of the following conditions exist:

- The CA EEM database is configured to use case-sensitive group names.
- The external directory (such as Active Directory) that populates the CA EEM database is configured to use case-sensitive group names.

Otherwise, the request is not assigned to the group.

Test the settings by requesting services and verifying that the requests pending action are assigned to the groups that you specified.

Content Pack Issues

Note: This issue is resolved in CA Service Management patch 14.1.01. Find the patch and the download details from CA Support Online.

Issue with Importing Content Packs when 'Business Unit ID' and ‘Business Unit Login ID’ are different

You cannot import content packs when the ‘Business Unit ID’ and ‘Business Unit Login ID’ are different.

To work around this issue, update the 'Business Unit Login ID’ with the value of ‘Business Unit ID’ and then import the content pack. When the import is completed, revert 'Business Unit Login ID' to its original value.

CA Service Catalog Localization Known Issues

This section contains the following CA Service Catalog Localization Known Issues:

Issue with Display of Units of a Cost Element in Localized UI

For all languages, CA Service Catalog displays the units that comprise a cost element using the following fixed sequence. This sequence is customary for English and other languages, but not for all languages.

<Billing Cycle> + <Charge Type> + “of” <Currency> +<Unit Cost>+<Display Unit Type>

Examples include the following cost elements:

- One Time Charge of $3 each
- Recurring Credit of €199 each
- Installment Charge totaling 10 x £199 for 10 items

System Alert Messages and Dashboard Builder not Localized

System alert messages always appear in English, even when CA Service Catalog is installed on non-English operating systems. System alert messages appear for individual requests when you view their request details. An example is selecting Home, Requests.

Similarly, certain text strings in the GUI elements and published content of the Dashboard Builder of CA Service Catalog always appear in English, even when CA Service Catalog is installed on non-English operating systems.

Double-byte Numerals not Supported

The numeric fields on localized operating systems support only single-byte numerals that are used on English-based operating systems.

CA Service Catalog Reporting and Form Designer Known Issues

This section contains the following known issues:

Values Missing from Reports

This issue applies only if you are integrating CA Service Catalog with CA Service Desk Manager and CMDB.

The predefined CA Business Intelligence report named Requests _Change Orders_CI Association does not display any value for the following columns:

- CI Resource Name
- CI Family Name
- CI Class Name

Cannot Drag and Drop Table Row in the Preview Pane

Note: This issue is resolved in CA Service Management patch 14.1.01. Find the patch and the download details from CA Support Online.

In the Forms Designer you cannot drag and drop the table row to the table in the Preview pane. To work around this issue, drag and drop the table row to the table in the Components pane.

CA Service Catalog Integration Known Issues

This section contains the following CA Service Catalog reporting known issues:

CA EEM Application Installation Fails

The CA EEM application installation may fail for one or more of the following reasons:

- The length of the application name is more than 50 characters.
- The application name contains a double quote (“), comma (,), forward slash (/), back slash (\), number sign (#), ampersand (&), or plus sign (+).

To work around this issue, correct the error, and try again to install the CA EEM application.

Issue with the Use of CA EEM Global Groups

This issue applies if both the following conditions exist:

- The user store is configured as External LDAP Directory.
- The Configuration Type is configured as Multiple Microsoft Active Directory.

To work around this issue and use CA EEM global groups with CA Service Catalog for permission control, use user-defined groups.

CA EEM Application Installation Fails

The CA EEM application installation may fail for one or more of the following reasons:

- The length of the application name is more than 50 characters.
- The application name contains a double quote (“), comma (,), forward slash (/), back slash (\), number sign (#), ampersand (&), or plus sign (+).

To work around this issue, correct the error, and try again to install the CA EEM application.

Issue with the Use of CA EEM Global Groups

This issue applies if both the following conditions exist:

- The user store is configured as External LDAP Directory.
- The Configuration Type is configured as Multiple Microsoft Active Directory.

To work around this issue and use CA EEM global groups with CA Service Catalog for permission control, use user-defined groups.

CA Process Automation action Disabled after Installation

Note: This issue is resolved in CA Service Management patch 14.1.01. Find the patch and the download details from CA Support Online.

If you are have integrated CA Service Catalog with CA Process Automation, the CA Process Automation actions for CA Service Catalog rules are enabled or disabled by default, as follows:

- The actions are disabled by default for CA Service Catalog upgrades
- The actions are enabled by default for new installations of CA Service Catalog.

However, even for new installations, the CA Process Automation action is disabled by default for the rule named *When Category is Software and Status is Pending Fulfillment*. Therefore, to use this action, enable it manually.

CA Service Catalog Request Processing Known Issues

This section contains the following CA Service Catalog Request Processing Known Issues:

- Issue with Suspension of a Subscribed Service (see page 211)

Issue with Suspension of a Subscribed Service

If you suspend a subscribed service, the suspension works properly as long as the Period Start Date for the suspension remains set to the default value. However, the suspension fails if the value for the Period Start Date field is changed to a non-default value.

Retrying Failed Actions Does Not Work

When an action fails while a request is being processed, the request can become stuck. Stuck requests cannot move to the next state of the request life cycle without manual intervention by you or another user. Stuck requests are marked with an alert status. By default, the alert is a yellow warning icon in the Status column of several request windows, including the Open Requests window.

If you are unable to retry the failed action successfully, override (push through) the alert to move the request to the next state.

Email Notifications not Sent

Note: This issue is resolved in CA Service Management patch 14.1.01. Find the patch and the download details from CA Support Online.

This issue applies if you have configured email notifications for requests. Requestors occasionally do not receive email notifications when their requests are assigned, approved, or rejected.

Notes and Attachments Deleted

Note: This issue is resolved in CA Service Management patch 14.1.01. Find the patch and the download details from CA Support Online.

This issue applies when both of the following conditions exist:

- A request includes two or more instances of the same service.
- The catalog user deletes one or more instances of the service after submitting the request.

In such cases, the Catalog system can inadvertently delete notes and attachments from the remaining instances of the service in the request.

To work around this issue, inform catalog users of this behavior and advise them to perform the following actions:

- Verify that these notes and attachments still exist in the remaining instances of the service.
- Create any notes and attachments again, if necessary, that were inadvertently deleted.

Oracle RAC Failover

During the failover of Oracle 11g r2 RAC nodes, error message is displayed instead of requests list on the CA Service Catalog requests page.

For more information, see Deploy Oracle RAC with CA Service Management (see page 745).

Browser Known Issues

This section contains the following known issues:

Batch Printing Fails with Mozilla Firefox

In Service Catalog Accounting component, batch printing can fail when you use the Mozilla Firefox web browser.

To work around this issue, use Microsoft Internet Explorer for batch printing.

Display Issue for CA Service Catalog Widgets on Safari

The CA Service Catalog Widgets are not displayed correctly in Unified Self-Service on the Apple Safari browser on an Apple iPad or an Apple desktop/laptop.

To work around this issue, go to the Privacy settings of the browser and set "Block Cookies" to "Never".

Display Issues for CA Service Catalog on Internet Explorer 10 and 11

CA Service Catalog is not displayed correctly on Internet Explorer 10 and 11, if the Security is Medium or High,

To work around this issue, follow these steps:

1. Open Internet Explorer.
2. Click **Internet Options, Privacy**, **Advanced**.
3. Check **Override automatic cookie handling** and **Always allow session cookies** options.

Display Issue for CA Service Catalog Widgets on Internet Explorer and Microsoft SharePoint 2010

The following issues occur for widgets, when users access them through Internet Explorer and when Microsoft SharePoint 2010 is the portal server:

- Catalog forms in requests do not render correctly in Internet Explorer.
  Microsoft SharePoint 2010 enforces XHTML standards and Internet Explorer complies with these standards. However, GXT does not support XHMTL and hence the forms are not rendered correctly in Internet Explorer.

- "Communication error" messages appear intermittently.

To work around this issue, access the widgets through Mozilla Firefox or Google Chrome when Microsoft SharePoint 2010 is the portal server. Else, use Microsoft SharePoint 2013 if your browser is Internet Explorer.

ActiveX Controls Do Not Run With Mozilla Firefox

In CA Service Catalog, objects that require Microsoft ActiveX controls do not appear when you use the Mozilla Firefox web browser, because of a limitation in Firefox. Examples include certain functions in the Dashboard Builder and the Report Builder.

To work around this issue, use the Microsoft Internet Explorer for actions that require ActiveX.

CA IT Asset Manager

This section contains the following known issues:

CA Asset Portfolio Management Installation Known Issues

The following known issues can affect how you install CA APM.

Restart the Server After Installation

Valid on all supported operating environments.

After you complete the product installation, restart each server on which you installed the product and the associated components. When you restart the servers, some of the services that the product requires to operate are started. However, you must manually start some services. You can then successfully log in to and use the product.

Note: For more information about the services the product uses, which services need to be started manually, and how to verify the installation, see Verify CA APM Installation (see page 317).

Installation of CA EEM Certificate Fails

Valid on all supported operating environments.

Symptom:

The CA EEM installation fails to create the authentication certificate.

Solution:
Complete the following steps:

1. Log in to the server on which you started the CA APM installation.
2. Use the following command to change from the current directory to the EEMSetup directory:

   ```
   CD "[ISO Root Path]\Setups\EEM
   ```

3. Use the following command.

   a. **For SQL:**

```
[ISO Root Path]\Setups\EEM\AppLauncher.exe -ProductName=EEM -
EEMParameter='-EEMBackend="[EEM Host]",-EEMAdminPass="[Eiamadmin
password]",-EEMUapmPassword="[uapmadmin password]",-EEMCasmPassword="
[casmadmin password]",-DatabaseType="SQL Server",-DBServer="[MDB
Hostname]",-UserID="sa",-DBName="[mdb name]",-Port="[mdb port number]",-
DBOwner="dbo",-DBPassword="[sa password]",-MdbAdminPassword="[mdbadmin
password]",-BundleVersion="14.1"'
```

When the command is finished, the command displays a log from the CA EEM SDK. You can safely ignore the log.

[EEM Host]
Server where CA EEM is installed.
APM
CA EEM application name. Do not change this value.
EiamAdmin
CA EEM superuser ID. Do not change this value.
[EiamAdmin Password]
CA EEM superuser password specified during the installation.
uapmadmin
Uapmadmin user password specified during the installation. If you changed the default uapmadmin password during the installation, use the same password when logging in to CA APM.

b. **For Oracle:**

```
[ISO Root Path]\Setups\EEM\AppLauncher.exe -ProductName=EEM -
EEMParameter='-EEMBackend="[EEM Host]",-EEMAdminPass="[EEMAdminPass]",-
EEMUapmPassword="[EEMUapmPassword]",-EEMCasmPassword="[casmadmin
password]",-DatabaseType="Oracle",-DBServer="[Server Name]",-UserID="
mdbadmin",-DBName="[Net Service Name]",-Port="[mdb port number]",-
DBOwner="mdbadmin",-InstanceName="[Oracle SID]",-DBPassword="[Sys
Password]",-MdbAdminPassword="[MdbAdminPassword]",-BundleVersion="
14.1.0.57"'
```

When the command is finished, the command displays a log from the CA EEM SDK. You can safely ignore the log.

[EEM Host]
Server where CA EEM is installed.
APM
CA EEM application name. Do not change this value.
EiamAdmin
CA EEM superuser ID. Do not change this value.
[EiamAdmin Password]
CA EEM superuser password specified during the installation.
uapmadmin
Uapmadmin user password specified during the installation. If you changed the default uapmadmin password during the installation, use the same password when logging in to CA APM.

4. Verify that the command has successfully processed by completing the following steps:

a. Log in to the MDB using mdbadmin as both the User ID and password.

b. Use the following query:
SELECT CERTIFICATE FROM AL_PROCESS_ACCOUNT

If you see BLOB value, the utility has successfully processed. Log in to CA APM using uapmadmin as the user ID and your uapmadmin password.

CA APM Does Not Work When Windows Encryption Is Applied

Valid on all supported operating environments.

Symptom:

When I encrypt the CA APM installation folder, the product does not work.

Solution:

The default CA APM application pools process using the Network Service account, which has minimal system privileges. To work in an IIS environment in which the CA APM installation folder is encrypted, the CA APM application pools must process under the Administrator account.

When the CA APM installation folder is encrypted, use the Administrator account to configure the application pool (ITAM application pool on Windows Server 2008).

Follow these steps:

1. Click Start, Run.
2. Enter the following command:
   `inetmgr`
   The Internet Information Services (IIS) Manager appears.
3. (Windows Server 2008) Complete the following steps:
   a. On the left, expand Application Pools, select ITAM, and select Advanced Settings.
   b. Navigate to the Process Model section of the dialog.
   c. In the Identity field, click the ellipses and select Custom Account.
   d. Enter the Administrator user name and password and click OK.
   e. Restart the application pool.

Component Installation Fails

Valid on all supported operating environments.

Symptom:

During the installation and configuration of the CA APM components, one or more component installations fail.

Solution:

When another process (for example, an antivirus product) is locking the files that are necessary for the product component installation, the component installation fails. In this situation, temporarily disable the product that is locking the files. Then, click Retry Install. The Installation Manager retries only the component installations that failed previously and displays the setup summary.

Installation of CA Client Automation Fails

Valid on all supported operating environments.

Symptom:

After I install CA APM, the CA Client Automation installation fails.

Solution:

The CA Client Automation installation fails when compatibility mode for the MDB is enabled.

Follow these steps:

1. Start the CA Client Automation installation.
   A wizard appears to install the CA Client Automation.

2. When prompted, do not enable compatibility mode for the MDB.

3. Continue with the CA Client Automation installation.

4. CA Client Automation is installed successfully.

Note: If enabling compatibility mode for the MDB is required, contact CA Support at http://ca.com/support.

Installation Fails with Insufficient Tablespace

Valid on Release 11.3.4 Oracle database environment.

Symptom:

The CA APM database installation fails on a Release 11.3.4 Oracle environment when the Data tablespace size is insufficient. Subsequent installation attempts on the same database also fail, even if you increase the tablespace size.

Solution:

Before you install CA APM, verify that the following recommended default tablespace sizes are set:

- Data tablespace = 400 MB
- Index tablespace = 100 MB

Upgrade to SQL Server 2008 Does not Update Compatibility Level when Attaching a Database

Valid on SQL Server database environments.

Symptom:

I upgraded from SQL Server 2000 to SQL Server 2008 by attaching the database, and the correct Compatibility Level was not set.

Solution:

The minimum supported version of SQL Server is SQL Server 2005. If you upgrade from a version before 2005 by attaching the database, update the Compatibility Level manually after the upgrade.

Execute the following command on the SQL Server 2008 database:

```
ALTER DATABASE mdb SET COMPATIBILITY_LEVEL = appropriate_compatibility_level
```

For information about this command, refer to the Microsoft Developer Network (MSDN) using the following steps:

1. Access the MSDN site at the following URL:
   http://msdn.microsoft.com

2. Search for the following article number:
   ms191137

3. Select the Database Compatibility Level Option article with the following version (for SQL Server 2008):
   v=SQL.105

Note: You can also upgrade from a lower version of SQL Server to SQL Server 2008 by backing up the lower version database and then restoring it on SQL Server 2008. With this method, there is no issue with the Compatibility Level.

Location of CA EEM Installer

Valid on all supported operating environments.

Symptom:

I need to locate the CA EEM installer on the CA APM installation media to install CA EEM Server 12.51.0.4.

Solution:

CA APM does not install CA EEM automatically. However, CA EEM is a prerequisite for the CA APM installation. If you have CA EEM installed already on an existing server, you can use the existing CA EEM. If you do not, install CA EEM before you install CA APM.

Follow these steps:

1. On the server where you are installing CA EEM, access the following location on the CA APM installation media:
   [ISO Root Path]\EEMSetup\

2. Execute the following:
   EEMServer_12.51.0.4_win32.exe

Apache Tomcat Log File Shows Unregistration Error

Valid on all supported operating environments.

The Apache Tomcat Common Asset Viewer service causes an error with Apache Tomcat version 6.0.24 or 6.0.26. This error is displayed in the Tomcat log file as an unregistration error. However, the error does not affect the functioning of the Apache Tomcat Common Asset Viewer, and corrective action is not required.

Business Objects and CASM Do Not Run on the Same Computer

Valid on all supported operating environments.

Symptom:

When you start the CASM service on a computer where CA APM and Business Objects Tomcat server are installed, the service starts and stops immediately.

Solution:

By default, Business Objects Tomcat Server and CASM Tomcat Server use the same shutdown port. To avoid this scenario, you must change the Tomcat Server shutdown port to another available port.

Follow these steps:

1. On the computer where CA APM is installed, navigate to one of the following folder locations, depending on your server:
   C:\Program Files\CA\SharedComponents\CASM\Tomcat\conf\ (for 32-bit operating system)
   C:\Program Files (x86)\CA\SharedComponents\CASM\Tomcat\conf\ (for 64-bit operating system)

2. Select and open the server.xml file.

3. Navigate to the following section:

   ```
   <Server port="8005"
   shutdown="SHUTDOWN">
   ```

4. Update the Server port with any available port number other than 8005.

5. Save and close the server.xml file.

6. Restart the CASM service.

CA APM Installation and the CA Business Intelligence Tomcat Port

Valid on all supported operating environments.

Symptom:

The installation assumes that the CA Business Intelligence Tomcat port is 8080. However, my environment uses port 8080 for CA Service Desk Manager and a different port for CA Business Intelligence. The installation wizard does not allow me to specify another port for CA Business Intelligence. Thus, the installation fails because the CA Business Intelligence connection is not available on port 8080.

Solution:

You can use the following workaround to resolve this issue.

Follow these steps:

1. Log in to the CA Business Intelligence server as the administrator.
   Note: If you have a product or service using Tomcat port 8080, stop that product or service first.

2. Open a command prompt window and execute the following command:

   ```
   netsh interface portproxy add v4tov4 listenport=8080 connectaddress=cabi_server
   connectport=cabi_tomcat_port
   ```

   Replace cabi_server with the hostname and cabi_tomcat_port with your CA Business Intelligence Tomcat port number.
   This command creates a port proxy on the CA Business Intelligence server that forwards all traffic for port 8080 to your CA Business Intelligence Tomcat port.

3. Complete the installation.

4. Log in to CA APM.

5. Navigate to Administration, System Configuration, Web Server.

6. Change the Reporting Server Port from 8080 to your CA Business Intelligence Tomcat port number.

7. Restart Internet Information Services (IIS) by performing the following steps:

   a. On the CA APM web servers and application servers, open a command prompt window.

   b. Execute the following command:

      ```
      iisreset
      ```

8. Execute the following command on the CA Business Intelligence server:

```
netsh interface portproxy del v4tov4 8080
```

This command removes the port proxy that you used during installation.

Note: If you previously stopped a product or service using Tomcat port 8080, restart that product or service now.

Changing the CA EEM Server after Installing CA APM

Valid on all supported operating environments.

Symptom:

I finished installing CA APM, and I now want to change the CA EEM server.

Solution:

Use the following procedure to change the CA EEM server. For more information, see Integrate CA Asset Portfolio Management with CA EEM Manually (see page 3481).

CA EEM Integration Error While Installing CA APM

Valid on all supported operating environments.

Symptom:

While I install CA APM, the installation process fails with a CA EEM integration error while configuring CA APM.

Solution:

You can ignore the error message.

On the error dialogue box, click Ok. Then click Retry Install. The installation completes successfully.

CA Asset Portfolio Management Starting Known Issues

The following known issues can affect how you start CA APM.

- Tenancy Management Page Cannot Be Displayed Browser Error Appears (see page 221)
- Tenancy Management Page Does not Display with Google Chrome Browser (see page 222)
- Change the Web Site Port (see page 222)
- CA APM Home Page Links Do Not Work (see page 224)
- Login Fails with Service Model Activation Error (see page 225)

Tenancy Management Page Cannot Be Displayed Browser Error Appears

Valid on all supported operating environments.

Symptom:

The following browser error message appears when I click Administration, Tenancy Management:

Page cannot be displayed.

Solution:

When CA APM, including Tenancy Management, is accessed from a network that is outside of the computer on which you installed CA APM, the URL for Tenancy Management (the CASM service) becomes inaccessible. The URL for CASM cannot be accessed because the URL that is stored in the CA MDB uses an internal host name for the computer on which CASM is installed.

Follow these steps:

1. Log in and connect to the CA MDB database as the user who owns the MDB database (mdbadmin).

2. Execute the following script on the CA MDB database:

   ```
   UPDATE CA_APPLICATION_REGISTRATION
   SET product_specific_data='http://[EXTERNALHOSTNAME]:[CASMPORT]/
   itam/itam.html' WHERE product_code=2070
   ```

   The following fields require explanation:
   [EXTERNALHOSTNAME]
   Public host name or public IP of the computer on which the CASM service is installed, which can be accessed from an outside network.
   [CASMPORT]
   Port number on which the CASM service operates. The default port number is 9060. You can obtain this value by reviewing the existing CASM URL.

3. Restart the web server.
   The updated URL to access Tenancy Management (the CASM service) is accessible.

Tenancy Management Page Does not Display with Google Chrome Browser

Valid on all supported operating environments with Google Chrome browser.

The following browser error message appears when you try to access the CA APM Administration, Tenancy Management page using the Google Chrome browser.

Page cannot be displayed.

The Common Administration for Service Management (CA CASM) component provides multi-tenancy administration for CA APM. CA CASM does not support the Google Chrome browser. If you plan to perform Tenancy Management in CA APM, use a browser other than Google Chrome.

Change the Web Site Port

Valid on all supported operating environments.

Symptom:

As the administrator, I cannot use the default CA APM web site port number because another application in my environment is using that number.

Solution:

The default product web site port number is 80. You can change this default number to use a different number.

Follow these steps:

1. From the Start menu, select Run.
2. Enter inetmgr in the Run dialog.
   The Internet Information Services dialog opens.
3. Select the user-provided web site name on the Connections pane.
4. Click Bindings in the Actions pane.
   The Site Bindings dialog appears.
5. Click Add.
   The Add Site Binding dialog opens.
6. Enter the new port number for http and click OK.
7. Click Close on the Site Bindings dialog.
8. (Single Server Installation) Update the web site port number.
   Follow these steps:
   a. Log in to CA APM.
   b. Navigate to Administration, System Configuration, Application Server.
   c. Change the Server Port and the Component Server Port to the new values.
   d. Log in to the product database as the administrator.
   e. Execute the following command:

      ```
      Update al_cdb_configurationparameters set configvalue=New Port where
      configKey='ServerPort' and componentkey='Web_Server' and machineName='WEB
      SERVER NAME'
      ```

      Replace New Port with the new port value.
      Replace WEB SERVER NAME with the name of the web server in all upper case.
9. (Multiple Server Installation) Update the web site port number.

   Follow these steps to change the web site port for the web server (if required):

   a. Log in to the product database as the administrator.
   b. Execute the following command:

```
Update al_cdb_configurationparameters set configvalue=New Port where
configKey='ServerPort' and componentkey='Web_Server' and machineName='WEB
SERVER NAME'
```

c. Replace New Port with the new port value.

d. Replace WEB SERVER NAME with the name of the web server in all upper case.

Follow these steps to change the web site port for the application server (if required):

a. Log in to CA APM.

b. Navigate to Administration, System Configuration, Application Server.

c. Change the Server Port and the Component Server Port to the new values.

10. Notify product users that they need to update the port number in the CA APM browser URL address. Users need to perform this update each time that they access CA APM from the Start menu shortcut.
The following URL shows the default CA APM browser URL address:
http://localhost/ITAM/Pages/UserLogin.aspx
Users need to change this URL to the following URL address:
http://localhost:port/ITAM/Pages/UserLogin.aspx (http://localhostport)
Replace port with the new web site port number.

CA APM Home Page Links Do Not Work

Valid on all supported operating environments.

Symptom:

When I log in to the CA APM home page, none of the links on the page works. I receive the following error message:

Error: (System.InvalidOperationException: Unable to generate a temporary class

Solution:

Correct this problem by following the instructions from Microsoft.

Follow these steps:

1. Open a browser and navigate to http://support.microsoft.com.
2. In the Search field, enter 908158.
3. In the results list, select the article with the following title:
Error message when ASP.NET 2.0 is configured to run with a user account: "Unable to generate a temporary class".
4. Follow the instructions in the article.

Login Fails with Service Model Activation Error

Valid on all supported operating environments.

Symptom:

After I upgrade from a previous release to release 14.1, I receive the following error message when I try to log in to the product:

Could not load type System.ServiceModel.Activation.HttpModule

This message indicates an error with the ASP.NET registration with Internet Information Services (IIS).

Solution:

Follow these steps:

1. From the Start menu, open a command prompt.
2. Navigate to the appropriate Microsoft.NET framework folder. The following folders are examples:
   C:\Windows\Microsoft.Net\Framework64\v4.0.30319
   C:\Windows\Microsoft.Net\Framework\v4.0.30319
3. Run the following command:

   ```
   aspnet_regiis.exe -iru
   ```
4. Restart IIS by running the following command:

   ```
   iisreset
   ```

CA Asset Portfolio Management Configuration Known Issues

The following known issues can affect how you configure CA APM.

Adding Costs to Multiple Assets Fails on Oracle 12c Database

Symptom:

On an Oracle 12c database, I cannot add costs to multiple assets at the same time using the **Add Asset Cost** mass change utility or the data importer.

Workaround:

Update the cost record of each asset separately.

Configuration Changes and User Roles

Valid on all supported operating environments.

When you make configuration changes such as defining a configuration, defining an extended field, defining a hierarchy, granting security, and so forth, and then add user roles or assign a configuration to a role, verify that you shut down IIS on all but one application server in your web farm before you start configuration mode again. Complete your configurations, and then start the IIS instance on the remaining application servers in your web farm. You can then continue using the product.

Inactive Items Available When Defining Objects

Note: This issue is resolved in CA Service Management patch 14.1.01. Find the patch and the download details from CA Support Online.

Valid on all supported operating environments.

When you define an item and make it inactive, the item still appears and can be selected when defining an object.

Default Reference Field Searches Include Inactive Items

Note: This issue is resolved in CA Service Management patch 14.1.01. Find the patch and the download details from CA Support Online.

Valid on all supported operating environments.

Symptom:

When defining an object, you can use a reference field search to select a related object (for example, to select the model for an asset). The default reference field search results include both active and inactive records, and the search dialog does not indicate which records are inactive.

Solution:

When you use a reference field search to select an object, first change the Inactive drop-down list to No and click Go, so that only active records appear in the search results. You can then select an active record for the object.

Renaming Configurations

> **Note:** This issue is resolved in CA Service Management patch 14.1.01. Find the patch and the download details from CA Support Online.

Valid on all supported operating environments.

After you save a global or local configuration, you cannot rename it. Delete the configuration and add it again with the new name. When you delete a configuration, all configuration changes that you saved, such as hiding fields and buttons, moving fields, and defining extensions, are deleted.

Common Administration for Service Management (CASM) and Multi-Tenancy

Valid on all supported operating environments.

Symptom:

When CA APM is configured to support the Secure Socket Layer (SSL) protocol and the Common Administration for Service Management (CASM) is not configured to support SSL, you receive a message similar to the following when you click Administration, Tenancy Management:
You do not have required privileges to perform the action.

Solution:

Complete the following steps to configure CASM to support the SSL protocol:

1. Configure CASM to support the SSL protocol.
   Note: For more information about configuring CASM to support the SSL protocol, see the CASM documentation.

2. Complete the following steps on the CA APM database:

   a. Log in to the CA APM database using a client interface.

   b. Execute the following SQL statement:

```
UPDATE CA_APPLICATION_REGISTRATION SET PRODUCT_SPECIFIC_DATA = 'https://<
hostname>:<ssl-port>/itam/itam.html' WHERE PRODUCT_CODE = 2070;
```

3. Restart the IIS server on the CA APM web server.
   You can use CA APM with CASM with both products using SSL, and you can use CA APM with CASM with both products using non-SSL.

Hierarchy List Management

Note: This issue is resolved in CA Service Management patch 14.1.01. Find the patch and the download details from CA Support Online.

Valid on all supported operating environments.

You can define a multiple level hierarchy that begins with a new field, and then navigate to List Management to define the items that appear in the hierarchy fields. For any level in the hierarchy, a row of blank list items, and duplicate rows (that is, rows with identical values in all items) can be successfully saved. The product should not save the rows and should provide an appropriate message.

Adding Extended Fields and Existing Fields

Valid on all supported operating environments.

Symptom:

When I configure the user interface, the Add Extension and Add Existing Fields hyperlinks do not appear.

Solution:

The Add Extension and Add Existing Fields hyperlinks are only available for a global configuration. After you add an extended or existing field, the field is available to all users in both global and local configurations. If the field should not be available to users in a local configuration, update the local configuration and remove the field.

Tenant Drop-Down List Does Not Appear

Valid on all supported operating environments.

Symptom:

After I enable multi-tenancy, a tenant drop-down list does not appear when entering information for objects and when generating reports.

Solution:

Restart Internet Information Services (IIS) on the CA APM web server using the iisreset command.

Contacts and Locations Do Not Appear

Valid on all supported operating environments.

Symptom:

After I define a contact or location using Administration, Tenancy Management, the contact or location is not available when entering information for objects.

Solution:

Restart Internet Information Services (IIS) on the CA APM web server using the iisreset command.

Adding Existing Fields for Software Assets

Valid on all supported operating environments.

In an integrated environment with CA Software Compliance Manager, you can configure the user interface and add an existing field for a software asset. When adding existing fields to either the Basic or Additional parts of the page, the product displays. You can select to add the Software License or SwCM License fields. When adding an existing field to the Basic or Additional parts of the page, do not select the SwCM License fields. However, you can add the Software License fields to any part of the page (License, Basic and Additional parts).

Database IDs are Required for Reference Field Event Definition

Valid on all supported operating environments.

When you define an event for a reference field on the Events page, you can select Old Value for the Value Changed From drop-down list and New Value for the Value Changed To drop-down list. When you make these selections, you can then specify the values in the Value fields. The values that you specify must be in the form of database IDs or UUIDs, not text entries. Locate the IDs or UUIDs in the database and enter the information in the appropriate Value fields on the Events page.

Note: For more information about defining an event, see Events and Notifications (see page 2376). For more information about reference fields, see Reference Field Configuration (see page 1551).

Family Field

Valid on all supported operating environments.

When defining a configuration for an asset, model, and legal document, the Family field appears. The Family field is different from the Asset Family field. The Asset Family field (previously named Asset Type) is used to organize and classify assets to track specialized information about products, services, or equipment used in your organization. The Asset Family field determines the information that you see on the page when you define an asset.

In contrast, the Family field is a simple indicator for the attribute to classify the current primary object. For example, Asset Family appears by default in the Family field for assets and models, and Legal Template appears by default in the Family field for legal documents. You define the configuration for the asset, model, and legal document based on the value in the Family field.

Restricting Users from Creating and Assigning Global Configurations

Valid on all supported operating environments.

Symptom:

I created a role for members of my team and assigned each user to the role. I did not assign a local or global configuration to the new role. A user in this role created a configuration and assigned the configuration globally to all users, even when I did not grant any security permissions to the user or role.

Solution:

When you do not assign a local or global configuration to a role, all users in the role are assigned the default permissions from global configurations. Global configurations are intended for administrators only. To restrict users from creating and assigning global configurations, complete the following steps:

1. Create local configurations and limit the security permissions based on your requirements.
   Important! To restrict a user from performing any configuration and not allow the user to create a configuration, create a local configuration and deny all configuration permissions for all objects. To deny all configuration permissions, deny a user the ability to define an extension, manage events, change a field label, move a field, make a field required, hide a field, and secure objects.

2. Save the local configurations.

3. Create roles and assign the local configurations to the roles.
   Each user in the roles cannot create and assign global configurations.

Defining a Hierarchy for a Software Model

Valid on all supported operating environments.

Symptom:

I defined a global configuration for a software model and selected to define a hierarchy. When defining the hierarchy levels, I selected the existing Capacity Units field as the top-level field for the hierarchy, completed the wizard, and saved the hierarchy. I then defined the list items for the hierarchy. After defining the hierarchy and the list items, I cannot search and select the hierarchy values when defining a software model.

Solution:

When defining a software model, the Capacity Units field is not available. Therefore, do not select the Capacity Units field as the top-level field in the hierarchy levels when defining a hierarchy for a software model.

Incorrect Data Appears for Hierarchy Fields

Valid on all supported operating environments.

Symptom:

At the end of the wizard to define a hierarchy that is based on an existing field, I clicked Save and New, canceled the wizard, and saved the global configuration. The hierarchy fields are not added to the global configuration and the hierarchy fields do not appear on the page. However, I can add values for the hierarchy fields using List Management. How can I add the hierarchy fields to the global configuration that I previously saved?

Solution:

To add the hierarchy fields to the global configuration, select the global configuration and click Add Existing Fields. In the wizard, select the same part of the page to add the hierarchy fields that you selected when you defined the hierarchy. If you select a different part of the page for the hierarchy fields, the data represented by the hierarchy fields does not match the values you specified using List Management. You can also define a new hierarchy.

Audit History and Extended Fields

Valid on all supported operating environments.

Symptom:

I defined an extended field for an object with a specific subtype (for example, an asset has a subtype of hardware). When a user defines an object with the subtype and views the audit history, the extended field that I added does not appear.

Solution:

Extended fields that are added for a subtype are not available in the default audit history for object records having the same subtype. To see the extended fields for the subtype, define a new audit history search that includes the missing extended fields for the specific subtype.

Removed Relationships

Valid on all supported operating environments.

The following relationships will be removed and will not be supported. We recommend that you do not use these relationships.

Object	Removed Relationship
Model	▪ Dependencies ▪ Product Evolution
Asset	▪ Budget Managers ▪ Product Upgrades ▪ Support Contacts ▪ User Allocations ▪ Contacts User

Object Relationships

Valid on all supported operating environments.

For the company allocation, contact allocation, location allocation, and legal asset relationships, you can see the relationship when you view both objects. For example, you can have a legal asset relationship between an asset and a legal document. When you view the asset, you can see the relationship to the legal document. When you view the legal document, you can see the relationship to the asset. For all other relationships, you can only see the relationship from the parent object. For example, when you view an asset, you can see the relationship to the image partitions. However, when you view the image partitions, you cannot see the relationship to the asset.

Audit History Displays Extended Field IDs Instead of Names

Valid on all supported operating environments.

You can define an extended field to help ensure that you capture all data in your repository that is critical to your asset management program. For example, define a reference field extension for an asset named Chipset so that users can enter and manage the chipset information (for example, Intel 5520). When a user views the audit history for an object, the internal field ID appears for the reference field extension (for example, 1000000) instead of the name (for example, Chipset). The product should display the extended field name instead of the internal field ID.

User Receives an Error when the Administrator Changes the Configuration

Valid on all supported operating environments.

Symptom:

If an administrator changes or deletes an object configuration while a user who is assigned to that configuration is creating an object, the user receives an error.

Solution:

The user can refresh the current page and continue working. The administrator can also plan to make configuration changes when users are not working.

Assets Allocated Page does not Display Assets Allocated to a Contact

Valid on all supported operating environments.

Symptom:

The Assets Allocated page does not display assets allocated to a contact in the following scenario:

In CA SDM you create a Model without a Family or Class and then assign the model and a primary contact to a new CI. When you access the assets allocated to the primary contact in CA APM, the page does not list the CI you created in CA SDM.

Solution:

CA APM displays the assets allocated to a contact only when the asset's family/class are the same as the model's family/class. Ensure that the model's family/class and the asset's family/class are the same.

CA Asset Portfolio Management Security Known Issues

The following known issues can affect how you secure CA APM.

- Deleted Users and Roles Can Access the Product (see page 233)
- Common Home Page Links Prompt for Credentials (see page 233)

Deleted Users and Roles Can Access the Product

Note: This issue is resolved in CA Service Management patch 14.1.01. Find the patch and the download details from CA Support Online

Valid on all supported operating environments.

When I delete a user or role, the deleted user, or the users in the deleted role, may be logged in to the product in another session. In this situation, the deleted user, or users in the deleted role, can still access the product until the session expires. When a user or role is deleted, the product should shut down the session for the user and not allow the user to access the product.

Common Home Page Links Prompt for Credentials

Valid on all supported operating environments.

Symptom:

The Common Home Page provides a single web-based home page for accessing the functions in both CA APM and CA SAM, including CA Business Intelligence reporting. However, when I click the links for CA SAM and CA Business Intelligence, I am asked to provide authentication credentials.

Solution:

You can eliminate the authentication prompts by configuring CA SAM and CA Business Intelligence.

Follow these steps:

1. (CA SAM) Configure CA SAM to Token authentication.
   Note: For more information, see the CA Software Asset Manager Administration Manual.

2. (CA Business Intelligence) Configure the CA Business Intelligence Windows Active Directory for either Kerberos or CA SiteMinder.

Note: Release 14.1 does not support CA Business Intelligence Trusted Authentication with CA APM.

CA Asset Portfolio Management Import Known Issues

The following known issues can affect how you import data into CA APM.

- Error When Trying to Import a Large Number of Users (see page 234)
- Error When Trying to Import Large number of Users from CA EEM Integrated with CA SiteMinder (see page 234)

Error When Trying to Import a Large Number of Users

Valid on all supported operating environments.

Symptom:

When importing and synchronizing users from an active directory or another CA EEM source such as an LDAP server, and the import list contains over 30 thousand users with the name beginning with the same letter, you receive the following message:

EE_POZERROR Repository Error. Problem with EEM connected Repository. Please try after some time.

Solution:

Import users in batches having less than 30 thousand users in each batch.

Error When Trying to Import Large number of Users from CA EEM Integrated with CA SiteMinder

Valid on all supported operating environments.

Symptom:

When importing a large number of users using LDAP Import Sync from CA EEM that is integrated with CA SiteMinder, you may experience an error.

Solution:

No known workaround.

User Name Appears as the Last Name for a User

Valid on all supported operating environments.

Symptom:

After importing users from CA EEM, the user name displays in the last name field in CA APM.

Solution:

The last name was not specified when the user was created in CA EEM. The last name is not a required field in CA EEM, but because a last name is required for CA APM, the user name is set as the last name. Verify that you specify a last name when creating a contact in CA EEM.

Importing Data for Extended Fields

Valid on all supported operating environments.

Symptom:

When you configure the data import process and use extended fields as part of the object lookup, you receive an error message similar to the following:

No keys specified for class <class name> Exception thrown! Return without creating object for class <class name>.

Solution:

Replace the extended field with a non-extended field in the lookup criteria.

Importing Secondary Objects for a Tenant

Valid on all supported operating environments.

When you import dependent secondary objects for a tenant to which you have access, the Data Importer creates the objects in the same tenant that you selected for the primary destination object. The product should create the object in the tenant that you select.

Extended Fields Do Not Appear for Subtype-Specific Secondary Objects During Column Mapping

Valid on all supported operating environments.

When you use the Data Importer to map your source columns to CA APM data fields, you select a main destination object that has a specific subtype. For example, when importing assets, the main destination object Asset(Hardware) indicates that the asset object has a subtype of hardware. During the column mapping process, you then select a destination field for each source column. The destination fields that you select are based on the main destination object and subtype that you selected (for example, you can select model fields with a subtype of hardware). Any extended fields that you defined for the selected secondary object subtype do not appear when mapping the columns and cannot be selected.

Submitting the Import Does not Validate the Data Importer Engine Status

Note: This issue is resolved in CA Service Management patch 14.1.01. Find the patch and the download details from CA Support Online.

Valid on all supported operating environments.

Symptom:

When I submit a Data Importer job for processing, I receive a message about a successful job submission. However, if the Data Importer Engine service is not running, my import job is not processed. CA APM does not check to verify that the Data Importer Engine service is started when I submit a job.

Solution:

Verify that the Data Importer Engine service is running. If not, start the service or contact your system administrator.

Object Names Beginning with Numbers Cause Errors

Note: This issue is resolved in CA Service Management patch 14.1.01. Find the patch and the download details from CA Support Online.

Objects imported from the Data Importer that have names beginning with numbers cause errors when you try to link to them in CA APM. For example, a company name that begins with a number causes an error when you try to create a cost center for the company. A similar error occurs if you try to create a company relationship for a company acquisition. If the acquired company name begins with a number, an error results and you cannot save the relationship.

https://wiki.ca.com/display/CASM/.CA+Service+Catalog+Installation+Known+Issues+v14.1

CA Asset Portfolio Management Search Known Issues

The following known issues can affect how you search for objects in CA APM.

Asset Searches for the CI and Asset Check Boxes

Valid on all supported operating environments.

When you configure an asset search in which you specify Yes or No for the CI and Asset fields, the search results return either 1 (true) or 0 (false). The search results should return Yes and No.

User-Defined Searches with Asset Families or Legal Templates

Note: This issue is resolved in CA Service Management patch 14.1.01. Find the patch and the download details from CA Support Online.

Valid on all supported operating environments.

Symptom:

When creating a user-defined search, I can select an asset family or legal template, or a group of asset families or legal templates for the primary object. When I select a related secondary object for the search, the product requires me to select an asset family or legal template for the secondary object. For example, I create an asset search and select both the hardware and computer asset families. I select the model object as the secondary object, and the product requires me to select an asset family for the model. The product should maintain the asset family or legal template from the primary object and not require me to select an asset family or legal template for the secondary object.

Solution:

Select the same set of asset families or legal templates for both the primary and secondary objects in the user-defined search.

Search Selection Dialog Appears (Firefox)

Valid on all supported operating environments.

When you define an object, you can enter part of a value in a search field, select the value, and press the Tab key or click another field. In this situation, the Search Selection dialog appears with the value that you previously selected. The product should save the value you previously selected and the Search Selection dialog should not appear.

Adding Fields to User-Defined Searches

Valid on all supported operating environments.

Symptom:

When selecting asset families or legal templates for a user-defined search, the product displays a long list of available fields in the Add Fields dialog. However, I cannot scroll down in the list to select the field.

Solution:

Scroll down in the Add Fields dialog using the scroll bar to the right in the product window. You can then select the asset families or legal templates for the user-defined search.

Selected Asset Families or Legal Templates

Valid on all supported operating environments.

After you create a user-defined search and select asset families or legal templates, the selected asset families or legal templates do not appear in the product user interface. For example, you create an asset search in which you select the hardware and computer asset families. You then open the search. The selected asset families for the search do not appear. The product should display the asset families that were selected when you created the search.

Inconsistent Behavior Restricting Service Provider and Supertenant Group Data

Valid on all supported operating environments.

In a multi-tenancy environment, CA APM and CA Service Desk Manager do not consistently restrict the display of service provider and supertenant group data when you search.

Note: The supertenant group is the group of the parent record's tenant.

The following information describes this known inconsistency:

- (CA Service Desk Manager) Referenced objects can be designated as SERVICE_PROVIDER_ELIGIBLE. When enabled, the data for the service provider and supertenant group appears, even when the supertenant group does not include the service provider tenant. When disabled, only data for the supertenant group appears. The data for the service provider only appears if the service provider is a member of the supertenant group.

- (CA APM) Referenced objects can be designated as SERVICE_PROVIDER_ELIGIBLE. When enabled, the data for the service provider and supertenant group only appears when the service provider is a member of supertenant group. When disabled, data for the service provider does not appear, even when the service provider is a member of the supertenant group.

Note: By default, the only SERVICE_PROVIDER_ELIGIBLE enabled attributes are available for the contact and organization objects.

Performance Can Be Slow for Some New Audit Search Functions

Valid on all supported operating environments.

With a high number of users (for example, 100), system performance can be slow when performing the following new audit search functions:

- Add fields for a new audit search

- Refresh an asset audit history

- View an audit history.

Users Cannot Create New Audit Searches for Objects with Extensions

Valid on all supported operating environments.

Symptom:

As a non-administrator user, I receive errors when I attempt to create a new Audit Search for an object that has an extension. The extension can be any type–Simple, Reference, or Hierarchy.

Solution:

Correct the problem by executing a database stored procedure.

Follow these steps:

1. Execute the following database stored procedure:
   al_build_security_hierarchy

2. Restart Internet Information Services (IIS) by performing the following steps:

1. a. On the CA APM web servers and application servers, open a Command Prompt window.

   b. Execute the following command:
   iisreset

CA Asset Portfolio Management Integration Known Issues

The following known issues can affect how you integrate CA APM with other products.

CMDB Model Consistency between CA Service Desk Manager and CA APM

Valid on all supported operating environments.

If CA APM is integrated with a compatible version of CA SDM on the same Database and you create a Model in CA Service Desk Manager and you then update the Class value, the corresponding Family is automatically added to the Database. The same Model is now visible in CA APM.

Note: The Administrator must ensure that the Models and assets belong to the same family because of this auto update feature. Also, if the Model created in CA SDM does not have Family, it is not visible in CA APM.

For example, if the user has created a Model with Class as "Hardware" and then the user updates this value to "License", the Family of CA APM now is automatically changed to "Software" from the initial value of "Hardware". Now, you have the Asset as Hardware even though the Model is changed to "Software". To overcome this inconsistency, use the Change Asset Family wizard in CA APM.

CA Software Compliance Manager and CA APM in a Multi-Tenancy Environment

Valid on all supported operating environments.

Do not use CA Software Compliance Manager in an environment that includes a tenanted release of CA APM. If you do, a CA Software Compliance Manager user may be able to view and update tenanted CA APM data to which they should not have access.

Oracle MDB in an Integrated Product Environment

Valid on all supported operating environments.

When you create or use an Oracle MDB in an integrated product environment, verify that tablespace values for data and indexes are consistent among the integrated products. Consider the following information:

- CA APM and CA Service Desk Manager allow the product administrator to select the tablespaces for data and indexes during the CA MDB installation.
- CA Service Catalog uses fixed values of MDB_DATA and MDB_INDEX for the data and index tablespaces, respectively. The fixed values are contained within the installation and the product administrator cannot change the values.
- CA Client Automation uses fixed values of mdb_data and mdb_index for the data and index tablespaces, respectively. The tablespace values are contained within a script and the product administration can manually change the values.

When installing in an integrated product environment, plan your installation accordingly. Make the necessary changes to the data and index tablespace values so they are consistent (including uppercase and lowercase formatting) across the products.

Asset Families Not Completely Defined

Valid on all supported operating environments.

Symptom:

When using CA APM, the following product behavior occurs:

- Hardware reconciliation does not complete as expected.

- You experience incorrect behavior and fields on the Asset and Model pages.
- You receive incomplete search results for asset searches that you configure to include the Asset Family, Is Software and Reconcile Hardware fields. The incomplete search results include assets from CA Service Desk Manager and CA Service Catalog.

Solution:

CA Service Desk Manager and CA Service Catalog do not assign a value to the Asset Family, Is Software and Reconcile Hardware fields. If CA Service Desk Manager, CA Service Catalog, or both products are installed before CA APM, verify in CA APM that the Is Software and Reconcile Hardware fields for Asset Family (Computer, Hardware, Other, Projects, Service, and Software) are correctly set. Click the Directory tab, List Management and select Asset Family to verify these field settings.

User-Defined Searches and the Is Software Field

Valid on all supported operating environments.

When you integrate CA Service Catalog and CA APM, you can create and successfully save a user-defined search in which the Is Software field is set to Yes. If you then update the user-defined search and change the Is Software field to No, a message appears indicating that the search is successfully saved. However, the product does not save the Is Software field update for the search.

Legal Document Records from the CA CMDB Asset Viewer Do Not Appear

Valid on all supported operating environments.

Symptom:

In an integrated environment with CA Service Desk Manager or CA CMDB, the Common Asset Viewer may not display data as expected. For example, when you select an asset in CA APM, the Common Asset Viewer displays one or more legal document records. However, when you select the same asset in CA Service Desk Manager or CA CMDB, the Common Asset Viewer does not display the legal document record. The legal document record may not appear because insufficient privileges are assigned to the CA Service Desk Manager or CA CMDB database user in the Common Asset Viewer. properties file (by default, C:\Program Files\CA\Service Desk Manager\bopcfg\www\CATALINA_BASE\webapps\AMS\WEB-INF\classes).

Solution:

Complete the following steps to assign the correct privileges to the database user:

1. Assign the user explicit SELECT grant privileges to the tables used by the Common Asset Viewer, or assign the user to a group having explicit grant privileges to the tables.
   Note: If you receive an error about a table not being found, you can safely ignore this error.

2. Restart the appropriate service in CA Service Desk Manager, and the Apache Tomcat Common Asset Viewer service in CA APM.
   The same legal document records appear from both the CA Service Desk Manager or CA CMDB Asset Viewer, and the CA APM Asset Viewer.

Tables Used by the Common Asset Viewer

al_costdet	al_paydet	arg_action
arg_actiondf	arg_actionlk	arg_assetver
arg_costdet	arg_drpdnlst	arg_itemver
arg_legaldef	arg_legaldoc	arg_legasset
arg_linkdef	arg_paydet	arg_strlst
arg_link_asset_cost	arg_dl_cost_type	arg_dl_doc_location
arg_sl_contract_used	ca_application_registration	ca_currency_type
ca_asset	ca_asset_source	ca_asset_type
ca_capacity_unit	ca_company	ca_contact
ca_discovered_hardware	ca_discovered_hardware_ext	ca_discovered_software
ca_logical_asset	ca_model_def	ca_organization
ca_owned_resource	ca_resource_class	ca_resource_cost_center
ca_resource_family	ca_resource_gl_code	ca_resource_operating_system
ca_resource_status	ca_software_def	inv_generalinventory_item
inv_generalinventory_tree	inv_item_name_id	inv_tree_name_id
Invgene		

Gold Brick Icon in CA Service Catalog Fails to Fulfill with an Access Denied Error

Valid on all supported operating environments.

Symptom:

When I click the gold brick icon in CA Service Catalog to fulfill an asset request, CA APM starts but I receive an Access Denied error. I have verified that I'm a member of the System Administrator role and I have access to asset fulfillment.

Solution:

Complete the following steps to resolve this known issue:

1. Open a browser and navigate to http://support.ca.com.
   The CA Support Online page appears.

2. Log in to CA Support Online.

3. Enter TEC536192 in the Search text box and click Search.
   The search results appear.

4. Click the appropriate knowledge base article in the search results.

5. Complete the instructions that are documented in the knowledge base article.

Object Deletion Fails from an Integrated CA Software Compliance Manager Environment

Valid on all supported operating environments.

Symptom:

When I delete an object in CA Software Compliance Manager that has an extended field defined in CA APM, I receive an error in CA Software Compliance Manager.

Solution:

When CA APM and CA Software Compliance Manager are integrated, you can access and manage the following objects from both products:

- Company
- Contact
- Location
- Site
- Organization

However, if you define extended fields for one of these objects in CA APM, you can no longer delete the object in CA Software Compliance Manager. Delete the object in CA APM.

Cannot Assign CA APM Models to Service Option Groups in CA Service Catalog

Valid on all supported operating environments.

Symptom:

With an integration between CA APM and CA Service Catalog, CA Service Catalog sends requests to CA APM for models. These requests are in XML format. The Microsoft .NET Framework fails these requests with the following error message:
A potentially dangerous Request.Form value was detected from the client.

Solution:

Correct the problem by changing the request validation mode so that http requests are not validated.

Follow these steps:

1. On the application server where you installed CA APM, navigate to the Application Server folder under the ITAM installation directory.
2. Open the web.config configuration file.
3. Locate the following XML tag:
   httpRuntime
4. Add the following new attribute value to this tag:
   requestValidationMode="2.0"
5. Save the web.config file.

6. Restart Internet Information Services (IIS) by performing the following steps:

    a. On the CA APM web servers and application servers, open a command prompt window.

    b. Execute the following command:
    iisreset

Cannot View CA Business Intelligence Reports after Upgrading to CA APM Release 14.1

Valid on all supported operating environments.

Symptom:

I upgraded to CA APM Release 14.1 from a previous release. I can now no longer view CA APM reports in CA Business Intelligence. One of the following error messages appears when I open the reports from CA Business Intelligence launch Pad:

A Database error occurred. The database error text is : (CS) SSO failed in CMS, contact sysadmin for details: Single Sign-On failed. Contact your system administrator for details. (FWB 00020). (WIS 10901)

A Database error occurred. The database error text is : (CS) Specified RDBMS is invalid. (WIS 10901)

Solution:

Use the following procedure to correct the problem.

Follow these steps:

1. Click Start, All Programs , CA, CA Business Intelligence 4.1 Client Tools, Universe Design Tool and open the CA IT Asset Manager universe.
2. Click Tools, Connections and select the CA ITAM connection.
3. Click Edit.
4. Enter the password for the database user.
5. Verify the connectivity by clicking Test connection.
6. Click Next to complete the wizard.
7. Save the universe and close the universe.
8. Click Import and provide the details for the previously saved universe.
9. Click OK to import the universe.
10. Save the universe and exit the CA Business Intelligence Universe Design Tool.

Database Replication Does not Work after Migration

Valid on all supported operating environments.

Symptom:

I have an integration between CA APM Release 11.3 and CA Service Desk Manager. I have unique asset extension database tables for each product. For example, CA APM uses the ucapme_asset table and CA Service Desk Manager uses the usp_owned_resource table. I have fields in both tables that represent the same data (for example, the ucapme_asset table includes the mycustomfield column and the usp_owned_resource table includes the zmycustomfield column). A replication process keeps the fields in both tables synchronized. However, the replication process will not work after I migrate data from Release 11.3 to Release 14.1.

Solution:

You can resolve this issue before or after you upgrade and migrate your data.

Resolve before Migration (Recommended)

Follow these steps:

1. Disable your replication process.
2. Log in to http://support.ca.com.
3. Enter the following document file name in the Search field:
   CA_ITAM_Integrations_Best_Practices
4. Click the ITAM Integrations PDF link for the most recent update.
5. Search for the scenario about Sharing Global Extension Fields.
6. Follow the instructions to move to global tables and fields in your Release 11.3 environment.

Resolve after Migration

Follow these steps:

1. Disable your replication process.
2. Identify the shared fields between the legacy CA APM table and the CA Service Desk Manager table.
3. In CA APM Configuration, hide the CA APM fields.
4. In CA APM Configuration, expose the CA Service Desk Manager fields.

CA Asset Portfolio Management Normalization Known Issues

The following known issues can affect how you normalize data using CA APM.

- Normalization Lists with Removed Values (SQL Server) (see page 245)
- Map Button is Disabled for Normalization Rule Mapping (see page 246)

Normalization Lists with Removed Values (SQL Server)

Valid on all supported operating environments.

Symptom:

After I initially map the items in a normalization list (for example, nonauthoritative collected companies to normalized authoritative companies), the normalized value is removed from the list. The value is no longer available for mapping additional items.

Note: When a normalized item appears multiple times in the list for different tenants, each normalized item having the same value is removed from the list.

Solution:

To map additional items to the normalized value, complete the following steps:

1. Delete the existing items from the mapping.
2. Map the items again, with any additional items.

Map Button is Disabled for Normalization Rule Mapping

Valid on all supported operating environments.

You define a company, operating system, or system model normalization rule in the product (Directory, List Management, Normalization) by mapping a collected (discovered) object with an authoritative normalized object. The normalization pages display lists of collected objects and normalized objects. When you select the objects that you want to map, you must select the normalized object first and then the collected object to enable the Map button. If you select the collected object first and then the normalized object, the Map button is disabled. You cannot map the objects until you select the objects in the correct order.

CA Asset Portfolio Management Data Validation Known Issues

Data Validations for Currency Fields

Valid on all supported operating environments.

CA APM performs prevalidations of the format and content for currency fields. As a result, when you define a data validation for a currency field, do not include validations for the currency symbol, grouping symbol, and grouping limit. The prevalidations validate these items.

Important! Use the following regular expression to define currency field data validations. If you specify a different expression, CA APM overrides your expression with the following expression.

The following regular expression is the valid expression for CA APM currency field data validations:

^\d+(\<decimal_separator_symbol>\d{1,2})?$

The *decimal_separator_symbol* can vary depending on the locale, but the default is a period (.).

Examples of Valid Currency Values: 4555, 455.66, 455.5

CA Software Asset Manager Known Issues

The following known issues can affect software asset management.

Deletion Change Events Do not Work for Extended Fields

Valid on all supported operating environments.

A CA APM change event lets you monitor a CA APM field and receive a notification when a change occurs to the field value. You can define a deletion change event that processes and sends a notification when a record is deleted. If you define the deletion change event for an extended field of an asset, model, or legal document object and then you delete the object, the event does not occur. As a result, you do not receive notification that the object was deleted.

Field Validation Errors during Automatic Data Synchronization

Valid on all supported operating environments.

During automatic data synchronization, errors can occur as a result of differences between CA APM and CA SAM field validations. For example, CA APM allows a maximum of 20 characters for the Location Zip field. However, CA SAM allows a maximum of ten characters for that field. If CA APM sends Location Zip data with more than ten characters to CA SAM, CA SAM rejects the data.

To troubleshoot and resolve these field validation errors, review the error messages in the CA SAM log file and correct the CA APM data.

CA SCM Fields Are Displayed in CA APM after CA SCM Uninstallation

Valid on all supported operating environments.
If you have an environment with CA APM integrated with CA SCM, you see software-related fields from CA SCM displayed in CA APM. When you want to enable SAM capabilities in CA APM, you uninstall CA SCM. However, just uninstalling CA SCM does not remove the CA SCM fields from CA APM. You must also enable the SAM capabilities in CA APM (Administration, System Configuration, Software Asset Management). Then CA SCM fields are removed from CA APM.

Intermittent Error Occurs with Multiple Workflow Providers

Valid on all supported operating environments.

If you have implemented CA SAM with CA APM, the following message appears intermittently in the CA APM Event Service log file:

```
ERROR CA.Applications.EventService.EventService - Web Service threw
exception
CA.Common.Utilities.Exceptions.ValidationException: Another user
updated this record after it was loaded.

at CA.Common.Data.Persistence.Persister.Save(IEntity entity)at CA.
Common.Business.BusinessEntityImp.Save()at CA.Applications.Business.
FiredEvent.Save()at WebService.Service.
Save_WithoutInjectedLogging3619502461923(Byte[]RequestStream)
```

This message indicates that multiple workflow providers (for example, CA Process Automation and the CA SAM Workflow provider) attempted to update the status of the same event. The update failed. However, the event is updated successfully during the next Status updater processing cycle of the Event Service.

CA APM Components Fail when IIS 7 is Installed on Windows 2008

Valid on Windows 2008 operating environments.

Symptom:

When I have Microsoft Internet Information Services (IIS) 7 installed on Windows 2008, the WCF Services do not work. CA APM uses a WCF Service to implement the web services function.

Solution:

This problem occurs because the service file types are mapped incorrectly or the Windows components, including IIS 7, were installed in an incorrect order. To correct the problem, verify and change (if necessary) the IIS settings. Microsoft provides information and solutions for the problem.

Follow these steps:

1. In a web browser, open the Microsoft website (http://www.microsoft.com) and search for "IIS Hosted Service Fails".

2. Follow the instructions in the article.

Common Asset Viewer Does not Display Device Details with Certain Special Characters

Valid on all supporting operating environments.

Common Asset Viewer fails to display Device details when the details in CA SAM contain straight quotation marks followed by a semicolon (";).

The following error message is displayed:

There was an error when attempting to connect SAM web service. Please see the log for more details.

Software Asset Management Configuration Page Displays Incorrect Message

Valid on all supported operating environments.

If you implemented CA SAM with CA APM in a previous release, you need to enter some additional CA SAM configuration parameters after you upgrade to release 14.1. On the product user interface, you navigate to the Administration tab, System Configuration, Software Asset Management page. Fields are available for single sign-on (SSO) and CA SAM web services. After you complete these fields and click Save, you should receive the following message:

The save has completed successfully.

Instead, the following message appears:

You cannot undo this action. Are you sure you want to enable CA APM with SAM capabilities?

This message should not be displayed because CA SAM is already implemented with CA APM.

Cannot Save Zend Server Configurations during CA SAM Installation with Internet Explorer 8

Valid on all supported operating environments with Internet Explorer 8.

Symptom:

During the CA SAM installation, I install and configure the Zend server. (For more information about installing and configuring the Zend server, see the CA SAM product documentation.) However, while configuring the Zend server with Internet Explorer 8, I cannot save the configurations. The Save button is disabled on the configuration page.

Solution:

To configure the Zend server, use one of the following browsers and versions:

- Firefox 10 or higher
- Chrome 17 or higher
- Internet Explorer 9 or higher
- Opera 11
- Safari 5

CA Asset Portfolio Management Web Services Known Issues

The following known issues can affect how you use web services with CA APM.

- Objects with Negative Key Values (see page 250)
- CA Process Automation Does not Load the CA APM Web Services WSDL Correctly (see page 250)

Objects with Negative Key Values

Valid on all supported operating environments.

You can use the web services to create CA APM objects from your external client application. When you use the web services, do not create CA APM objects in which you set the key with a negative value. If you create an object with a negative key value, the object is successfully created in certain circumstances and the key value is available in the database. However, the key value does not appear in the product user interface.

CA Process Automation Does not Load the CA APM Web Services WSDL Correctly

Valid on all supported operating environments.

Symptom:

The CA APM web services allow you to download a WSDL (.wsdl) file. You open the WSDL file in CA Process Automation and set the values for the web service parameters. However, CA Process Automation encounters some problems with the SOAP message format and structure of the CA APM WSDL. As a result, CA Process Automation may not load the WSDL correctly.

Solution:

Create each SOAP message that you need and use it in CA Process Automation as a preformatted SOAP message file. Create a separate SOAP message for each operation (on each object) that you want to perform.

Complete the following steps to create and implement preformatted SOAP messages:

1. Navigate to Administration, Web Services and download the WSDL (.wsdl) file to your local computer.

2. Open the WSDL file in your preferred SOAP message tool.

3. Create a SOAP message XML file for each method and operation that you want to perform in web services.
   Note: You must create a SOAP message file for the Login method.

4. Save the SOAP message files on a server that CA Process Automation can access. The following example shows a path and file name for a SOAP message file that is named SearchContact.xml:
   C:\Program Files\CA\ITAM\SOAPS\SearchContact.xml

5. Open CA Process Automation and create or open the required CA Process Automation process.

6. Use the saved SOAP messages as preformatted messages with the SOAP operator in CA Process Automation.

7. Modify the data and settings for the SOAP message files, if required.

8. Start the process.
   Note: After the Login method has run and you receive the authentication ticket ID, save the ID in a temporary variable or data set in the process.

Example: SOAP Message for Logging in to CA APM

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Body>
        <ns3:Login
        xmlns="http://schemas.microsoft.com/2003/10/Serialization/Arrays"
        xmlns:ns2="http://schemas.datacontract.org/2004/07/CA/ITAM/Service/Core"
        xmlns:ns3="http://www.ca.com/ITAM/APIService"
        xmlns:ns4="http://schemas.datacontract.org/2004/07/CA/ITAM/Service/DataModel
/BAAAAAA"
        xmlns:ns5="http://schemas.microsoft.com/2003/10/Serialization/">
        <ns3:UserName>uapmadmin</ns3:UserName>
        <ns3:Password>uapmadmin</ns3:Password>
        </ns3:Login>
    </soap:Body>
</soap:Envelope>
```

Example: SOAP Message for Searching for a Location by Name

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header>
        <ns2:ITAMHeader
        xmlns:ns5="http://schemas.microsoft.com/2003/10/Serialization/"
        xmlns:ns4="http://www.ca.com/ITAM/APIService"
        xmlns:ns3="http://schemas.datacontract.org/2004/07/CA/ITAM/Service/DataModel
/BAAAAAA"
        xmlns:ns2="http://schemas.datacontract.org/2004/07/CA/ITAM/Service/Core"
        xmlns="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
        <ns2:TicketID>Xkgz1GAcxkyFqyQQt/CAqw==</ns2:TicketID>
        </ns2:ITAMHeader>
    </soap:Header>
    <soap:Body>
        <ns3:Search
        xmlns="http://schemas.microsoft.com/2003/10/Serialization/Arrays"
        xmlns:ns2="http://schemas.datacontract.org/2004/07/CA/ITAM/Service/Core"
        xmlns:ns3="http://www.ca.com/ITAM/APIService"
        xmlns:ns4="http://schemas.datacontract.org/2004/07/CA/ITAM/Service/DataModel
/BAAAAAA"
        xmlns:ns5="http://schemas.microsoft.com/2003/10/Serialization/">
        <ns3:searchDefinition xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="ns2:SearchDefinition">
        <ns2:FieldstoNull xsi:nil="true" />
        <ns2:Criteria>
        <ns2:FieldstoNull xsi:nil="true" />
        <ns2:SearchObjects xsi:nil="true" />
        <ns2:CriteriaList>
        <ns2:Criterion>
        <ns2:FieldstoNull xsi:nil="true" />
```

```
            <ns2:Operator>Equal</ns2:Operator>
            <ns2:SearchObjects>
            <ns2:ITAMObject xsi:type="ns4:location">
            <ns2:FieldstoNull xsi:nil="true" />
            <ns4:contactaddressflag xsi:nil="true" />
            <ns4:contactid xsi:nil="true" />
            <ns4:inactiveflag xsi:nil="true" />
            <ns4:locationid xsi:nil="true" />
            <ns4:locationname>Chennai</ns4:locationname>
            <ns4:organizationid xsi:nil="true" />
            <ns4:telephone xsi:nil="true" />
            <ns4:tenantid xsi:nil="true" />
            <ns4:versionnumber xsi:nil="true" />
            </ns2:ITAMObject>
            </ns2:SearchObjects>
            </ns2:Criterion>
            </ns2:CriteriaList>
            </ns2:Criteria>
            <ns2:EndRow>100</ns2:EndRow>
            <ns2:StartRow>-1</ns2:StartRow>
            </ns3:searchDefinition>
        </ns3:Search>
        </soap:Body>
</soap:Envelope>
```

CA Asset Portfolio Management Migration Known Issues

Migration Toolkit Shortcut is not Removed after Uninstallation

Valid on all supported operating environments.

Symptom:

During the uninstallation of CA APM, the Migration Toolkit is also uninstalled. However, the Migration Toolkit shortcut still displays on the Start menu after the uninstallation.

Solution:

To delete the shortcut, select it from the Start menu (Start, Programs, CA, Asset Portfolio Management, CA APM Migration Toolkit). You receive a prompt to remove the shortcut. Click Yes.

CA Asset Portfolio Management Events and Notifications Known Issues

The following known issues can affect how you manage events and notifications using CA APM.

- Notifications Are not Sent for Change Event with Record Deleted Only (see page 252)
- Event Service Does Not Process Events When Components Are not Working (see page 253)
- Notification Process Files Are not Available on the CA APM Installation Media (see page 253)
- CA APM Notifications Do not Occur if CA Process Automation Is not Installed (see page 254)

Notifications Are not Sent for Change Event with Record Deleted Only

Valid on all supported operating environments.

CA APM events are associated with configurations. Therefore, for Asset, Model and Legal Document, you can define different events for each family (asset and model) or legal document template. When an event is evaluated for one of these objects, the product tries to match the configuration and family or template of the event with the object. With expected product behavior, if there is no match, the event workflow is skipped and the notification is not sent.

However, this issue occurs even when the asset family or legal template matches the object. This issue happens with most Asset, Model, and Legal Document relationship objects when the Event Type is Change Event and the Event Cause is Record Deleted Only.

Event Service Does Not Process Events When Components Are not Working

Valid on all supported operating environments.

Symptom:

When I configure the Event Service (Administration tab, System Configuration), I set the following values:

- Provider URL (for example, CA Process Automation URL)
- SMTP server (email server)

During processing, the Event Service lost communications with the Provider URL or the SMTP server. As a result, the Event Service does not process events, including CA Process Automation events and CA SAM data synchronization events.

Solution:

To resolve this situation, verify that the Provider URL and the SMTP server are working. Then restart the Event Service.

Notification Process Files Are not Available on the CA APM Installation Media

Valid on all supported operating environments.

Symptom:

I am implementing events and notifications in CA APM. I want to import the default notification process files into the workflow provider (for example, CA Process Automation). The Implementation information states that these files are available in the ITAM.xml file, which is found in the following path on the installation media:

CD1\SetupFiles\ITPAM

However, I cannot find this path on the installation media.

Solution:

The ITAM.xml file is not available on the CA APM installation media. You can download this file from CA Support Online.

Note: The ITAM.xml file is available on the installation media for previous releases.

Follow these steps:

1. Click the following link:
   ftp://ftp.ca.com/pub/ca_itam/ca_apm/apm12_9/ITAM.xml.zip

2. Save ITAM.xml.zip in the desired directory.

3. Extract the contents of ITAM.xml.zip.
   The contents of ITAM.xml.zip include one file, ITAM.xml. The ITAM.xml file incorporates the default notification process files.

4. Continue with the procedure Import the Workflow Provider Notification Process Files (see page 3490).

CA APM Notifications Do not Occur if CA Process Automation Is not Installed

Valid on all supported operating environments.

CA APM allows you to define and configure notifications that occur after specific events take place. CA Process Automation, which is the workflow provider for CA APM notifications, must be installed for the notifications process to work. If CA Process Automation is not installed, you cannot define and configure notifications and notification alerts are not produced.

You can install CA Process Automation by selecting the Install Event Service option during the CA APM installation.

CA Asset Portfolio Management Audit History Known Issues

Audit History Displays Entries for Deleted Relationship Objects

The CA APM audit history lets you view a list of all changes that were made to an object record. These change entries are removed from the audit history when the object is deleted. However, for some relationship objects (for example, legal document for an asset), the audit history retains the change entries even after the relationship object is deleted.

For example, you delete an existing asset legal document object. At a later time, you create a new legal document object for the same asset. When you look at the audit history for the new asset legal document, you see the history of changes for the deleted object and the new object.

CA Asset Portfolio Management Multi-tenancy Known Issues

Users with No Tenant Can Log In

Valid on all supported operating environments.

Symptom:

If I enable multi-tenancy after I create users or user roles, the roles and users are not updated with the correct tenant settings. As a result, users can log in and access tenant data when they do not belong to a tenant.

Solution:

To reset the tenant settings for the users and roles, complete the following steps:

1. Navigate to the Role Details page for each role that you created before you enabled multi-tenancy.
2. Verify that the tenant permissions are correct and click Save.
3. Navigate to the Contact Search page and delete each user that you created before you enabled multi-tenancy.
4. Create each user again (New Contact), assign the correct tenant, and click Save.

CA Asset Portfolio Management User Interface Known Issues

The following known issues can affect how you work with the CA APM user interface.

- Currency Symbol Does not Match the Currency Type (see page 255)
- Attachment File Name with Spaces is Truncated in Firefox (see page 255)

Currency Symbol Does not Match the Currency Type

Valid on all supported operating environments.

Some currency types do not have associated currency symbols in CA APM. In this situation, a CA APM currency field (for example, Unit Amount) displays the currency symbol that is associated with the browser locale. This symbol may not match the selected currency type. The Currency Type field displays the correct type even if the currency symbol is incorrect.

Attachment File Name with Spaces is Truncated in Firefox

Valid on all supported operating environments with Firefox.

Symptom:

With the Mozilla Firefox browser, I see that a file attachment file name with spaces is truncated after the first space. The attachment content is displayed correctly.

Solution:

You can install a fix for the Firefox browser so that the entire file name displays.

Follow these steps:

1. Open a Firefox browser window.
2. Access the following URL address:
   http://www.polarcloud.com
3. Click Firefox at the top of the page.
4. Scroll to the article that is titled "TruncFix 1.04" and click the article.
5. Follow the instructions to download and install the fix.

6. When the installation is complete, open the file attachment again.
   The attachment opens and the file name displays correctly.

CA Asset Portfolio Management Upgrade Known Issues

The following known issues ca affect how you upgrade CA APM.

- CA APM User Interface Displays Error Message after Upgrade (see page 256)
- Error Message During CA APM Upgrade (see page 257)
- CA EEM Integration with CA APM fails on Oracle Database during Upgrade (see page 257)

CA APM User Interface Displays Error Message after Upgrade

Symptom:

After I upgrade CA APM from release 12.9 to release 14.1 and open the CA APM interface, an error message is displayed.

Solution:

This issue can be seen in any environment where you modified the web.config file manually after CA APM 12.9 installation. Installing release 14.1 does not replace the file, as the file was manually edited and thus retains the changes made to the file.

Follow these steps:

1. Open the web.config at [ITAM Root Path]\Web Server folder file in notepad.

2. Find the following entries:

```
<add assembly="BusinessObjects.DSWS.Session, Version=11.5.4100.0,
Culture=neutral, PublicKeyToken=692FBEA5521E1304"/>
<add assembly="BusinessObjects.DSWS.ReportEngine, Version=11.5.4100.0,
Culture=neutral, PublicKeyToken=692FBEA5521E1304"/>
<add assembly="BusinessObjects.DSWS, Version=11.5.4100.0, Culture=neutral,
PublicKeyToken=692FBEA5521E1304"/>
<add assembly="BusinessObjects.DSWS.BIPlatform, Version=11.5.4100.0,
Culture=neutral, PublicKeyToken=692FBEA5521E1304"/>
<add assembly="BusinessObjects.DSWS.QueryService, Version=11.5.4100.0,
Culture=neutral, PublicKeyToken=692FBEA5521E1304"/>
```

3. Replace the entries with the following entries:

```
<add assembly="BusinessObjects.DSWS.Session, Version=14.0.2000.0,
Culture=neutral, PublicKeyToken=692FBEA5521E1304"/>
<add assembly="BusinessObjects.DSWS.ReportEngine, Version=14.0.2000.0,
Culture=neutral, PublicKeyToken=692FBEA5521E1304"/>
<add assembly="BusinessObjects.DSWS, Version=14.0.2000.0, Culture=neutral,
PublicKeyToken=692FBEA5521E1304"/>
<add assembly="BusinessObjects.DSWS.BIPlatform, Version=14.0.2000.0,
Culture=neutral, PublicKeyToken=692FBEA5521E1304"/>
```

4. Save and close the file.

Error Message During CA APM Upgrade

Symptom:

While trying to upgrade CA APM from an earlier release version to CA Service Management 14.1, I encounter the following error message:

The specified service does not exist as an installed service. Unable to delete AMS service.

Solution:

This error has no impact on the upgrade process. Click okay to continue and proceed with upgrade process.

CA EEM Integration with CA APM fails on Oracle Database during Upgrade

Symptom:

CA EEM integration fails if you are upgrading CA APM and you have selected **Redo Integration** on an Oracle Database. Integration does not happen successfully if you have given different names for Oracle Net Service and Oracle System ID (SID).

Solution:

Create a new Oracle Net Service Name with the same name as the Oracle SID and click **Retry** to proceed with the upgrade process.

CA Asset Portfolio Management Known Database Issues

This article contains the following known issues:

Application Login

Attempt to login to the application when a node is shutting down, will cause CA Asset Portfolio Management to generate an error message. For example:

Unable to establish a connection with the database. Oracle Error: ORA-03113: end-of-file on communication channel.

Object Creation

Attempt to create a core object when a node is shutting down, will cause CA Asset Portfolio Management to generate an error message. For example:

Unable to establish a connection with the database. Oracle Error: ORA-01089: immediate shutdown in progress - no operations are permitted.

Export CSV

Attempt to export CSV when a node is shutting down, will cause CA Asset Portfolio Management to generate an error message. For example:

The export request could not be completed. No output results were created.

CA Service Management Mobile Application Known Issues

This section contains the following Known Issues:

Unable to Open the Survey Form

Symptom:

You opened a CA Process Automation work item and clicked on the survey link. It opens the CA Service Desk Manager login page. When you enter your credentials, the survey form is not displayed.

Solution:

For using the survey and other CA Service Desk Manager related links, open the link on your desktop Internet Explorer or Mozilla Firefox web browser. In general hyperlinks located inside the CA Process Automation forms do not open, subject to any network limitations and limitations of launching the URL on the mobile device web browser.

Unsupported Form Fields

The *My Tasks* capability does not support the following:

- Lookup fields, select fields, and radio groups. If you have used a form with any of these fields in CA Process Automation or to create a work item, these fields are not displayed in the *My Tasks* capability when you view the work item.
- CA Process Automation form features which were introduced in CA Process Automation 4.1, such as java script form manipulation.
- Minimum and maximum length for string input fields in CA Process Automation.

Slow or No Response from Workflow Engines

Symptom:

I am facing slow or no response from the associated workflow engines.

Solution:

This problem occurs if there is an overload of work items (for example, for more than 500 work items). Performance may be improved if you increase the cache for the associated workflows. The LRUBUFFERISIZE is an approximate number of pending tasks that are actively being referenced by CA Process Automation or CA Service Desk Manager. The default value is 1000.

Alternately, disabling SDMLOOKUP can also improve performance at the expense of reducing some functionality.

Note: After you disable SDMLOOKUP, restart the CA Service Desk Manager server.

Follow these steps:

1. Log in to the CA Service Desk Manager server.
2. Set NX_MOBILE_WFM_ITPAM_LRUBUFFERSIZE and NX_MOBILE_WFM_SDM_LRUBUFFERSIZE variables to an appropriate value. The default is 1000 entries.
3. Set the NX_MOBILE_WFM_ITPAM_DISABLE_SDMLOOKUP variable to YES. This action disables the extended information (such as start time, priority, and change order number).
4. Run the pdm_options_mgr command to update each variable. For example, run the pdm_options_mgr command to increase MOBILE_WFM_SDM_LRUBUFFERSIZE, as follows:

   ```
   pdm_options_mgr -c -a pdm_option.inst -s  MOBILE_WFM_SDM_LRUBUFFERSIZE -v 2000
   ```

5. Restart the CA Service Desk Manager server.

Data Partitions Created in CA Service Desk Manager not Supported

My Tasks capability does not take into consideration the data partition constraints that are created in CA Service Desk Manager. For this reason, the logged in user can see all the tasks and the related information, irrespective of the data partition. If a task is assigned to an authenticated user, the user can see the task.

Unified Self-Service Known Issues

The following known issues can affect how you use Unified Self-Service:

Integration Issue with Unified Self-Service

Symptom:

You might run into an issue during integration with Unified Self-Service and the install.log can contain the following errors:

```
2014/11/18 16.57.48.809 INFO  [DeployThread: Validating Unified Self-Service
Configuration] [VerifyOSOPConfig]  Verifying whether the Unified Self-Service is up
and running
2014/11/18 16.57.48.810 DEBUG [DeployThread: Validating Unified Self-Service
Configuration] [CommonUtil] Checking response from URL (http://USS_HOSTNAME:8686)
2014/11/18 17.00.45.991 DEBUG [DeployThread: Validating Unified Self-Service
Configuration] [CommonUtil] Response : 404
2014/11/18 17.15.38.518 DEBUG [DeployThread: Validating Unified Self-Service
Configuration] [CommonUtil] Retry after 10000 millis, Retry count 90 of 90
2014/11/18 17.15.38.519 ERROR [DeployThread: Validating Unified Self-Service
Configuration] [VerifyOSOPConfig] Unable to connect to Unified Self-Service on server
USS_HOSTNAME
2014/11/18 17.15.38.520 ERROR [DeployThread: Validating Unified Self-Service
Configuration] [VerifyOSOPConfig] Unable to connect to Unified Self-Service on server
USS_HOSTNAME
```

Solution:

1. Restart Unified Self-Service using Windows Services Control Panel. Unified Self-Service normally takes about 1.3 GB memory for java.exe process to start properly.

2. Log in to Unified Self-Service manually.

3. Check Unified Self-Service logs to ensure that there are no abnormal Tomcat or Unified Self-Service errors.

4. Retry the integration option through the CA Service Management installer again.

Apple Safari Browser on Windows Operating System is Not Supported

Valid on Windows

Unified Self-Service is Not Supported on Apple Safari Browser on Windows Operating System.

Unable to log in With the Special Character in Screen Name

Unified Self-Service only supports dot (.), hyphen (-), and underscrore (_) in the Screen Name. Ensure that you do not enter any other special characters.

Unable to Deploy Unified Self-Service

Symptom:

I am unable to deploy Unified Self-Service. Some of the database tables are not getting created or some of the war files are still present in the OSOP\deploy folder of the Unified Self-Service installation directory.

Solution:

Follow these steps:

1. Stop the Unified Self-Service services.
2. Log in to the Unified Self-Service server and open the portal-ext.properties file located in the OSOP folder of the Unified Self-Service installation directory.
3. Take a backup of the encrypted jdbc.default.password.
4. Modify the jdbc.default.password value with the password that you entered during the Unified Self-Service installation.
5. Set the jdbc.default.encrypted.password value to false.
6. Modify (for example, add a space and remove the space) and save the web.xml file located in the OSOP\tomcat-7.0.23\webapps\ROOT\WEB-INF\ folder.
7. Restart the Unified Self-Service services.
8. If the OSOP\deploy folder is empty, then Unified Self-Service has been deployed successfully.
9. Open the portal-ext.properties file and complete the following actions:
    a. Modify the jdbc.default.password value with the password that you backed up in step 3.
    b. Change the jdbc.default.encrypted.password value to true.
10. Save the file.

Attachment Does not Work for the Employee Access Type

Solution:

1. Inactivate the Pre-Update data partition constraint for the Employee role.
2. Set the Function Access level to Modify for the following functions for the Employee role.
    - Reference
    - Administration

Incorrect Priority Calculation When APC is Enabled or Disabled in CA SDM

Symptom:

I configured the CA SDM Data Source with ticket type as Incident. I created an incident in Unified Self-Service with a default priority, for example, 3. I observed the following incorrect changes:

- When APC is disabled in CA SDM, the urgency value of the incident is changing instead of assigning the priority to 1.
- When APC is enabled in CA SDM, the default priority field is not disabled in Unified Self-Service. Also the urgency and impact fields are not added.

Solution:

Currently no solution exists.

Unable to Re-Install Unified Self-Service

Valid on Windows

Symptom:

I am unable the install Unified Self-Service after uninstallating it. Uninstallation does not remove Unified Self-Service Related Entries in Installanywhere Registry XML

OR

I try to install Unified Self-Service and I get an error that the product is already installed (though the product does not exist in my computer).

Solution:

If the uninstaller does not remove the Unified Self-Service related entries in the InstallAnywhere registry XML file, you can change this registry file manually.

Modify the file.com.zerog.registry.xml under the directory C:\Program Files\Zero G registry after Unified Self-Service is uninstalled. Zero G Registry can be a hidden folder, so you have to enable the Show Hidden Folder option on Windows. Remove the following node <product name="Unified Self-Service"> and two other components nodes that are related to Unified Self-Service:

```
<registry install_date="2014-10-21 17:52:05" version="1.1" last_modified="2014-10-21
18:05:56">
<products>
<product name="Unified Self-Service" id="409328f9-1f0a-11b2-941e-b9699e36f638"
version="14.1.0.182" copyright="2014" info_url="" support_url="http://support.ca.com/"
 location="C:\Program Files\CA\Self Service" last_modified="2014-10-21 17:52:05">
<![CDATA[Unified Self-Service]]> <vendor name="CA, Inc." id="de0206eb-1ee1-11b2-84f1-
ce0895af55c4" home_page="www.ca.com" email=""/> <feature short_name="Open Sp" name="Op
en Space on Premise" last_modified="2014-10-21 17:52:05">
<![CDATA[This installs the Open Space on Premise Framework to support Service Desk
applications and features.]]> <component ref_id="409328f7-1f0a-11b2-941d-b9699e36f638"
 version="4.0.0.0" location="C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\CA\Unified Self-Service\Change Unified Self-Service Installation.lnk"/>
```

```
<component ref_id="409328fa-1f0a-11b2-941d-b9699e36f638" version="4.0.0.0" location="C
:\Program Files\CA\Self Service\Unified Self-Service_installation\Change Unified Self-
Service Installation.exe"/>
</feature>
</product> </products>
<components>
<component id="409328fa-1f0a-11b2-941d-b9699e36f638" version="4.0.0.0" name="InstallAn
ywhere Uninstall Component" location="C:\Program Files\CA\Self Service\Unified Self-
Service_installation\Change Unified Self-Service Installation.exe" vendor="CA, Inc."/>
<component id="409328f7-1f0a-11b2-941d-b9699e36f638" version="4.0.0.0" name="Common
Folder" location="C:\ProgramData\Microsoft\Windows\Start Menu\Programs\CA\Unified
Self-Service\Change Unified Self-Service Installation.lnk" vendor="CA, Inc."/>
</components>
</registry>
```

After removing the Unified Self-Service and components, you get to see the following code with no reference to Unified Self-Service:

```
<?xml version="1.0" encoding="UTF-8"?>
<registry install_date="2012-12-05 14:12:12" version="1.1" last_modified="2012-12-05
14:15:47">
<products></products>
<components></components>
</registry>
```

Starting of Tomcat Gives BeanLocator Exception

Symptom:

When I start the Tomcat, I get the following message:

[ServiceLocator:56] com.liferay.portal.kernel.bean.BeanLocatorException: BeanLocator has not been set for servlet context openspace-portlet in Tomcat Window.

Solution:

You can continue working as this error does not affect the Tomcat functionality.

Ignore the Error Table osop.Lock_does not Exist in Liferay Log

Symptom:

When Tomcat starts while installing Unified Self-Service, I get the following message in the Liferay. log:

Table osop.Lock_ does not exist.

Solution:

You can continue working as this error would not impact any Unified Self-Service functionality.

CA EEM Errors in FIPS Mode

Symptom:

When I work with FIPS mode supported Unified Self-Service, CA EEM API displays the following logs messages:

log4j:WARN Continuable parsing error 1 and column 20
log4j:WARN Document root element "EiamConfiguration", must match DOCTYPE root "null".
log4j:WARN Continuable parsing error 1 and column 20
log4j:WARN Document is invalid: no grammar found.
*log4j:ERROR DOM element is - not a <log4j:configuration> elemen*t.

Solution:

Unified Self-Service does not have a control over these logs and it does not affect any functionality of CA EEM.

Onboarding a Tenant Throws Tomcat Error

Symptom:

When I onboard a tenant, Liferay log shows the following error:

No theme loaders are deployed.

Solution:

This is a Liferay error, which you can see at the link: http://issues.liferay.com/browse/LPS-18614?page=com.atlassian.jira.plugin.system.issuetabpanels:all-tabpanel

You can continue working as this error would not impact any Unified Self-Service functionality.

Uninstallation does not Remove Unified Self-Service Related Entries in Installanywhere Registry XML

Valid on Windows

Solution:

For Windows Operating System, if the uninstaller does not change the InstallAnywhere registry XML file, you can change the registry manually. After Unified Self-Service is uninstalled, navigate to C:\Program Files\Zero G registry and modify the file.com.zerog.registry.xml file.

Zero G Registry can be a hidden folder, so you have to enable the Show Hidden Folder option on Windows. Remove the following node <product name="Unified Self-Service"> and two other components nodes that are related to Unified Self-Service:

```
<product name="Unified Self-Service" id="409328f9-1f0a-11b2-941e-b9699e36f638"
version="2.0.176.0" copyright="2012" info_url="" support_url="http://support.ca.com/"
location="C:\Program Files\CA\Self Service" last_modified="2012-12-05 14:12:12">
```

Unable to Open the Attached Files

Symptom:

I am unable to open the attached files of the Request and Incident in Unified Self-Service. When I click the attached file link of the request or incident in Unified Self-Service, the Service Desk Manager login page opens instead of the file.

Solution:

The name of the SERVER HOST NAME that is mentioned in CA Service Desk Manager Data Source configuration page (Administrator, Data sources, CA Service Desk Manager) of Unified Self-Service Server must match the name of the Server that is mentioned in Service Desk Repository (Administrator, Attachments, Library, Repositories, Service Desk).

Unable to Add Tags to a Question in Internet Explorer 9 Compatibility View

Symptom:

In Internet Explorer 9, when I create a new question, I do not see the option to add tags and hence cannot add tags to the question.

Solution:

No known workaround.

Accessibility Known Issues

This section contains the following known issues:

- Issue with Date and Table Components in CA Service Catalog Widgets (see page 265)

Issue with Date and Table Components in CA Service Catalog Widgets

The tab / arrows keys do not work correctly when you open a date control in the CA Service Catalog widgets because of a limitation with GXT. You cannot access some of the icons such as icons for today' s date, next month, previous month.

To work around this issue, use:

- Space bar to select **Today**
- Control + Right, Control + Left to change the month
- Shift+Up/Down to change the year

The general navigation techniques in a table also do not work correctly because of a limitation with GXT.

To work around this issue, use tab / arrow keys to navigate within the table.

CA SDM Connector Known Issues

This topic contains the following information:

Update on Service Relationships Does Not Work Properly

Symptom:

I update a relationship, affecting the scope of that relationship. A new relationship is created in Catalyst with the changed scope while the old relationship with the old scope still exists.

Example: I create a provider-dependent relationship between a portfolio application, PA1 and a service, S1. I modify the relationship by replacing S1 with another service, S2. Catalyst creates the relationship between PA1 and S2, but does not delete the relationship between PA1 and S1. This issue also occurs when I update the provider-dependent relationship between two services.

Solution:

We recommend that you delete or deactivate the relationship that you want to modify and then create the new relationship.

CA SDM Connector Does not Support High Availability

Symptom:

If the CA SDM server (on which this connector is installed) goes down, then the CA SDM connector service will also go down. As a result Service Asset and Configuration synchronization between CA SDM-CMDB and CA SOI, and CA Configuration Automation will stop working till CA SDM server is again up and running.

Solution:

Currently no solution exists.

CA CMDB and CA Confinguration Automation Integration Known Issues

This topic contains the following information:

Delay in Publishing Large Number of CIs

Symptom:

The CA Configuration Automation Connector handles data in batches. The CA Configuration Automation Connector pauses between sets of CIs before publishing to CA Catalyst. When CA Configuration Automation discovers a larger number of components, a considerable delay in publishing CIs to CA Catalyst can occur.

Solution:

You can configure the priming utility of CA Catalyst for CA Configuration Automation and can execute it. The primer tells CA Catalyst to plan the synchronization again.

Existing CA Configuration Automation Data Not Synchronized

Symptom:

If you run a CA Configuration Automation job before the CA SDM connector is configured and running with CA Catalyst, the data is not pushed to CA SDM from CA Catalyst. When a new connector is plugged in, CA Catalyst does not synchronize with the new CA SDM connector.

Solution:

No solution currently exists.

Number of Relationships in CMDB and the ServiceDesk-CMDB Projection Sheet in CA Catalyst May Differ

Symptom:

USM enforces a constraint that relationships are correlated using source, target, semantic and scope. Scope is an attribute which represents the service object that this relationship affects. When CA Catalyst sends relationships to CMDB for creation, the CA SDM Connector creates the CI and traverses the CMDB network of CIs to find its scope. If the scope is not found, the CA SDM Connector publishes the unscoped version of the relationship to CA Catalyst. Later, if the CA SDM connector finds the scope due to some update activity on the relationship, it publishes the scoped relationship to CA Catalyst. The scoped and the unscoped relationship does not correlate and results in extra relationships in the CA Catalyst database. However, there are no side-effects of these relationships in the CA Catalyst database, but they tend to persist in CA Catalyst, until they are removed from CMDB. When the relationship is removed from CMDB, it deletes the scoped, as well as the unscoped relationships from CA Catalyst.

Solution:

No solution currently exists.

CA SDM Contact Details are Updated if Business Owner/IT Owner Details are Changed in CA Configuration Automation

Symptom:

Change the Business Owner/IT Owner information of the service or server in CA Configuration Automation. Run the Catalyst Job again and view the contact information in CA SDM. User ID gets updated in CA SDM and not in the CI details of the contact.

Example:

CMDB obtains two users, User-1(username: User 1) and User-2 (username: User 2) from the CMDB import. User-1 is modified to contain the same username as User-2 in CA Configuration Automation. Both the users have different MDR element IDs. Once they are published to the Catalyst, the correlator correlates both user-1 and user-2, puts them under the same notebook, and removes the User-1 projection from the original notebook.

Solution:

No solution currently exists.

CIs and Relationships are Not Synchronized after Restarting the CA SDM Service

Symptom:

If CA SDM is restarted, the CA SDM Connector stops synchronizing both inbound and outbound CIs and Relationships. The same behavior is observed when the CA SDM Connector is restarted using the CA Catalyst Admin UI.

Solution:

Restart CA Catalyst Container service on the CA SDM Connector host.

All the Relationships are Not Deleted When the Data is Loaded through TWA

Symptom:

Some relationships are not removed from CMDB when the data is loaded through TWA.

To perform the root cause analysis and impact analysis in CMDB, CMDB must contain the relationships between the Enterprise Service and software.COTS family that the other MDRs do not provide. For example, CA Configuration Automation. The CA SDM Connector creates these relationships from the scope of the incoming relationship. When the relationships are deleted, it does not contain any information about the scope of the relationship and the CA SDM Connector has no knowledge to clean up those relationships from CMDB.

Solution:

Manually identify those relationships in CMDB and delete.

Implementing

Audience: As an Implementation Consultant, you can refer this page to help you get started with CA Service Management and to plan, install, and upgrade the product.

Getting Started

About CA Service Management (see page 270)

What's New in this Release (see page 69)

Supported Installation and Upgrade Scenarios (see page 274)

Getting Started with Installation (see page 274)

CA Service Desk Manager

Plan your Installation (see page 450)

Install the Product (see page 479)

Upgrade the Product (see page 399)

Configure the Product for First Use (see page 505)

CA Service Catalog

Plan your Installation (see page 564)

Install the Product (see page 590)

Upgrade the Product (see page 579)

Configure the Product for First Use (see page 596)

CA IT Asset Manager

Plan your Installation (see page 304)

Install the Product (see page 309)

Upgrade the Product (see page 325)

Configure the Product for First Use (see page 319)

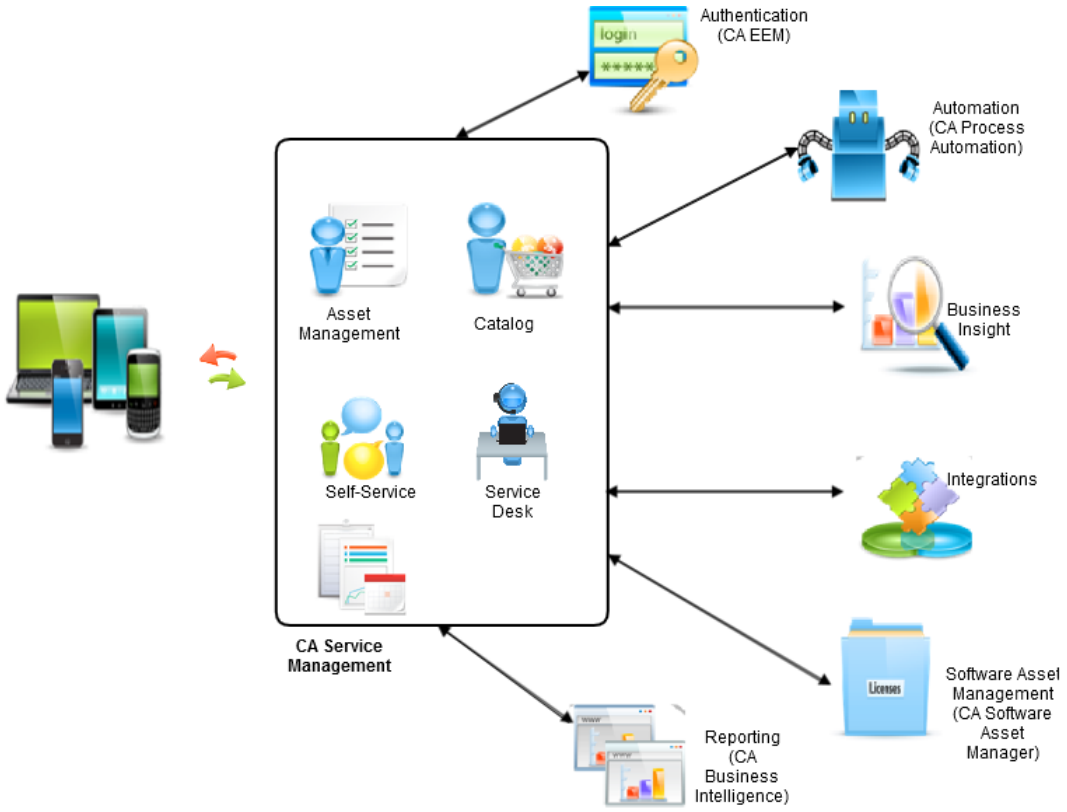
Implementing CA Service Management 14.1

CA Service Management is a seamless integration of three products namely, CA Service Desk Manager, CA Service Catalog, and CA IT Asset Manager. The solution also consists of a collaborative platform called Unified Self-Service, that lets you connect and share knowledge with the people in your organization. Unified Self-Service also offers self-service functionalities for your business users and administrators.

CA Service Management helps you do the following:

- Deliver efficient IT service management to consumers, IT teams, and management.
- Increase the value that IT provides to the business by communicating service offerings in terms that users can understand.
- Manage IT assets to deliver proven ROI and control IT spending, enable regulatory and policy compliance and improve service delivery.

The following diagram illustrates the capabilities that CA Service Management offers:



Products or Capabilities in the Solution

CA Service Management lets you leverage several capabilities that you earlier implemented by manually integrating individual solutions. For example, you can associate CA APM assets with assets requested through CA Service Catalog without having to manually integrate CA Asset Portfolio Management and CA Service Catalog.

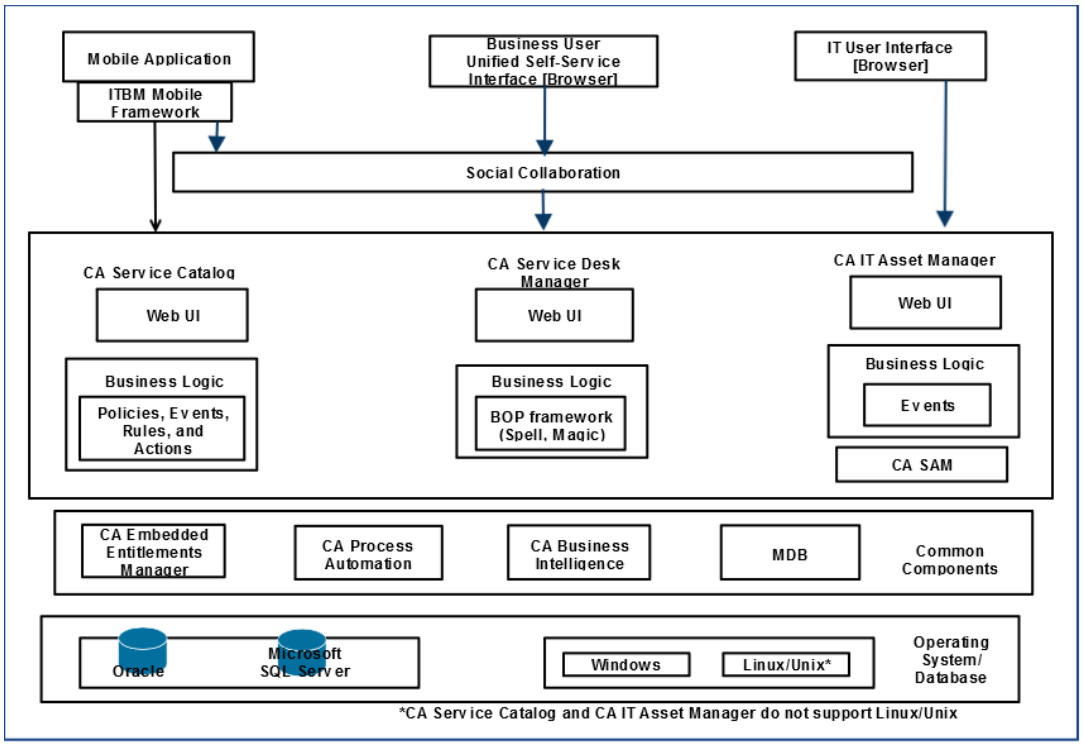
Through CA Service Management you can implement:

- CA Service Desk Manager capabilities such as Ticket (incident, problem, request, issue) Management, Change Management, Configuration Management, Knowledge Management, Support Automation
- CA IT Asset Manager capabilities such as Contract Management, Financial Management, Hardware Asset Management, Software Asset Management, Vendor Management. CA IT Asset Manager is a combination of CA Asset Portfolio Management (CA APM) and CA Software Asset Manager (CA SAM).
- CA Service Catalog capabilities such as Service Catalog Management, Service Accounting
- Unified Self-Service capabilities such as collaborating through communities, reporting issues, and requesting hardware or software services.

Note: Unified Self-Service can now be integrated with either CA Service Desk Manager or CA Service Catalog only.

Solution Architecture

The following diagram represents the CA Service Management Architecture:



Hardware and Server Requirements

The hardware requirements for each of the CA Service Management products are in the following sections.

- CA Service Desk Manager Hardware Requirements (see page 452)
- CA Asset Portfolio Management Hardware Requirements (see page 304)
- CA Service Catalog Hardware Requirements (see page 573)
- Unified Self-Service Hardware Requirements (see page 273)

For information about the supported Operating Systems, databases, and browsers, see the CA Service Management Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix).

Server Requirements

The following table lists the different components in the solution and the minimum number ofserveryou will requireforeach of them:

Component	Number of Servers (Minimum)	Description
CA Service Catalog	1	

Component	Number of Servers (Minimum)	Description
		CA Service Catalog and the accounting component are installed on the same server.
CA Service Desk Manager (Conventional Configuration)	1	One Primary Server
CA Service Desk Manager (Advanced Availability Configuration)	3	One Background Server, one Standby Server, one Application Server **Recommended:** 4 servers. One Background Server, one Standby Server, two Application Servers
CA IT Asset Manager	1	Web and Application Server can be installed on the same server. **Recommended:** 2 servers; one each for Web and Application servers.
CA EEM	Cluster: 2 Standalone: 1	
CA Business Intelligence	1	
CA Process Automation	1	
MDB	1	

Unified Self-Service Hardware Requirements

If you plan to install Unified Self-Server on a different server other than where you installed CA SDM or CA Service Catalog, you must meet the specified hardware requirements.

You must meet or exceed the following requirements to successfully install and run Unified Self Service:

Hardware	Requirements
CPU	Dual Processor 2.0 GHz preferred
RAM	Minimum 4 GB
Disk Space	4 GB

You must meet or exceed the following requirements to successfully access Unified Self-Service Web Client computer with better performance:

Hardware	Requirements
CPU	Dual Processor 2.0 GHz preferred
RAM	Minimum 2 GB available free memory
Disk Space	4 GB

You must meet or exceed the following requirements based on the size of your Unified Self-Service environment, to successfully install and run Unified Self-Service:

Database Size	Hardware	Requirements
Small—Used for installing Unified Self-Service in a test environment.	CPU	Minimum Dual Processor 2.0 GHz
	RAM	Minimum 4 GB
	Disk Space	Minimum 4 GB minimum. This will increase over time to accommodate database growth
Medium—The Unified Self-Service default. The recommended setting for most Unified Self-Service installations.	CPU	Dual Processor 2.0 GHz
	RAM	Minimum 8 GB
	Disk Space	Minimum 8 GB. This will increase over time to accommodate database growth
Large—Used for large Unified Self-Service installations.	CPU	Quad Processor 2.0 GHz
	RAM	Minimum 16 GB
	Disk Space	Minimum 8 GB. This will increase over time to accommodate database growth

Step 1 - Identify your Installation or Upgrade Scenario

You can install any combination of the products in the solution. Use the CA Service Management installer to install or upgrade the following:

- Any product in CA Service Management (CA Service Desk Manager, CA Service Catalog, and CA Asset Portfolio Management).
- Any combination of products (CA Service Desk Manager, CA Service Catalog, and CA Asset Portfolio Management)
- The entire solution with all the products.

Note: You can install Unified Self-Service only with CA Service Desk Manager or CA Service Catalog or if either of these products are already found in the environment. We recommend that you install Unified Self-Service with any combination of the products to manage the solution administration through Unified Self-Service.

Ensure that the CA Service Management products that you want to integrate share the same MDB. For example, if you have CA Service Desk Manager on non-Windows and the other products on Windows, you can integrate only if the two products share the same MDB.

You can also use the CA Service Management Installer to install and integrate any of the common components (CA EEM, CA Business Intelligence, and CA Process Automation) with the CA Service Management products. If you have an existing set up of these products, you can use them with CA Service Management, provided that the versions are supported. For information on supported versions, see the Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix).

Some of the installation and upgrade scenarios that CA Service Management Installer supports are as follows:

- Scenario 1: New Installation of one of the CA Service Management products and integrating with a common component (see page 275)
- Scenario 2: New installation of two or more CA Service Management products (see page 276)
- Scenario 3: New installation of one or more products in an existing CA Service Management 14.1 environment (see page 276)
- Scenario 4: Upgrading an existing version of the product to CA Service Management 14.1 (see page 277)
- Scenario 5: Upgrading the existing version of two or more non-integrated CA Service Management products (see page 277)
- Scenario 6: Upgrading the existing version of two or more integrated CA Service Management products (see page 278)
- Scenario 7: Upgrading the existing version of a CA Service Management product and installing another new product (see page 279)
- Scenario 8: Upgrading the existing version of a CA Service Management product when the common components are not the same (see page 279)

Scenario 1: New Installation of one of the CA Service Management products and integrating with a common component

Example: Installing CA Service Desk Manager and integrating with a common component

1. Plan your CA Service Desk Manager implementation (see page 450).

2. Install the common components (see page 283). Alternatively you can use an existing supported version of these products as listed in the Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix).

3. Install CA Service Desk Manager (see page 479) with the required configuration on each CA Service Desk Manager server. Use the "Configure Common Components" to integrate CA Service Desk Manager with any of the common components.
   The installer installs CA Service Desk Manager 14.1 and integrates it with the common component.

Note: The flow applies for CA Service Catalog and CA Asset Portfolio Management too.

Scenario 2: New installation of two or more CA Service Management products

Example: Installing CA Service Desk Manager, CA Service Catalog, and CA Asset Portfolio Management

1. Plan your CA Service Desk Manager implementation (see page 450).
2. Plan your CA Service Catalog implementation (see page 564).
3. Plan your CA Asset Portfolio Management implementation (see page 304).
4. Install the common components (see page 283) according to your requirement. Alternatively you can use an existing supported version of these products as listed in the Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix).

   Note: Ensure that you have at least one CA EEM in your environment because CA EEM is mandatory for CA Service Catalog and CA Asset Portfolio Management.

5. Install CA Service Desk Manager (see page 479) with the required configuration on each CA Service Desk Manager server.
6. Step 2 - Install CA Service Catalog (see page 590) with the required configuration on each CA Service Catalog server.
7. Install CA Asset Portfolio Management (see page 309) with the required configuration on each CA CA Asset Portfolio Management
   The installer automatically detects that CA Service Desk Manager 14.1 is already installed in the environment and integrates both CA Service Catalog 14.1 and CA Asset Portfolio Management 14.1 with each other and also with CA Service Desk Manager.
8. (Recommended) Use the common administration interface (see page 763) from the Unified Self-Service interface (if Unified Self-Service is installed) foruser, role, and tenancy management of CA Service Desk Manager and CA Service Catalog.

Scenario 3: New installation of one or more products in an existing CA Service Management 14.1 environment

Example: Installing CA Service Catalog in an environment that already has CA Service Desk Manager 14.1

1. Plan your CA Service Catalog implementation (see page 564).
2. Install the common components (see page 283). Alternatively you can use an existing supported version of these products as listed in the Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix).

Note: Ensure that you have at least one CA EEM in your environment because CA EEM is mandatory for CA Service Catalog.

3. Step 2 - Install CA Service Catalog (see page 590) with the required configuration on each CA Service Catalog server.
   The installer automatically detects that CA Service Desk Manager 14.1 is already installed and integrates CA Service Catalog with CA Service Desk Manager. Any new component that is selected for CA Service Catalog is also integrated with CA Service Desk Manager.

4. (Recommended) Use the common administration interface (see page 763) from the Unified Self-Service interface (if Unified Self-Service is installed) foruser, role, and tenancy management of CA Service Desk Manager and CA Service Catalog.

Scenario 4: Upgrading an existing version of the product to CA Service Management 14.1

Example: Upgrading CA Service Desk Manager 12.9 to 14.1

1. Plan for the upgrade of CA Service Desk Manager (see page 399).

2. Install the common components (see page 283), if required. Alternatively you can use an existing supported version of these products as listed in the Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix).

3. Upgrade CA Service Desk Manager (see page 399) on each CA Service Desk Manager server. The installer detects the version of CA Service Desk Manager and upgrades it to 14.1.

Note: The flow remains the same for Catalog except that the upgrade can be done using the traditional upgrade or migration-model upgrade.

Scenario 5: Upgrading the existing version of two or more non-integrated CA Service Management products

Example: Upgrading CA Service Desk Manager and CA Service Catalog from 12.9 to 14.1 but the products are not already integrated

1. Plan for the upgrade of CA Service Desk Manager (see page 399).

2. Plan your CA Service Catalog Upgrade (see page 580).

3. Install the common components (see page 283). Alternatively you can use an existing supported version of these products as listed in the Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix).

> **Note:** Ensure that you have at least one CA EEM in your environment because CA EEM is mandatory for CA Service Catalog.

4. Upgrade CA Service Desk Manager (see page 399) on each CA Service Desk Manager server.

5. Upgrade CA Service Catalog (see page 586) on each CA Service Catalog server.
   The installer automatically detects the existing versions of the products. It upgrades the productsto 14.1 and integrates them. Any common component integrations selected for CA Service Desk Manageris also integrated with CA Service Catalog. Also, ifany new integration is selected for CA Service Catalog, existing CA Service Desk Manager is integrated with the new common component.

6. (Recommended) Use the common administration interface (see page 763) from the Unified Self-Service interface (if Unified Self-Service is installed) foruser, role, and tenancy management of CA Service Desk Manager and CA Service Catalog.

Scenario 6: Upgrading the existing version of two or more integrated CA Service Management products

Example: Upgrading CA Service Desk Manager and CA Service Catalog from 12.9 to 14.1 and the products are already integrated

1. Plan for the upgrade of CA Service Desk Manager (see page 399).

2. Plan your CA Service Catalog Upgrade (see page 580).

3. Install the common components (see page 283). Alternatively you can use an existing supported version of these products as listed in the Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix).

> **Note:** Use the same common components for both the products.

4. Upgrade CA Service Desk Manager (see page 399) on each CA Service Desk Manager server.

5. Upgrade CA Service Catalog (see page 586) on each CA Service Catalog server.
   The installer detects the existing versions of the products and upgrades the productsto 14.1. No changes are made to existing integration. Any new component selected is integrated with both CA Service Desk Manager and CA Service Catalog.

6. (Recommended) Use the common administration interface (see page 763) from the Unified Self-Service interface (if Unified Self-Service is installed) foruser, role, and tenancy management of CA Service Desk Manager and CA Service Catalog.

Scenario 7: Upgrading the existing version of a CA Service Management product and installing another new product

Example: Upgrading CA Service Desk Manager from 12.9 to 14.1 and installing CA Service Catalog 14.1

1. Plan for the upgrade of CA Service Desk Manager (see page 399).
2. Plan your CA Service Catalog installation (see page 564).
3. Install the common components (see page 283). Alternatively you can use an existing supported version of these products as listed in the Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix).

   Note: Use the same common components for both CA Service Desk Manager and CA Service Catalog.

4. Upgrade CA Service Desk Manager (see page 399) on each CA Service Desk Manager server.
5. Install CA Service Catalog (see page 590) with the required configuration on each CA Service Catalog server.
   The installer automatically detects that CA Service Desk Manager is already installed in the environment and integrates CA Service Catalog with CA Service Desk Manager. Any new component selected is integrated with both CA Service Desk Manager and CA Service Catalog.
6. (Recommended) Use the common administration interface (see page 763) from the Unified Self-Service interface (if Unified Self-Service is installed) foruser, role, and tenancy management of CA Service Desk Manager and CA Service Catalog.

Scenario 8: Upgrading the existing version of a CA Service Management product when the common components are not the same

For example, upgrading CA Service Desk Manager12.9 integrated with CA EEM Server 1 and CA Service Catalog integrated 12.9 with CA EEM Server 2. In this scenario you can also change the common component during the upgrade process.

1. Plan for the upgrade of CA Service Desk Manager (see page 399).
2. Plan your CA Service Catalog Upgrade (see page 580).
3. Install the common components (see page 283). Alternatively you can use an existing supported version of these products as listed in the Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix).
4. Upgrade CA Service Desk Manager (see page 399) on each CA Service Desk Manager server.

5. Upgrade CA Service Catalog (see page 586) on each CA Service Catalog server.
   The installer detects the existing integrations and auto populates the information about the existing integration during the upgrade. Because the CA EEM server (CA EEM Server 2) discovered during the second upgrade is different from the CA EEM Server 1 detected in the environment already, the conflict is highlighted in the integration screen. The installer recommends using the CA EEM Server 1 used in the solution.

   - If you select to use the new common CA EEM server for integration, both the CA Service Catalog servers are integrated with the value of CA EEM Server 1,
   - If you select to not resolve the conflict, then the integration settings are not changed.

   The installer upgrades both the CA Service Catalog servers to 14.1.

6. (Recommended) Use the common administration interface (see page 763) from the Unified Self-Service interface (if Unified Self-Service is installed) foruser, role, and tenancy management of CA Service Desk Manager and CA Service Catalog.

Step 2 - Plan your CA Service Management Installation

Before proceeding with CA Service Management installation, ensure that you have reviewed the following installation planning considerations and completed the prerequisite checks for the products.

Note: CA Asset Portfolio Management App Server uses the reserved port 9080 and CA Service Catalog uses the reserved port 7777. Reserved ports are set internally and are not configurable during CA Service Managementproducts installation. You must not configure any other services on these reserved ports.

Customization

Perform Customization

Any “modifications” or “adaptions” or “configurations” that are done administratively through the interface (web browser, command-line, Web Screen Painter) are “supported”, meaning CA Support can assist with the basic suggestions and troubleshooting. CA Support do NOT perform any changes for the customer. The customer is responsible for the changes made. For example, adding a field to a table and putting the field on a form through Web Screen Painter is a fully supported “modification”. Similarly, installing or uninstalling a feature through the Options Manager administration is a fully supported “configuration”. Anything to do with SPEL code, Javascripting(or any language scripting), or a customer-specific changetothe underlying base code-line (done by CA Services or a Partner), is NOT supported by CA Support. The customer can perform these actions, but is responsible for the support, maintenance, and troubleshooting when an issue occurs. If such “customization” affect expected out-of-the-box behavior, CA Support will ask the customer to remove the customization and see if the behavior persists.

Retain Customization

When any form is modified, the customer changes are overwritten and has to be recreated. There is a process in the upgrade that attempts to detect and identify the differences in the forms, and reports it to the customer for their investigation. However, it is highly recommended to document your customization BEFORE you perform any upgrade. In some cases, a new feature may be similar to the user customization, so the user changes must be removed.

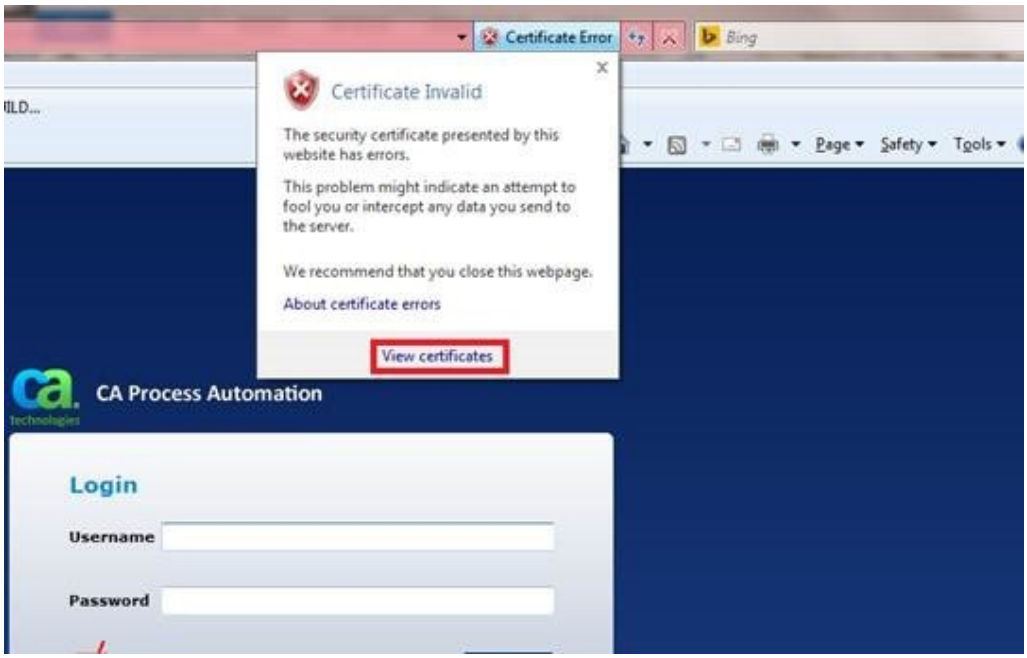
CA Process Automation Installation in an HTTPS Environment

Before the installation or upgrade, if your CA Process Automation instance is SSL enabled (configured withhttps), ensure that you add a CA Process Automation SSL certificate to the Java Runtime Environment (JRE)keystore. Without this certificate, JRE, under which the installer is running, does not connect to the CA Process Automation SSL URL and the following SSL validation errors may appear during the installation:

```
2014/11/11 19.04.39.728 DEBUG [AWT-EventQueue-0] [PAMWebserviceManager] Get ITPAM
version
2014/11/11 19.04.39.752 ERROR [AWT-EventQueue-0] [PAMValidator] CA PAM validation
failed
com.ca.smsi.installcore.webservices.WebserviceException: ; nested exception is:
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX
path building failed: sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested target
at com.ca.smsi.installcore.webservices.PAMWebserviceManager.getITPAMVersion
(PAMWebserviceManager.java:265)
```

Complete the following steps to add a CA Process Automation SSL certificate to the JREkeystore:

1. Download the SSL Certificate by accessing the CA Process Automation URL.



2. Copy this certificate file to some location. For example, c:\ItpamCert.cer

3. Extract the CA SDM DVD to a local drive. For example, C:\CASMDVD14\< >

4. Import the CA Process Automation SSL Certificate to a keystore file using the following command:

```
c:\CASMDVD14\java\jre\bin\keytool -importcert -file c:\ItpamCert.cer -alias
somealias -keystore c:/keystore_file -storepass somepass\
```

5. To enter the keystore and password values to the JRE, open the C:\CASMDVD14\setup.lax file in Wordpad or a similar text editor.

   Note: To avoid any formatting issues, it is recommended NOT to use Notepad.

6. Identify the "lax.nl.java.option.additional" property.

7. Append the reference to the JAVA keystore and keystorepass entries as follows:

   ```
   -Djavax.net.ssl.trustStore=c:/keystore_file -Djavax.net.ssl.
   trustStorePassword=somepass
   ```

   After the modification, the line would look like:

   ```
   lax.nl.java.option.additional=-Djava.library.path=".\\java\\bin; -
   DGET_SD_PRESETS=true -Djavax.net.ssl.trustStore=c:/keystore_file -Djavax.net.
   ssl.trustStorePassword=somepass
   ```

8. Save the file and restart the setup by executing C:\CASMDVD14\setup.exe command

CA Asset Portfoli o Management I nstallat ion Planning

Review and consider the prerequisites and installation planning consideration before proceeding with CA Asset Portfolio Management (CA APM) installation. For more information, see Plan your CA APM Installation (see page 304).

CA Service Catalog Installation Planning

Review and consider the prerequisites and installation planning consideration before proceeding with CA Service Catalog installation. For more information, see plan your CA Service Catalog installation (see page 564).

CA Service Desk Manager Installation Planning

Review and consider the prerequisites and installation planning consideration before proceeding with CA Service Desk Manager installation. For more information, see Step 1- Plan your CA SDM Installation (see page 450).

Important! To install CA Service Management from the non-root user on Unix or Linux, you must have the permissions to execute the sudo command.

Follow these steps:

1. Export the appropriate oracle variables and library paths.

2. Go to the CA Service Management instalelr DVD, then execute the below command:
   sudo -E PATH=$PATH ./setup.sh

Step 3 - Install the Common Components

Common components such as CA Embedded Entitlements Manager (CA EEM), CA Business Intelligence, and CA Process Automation provide the ability to integrate the CA Service Management products. If you have an existing installation of the common components in your environment, you can use these for CA Service Management as well. Ensure that the common components that you have installed is supported for CA Service Management, as listed in the Supportability Matrix (see page 119).

The common components provide the following capabilities:

- CA EEM provides the authentication and authorization capability. CA EEM eliminates plain text user names and passwords from being passed for authentication purposes.

  Note: CA EEM is mandatory for CA Service Catalog and CA Asset Portfolio Management.

- CA Business Intelligence provides the reporting capability.
- CA Process Automation provides the business process automation capability.

Install the following components, depending upon your requirement:

- Install CA Embedded Entitlements Manager (see page 283)
- Install CA Business Intelligence (see page 285)
- Install CA Process Automation (see page 292)

Install CA Embedded Entitlements Manager

This topic contains the following information:

The CA Service Management installer launches the CA EEM installer based on the system architecture. Hence, on a 32-bit Windows computer, the CA Service Management installer launches the 32-bit CA EEM installer and on a 64-bit computer, the CA Service Management installer launches the 64-bit CA EEM installer.

If CA iTechnology iGateway for CA APM installation is running as a 32-bit application on a 64-bit Windows computer, then CA EEM also runs as a 32-bit application.

If you have a 32-bit CA EEM installed on a 64-bit operating system, you see an error when you select **CA Embedded Entitlements Manager (CA EEM)** in **Select the required Installer** screen of the CA Service Management installer because the installer invokes the 64-bit CA EEM installer.

If you want to upgrade your existing 32-bit CA EEM on a 64-bit operating system, launch the CA EEM installer from the following location and not from the CA Service Management installer:

```
DVD\products\EEM\win32
```

Cluster-related CA EEM Requirements for CA Service Catalog

An installation of CA Service Catalog can include several clustered computers. Each installation of CA Service Catalog must map to an application name in CA EEM. You can set up a single instance of CA EEM and the CA Service Catalog database for multiple installations of CA Service Catalog (for example, Test and Production).

In this type of setup, the setup-related parameters (for example, the database, user, and application names) have the same values on every computer. Therefore, when you run the setup utility, you can use the remote configuration feature to copy the parameter settings from one computer to another.

If CA EEM is clustered with a load balancer, follow these steps before you run the setup utility:

1. Edit the Apache load balancer configuration file, proxy.conf file. This file is in the conf folder of the Apache installation directory.
2. Record the current setting of the MaxKeepAliveRequests property.
3. Set the MaxKeepAliveRequests property value to 0.
4. Restart the Apache load balancer services to make the configuration changes take effect.

For best performance, we recommend that you install CA EEM on a different server than the DBMS server.

Important! Make a note of your CA EEM administration password that you provide during CA EEM installation. You use this password while integrating CA Service Management products with CA EEM.

If you have a clustered environment, ensure that all the nodes in the CA EEM cluster are up and running before you install any of the CA Service Management products.

Install CA Embedded Entitlements Manager

Follow these steps:

1. Launch the CA Service Management Installer.

Note: If the Installation wizard does not open automatically, start the installation by double-clicking the setup.exe file, located at the root of the installation media.

2. Click **Select Language** to select a language from the list in the **Language Selection** screen.

3. Select **CA Embedded Entitlements Manager (CA EEM)** in **Select the required Installer** screen to launch the CA EEM installation.
   The wizard guides you through the process of installing or upgrading CA EEM.

   Note: CA EEM and CA Service Catalog each installs and uses its own JRE. Therefore, the JRE version of each product can be different.

   CA EEM has been installed.

4. Go to Start, All Programs, CA, Embedded Entitlements Manager, Admin UI on the CA EEM machine. Log into the application to ensure that the CA EEM installation was successful.

   Note: If CA EEM is configured to use an external LDAP data store, the privileged user must be created in the LDAP Directory.

You can optionally install one or more additional instances of CA EEM. To obtain high availability and fail over protection for CA EEM, cluster all CA EEM computers. For more information, see Failover configuration (https://wiki.ca.com/display/eem1251/How+to+Set+Up+a+Failover+Environment). For more information about CA EEM installation, see Installing CA EEM (https://docops.ca.com/display/eem1251/Windows+Installation).

Install CA Business Intelligence

CA Business Intelligence provides a consistent installation of SAP Business Objects Enterprise edition. Multiple CA Technologies products can share a license of CA Business Intelligence.

Important! You can integrate any CA Service Management product with CA Business Intelligence that is running on English Windows only.

Follow these steps:

- Review Hardware and Software Requirements (see page 286)
- Review Installation Considerations (see page 286)
- Install CA Business Intelligence Server and Client Tool Components (see page 287)
  - Special Instructions for Derived Universe (see page 288)
- Migrate Content from Release 3.3 to Release 4.1 SP3 (see page 288)
  - Back up Custom Universe (see page 288)
  - Import CA Business Intelligence Content (see page 289)
- Review the Best Practices to Use CA Business Intelligence (see page 292)

Review Hardware and Software Requirements

Understand the requirements and installation considerations for CA Business Intelligence from the CA Business Intelligence documentation (https://wiki.ca.com/display/CABI41SP3/Hardware+and+Software+Requirements+for+Installation). The minimum server hardware requirements for CA Business Intelligence 4.1 are:

- CPU performance of at least 8000 SAPS

  Note: SAPS, or the **SAP Application Performance Standard**, is a unit of measurement that describes the performance (throughput (http://en.wikipedia.org/wiki/Throughput) result) of a SAP system configuration. This hardware-independent unit is based on the SAP Sales and Distribution (SD) Benchmark.

- For CABI 4.x, SAP recommends 16GB RAM for a Development class machine.

Review Installation Considerations

Important! If you want to retain any one of the CA Service Management products at an older release level, you must have two instances of CA Business Intelligence. One CA Business Intelligence instance for the older release and one CA Business Intelligence 4.1 instance for 14.1. You can then access the reports for respective releases of CA Service Management products.

- Temporarily disable any antivirus software on the computer where you are installing CA Business Intelligence.
- CA Service Management integration with CA Business Intelligence is supported only when Apache Tomcat is the CA Business Intelligence application server.
- The database server details and the authentication details are available.
- You have the permission to install a new SQL Anywhere database or to use an existing SQL Anywhere database.
- You have the name for Server Intelligence Agent (SIA).
- The web application server has been installed and configured.
- For CA Asset Portfolio Management integration with CA Business Intelligence:
  - If you use MS SQL as the MDB, ensure that you install Microsoft SQL Server Native Client (64-bit) on the server where CA Business Intelligence is installed.
  - If you use Oracle as the MDB, define an Oracle Net Service Name (64-bit) on the server where CA Business Intelligence is installed. Make a note of the NSN, which you are asked to enter during the CA Asset Portfolio Management installation.

- The credentials for the CA Business Intelligence Administrator Account must be defined before running the installer for both new and custom installation.
- SAP Business Objects users with an existing installation of Business Objects can install and configure CA Business Intelligence (recommended) or they can use their existing Business Objects installation.

> **Note:** To modify the JRE version that is provided with CA Business Intelligence, see upgrade JRE in CA Business Intelligence (https://wiki.ca.com/display/CABI41SP3/Upgrade+JDK+and+JRE+in+CABI+4.1+SP3).

- Server and client installations are separate and can be installed on the same or different servers. For more information about platform installation, see CA Business Intelligence Platform Installation (https://wiki.ca.com/display/CABI41SP3/CA+Business+Intelligence+Platform+Installation).

> **Important!** For the successful CA Business Intelligence Configuration for CA Service Desk Manager, enter the Central Management Server (CMS) port number as 6400 while installing the CA Business Intelligence Server.

Install CA Business Intelligence Server and Client Tool Components

Install CA Business Intelligence on a separate server. Server and client tool components are installed separately for CA Business Intelligence Release 4.1 SP3. Both can be installed from the CA Service Management installer on the same or different servers.

Server components include Central Configuration Manager, Upgrade Management Tool, Central Management Console, BI Launchpad, Tomcat Configuration, and Tomcat Administration.

> **Note:** Before proceeding with the CA Business Intelligence Server installation, see the CA Business Intelligence Installation (https://wiki.ca.com/display/CABI41SP3/CABI+Installation+on+Windows) documentation.

Client tool components include Universe Design Tool (earlier known as Designer), Webi Rich Client, Business View Manager, Information Designer Tool, Translation Management tool, and so on. Universe Design tool is used for creating or modifying the Universes(.unv); IDT(Information Design Tool) is used for creating multi Source Universe(.unx); Webi rich Client is used for creating Webi Reports.

Follow these steps:

1. Launch the CA Service Management installer.
2. Click **Select Language** to select a language from the list in the **Language Selection** screen.

3. Select **CA Business Intelligence Server Installation** from the **Select the required installer** screen.

   Important! Refer to CA Support Online (https://support.ca.com/irj/portal/ProdCDNResults) for the correct DVD number.

4. Proceed with the installation. For more information, see the Full Installation (https://wiki.ca.com/display/CABI41SP3/Full+Installation) documentation.

5. Select **CA Business Intelligence Client Tools Installation** from the **Select the required installer** screen and complete the installation.
   You have successfully installed CA Business Intelligence.

Special Instructions for Derived Universe

Follow these steps:

1. Import the *CA Service Desk* universe from *Universe Design Tool* on the CABI Client Tools installed system.
2. Save and export the *CA Service Desk* universe.
3. From the *Universe Design Tool*, open the saved derived universe.
4. From the **File** menu, click **Parameters**.
5. Click the **Links** tab, add a link to enable the **Change Source** button.
6. Select the *CA Service Desk.unv*. Click **OK**.
7. Save and export the universe.

Migrate Content from Release 3.3 to Release 4.1 SP3

Before you migrate, ensure that you created the previous version of CA Business Intelligence content by creating the BIAR for each of the CA Service Management products. Create the BIAR using the Import wizard from the CA Business Intelligence Release 3.3 server. The BIAR includes all the previous version of out of the box Universe, Reports, Users and Groups. Also include Scheduled Instances and Custom Reports, if any.

Back up Custom Universe

If you have custom universe, take a backup.

Follow these steps:

1. Start Universe Designer.
2. Import your custom universe.

3. Save a copy of the universe on your local drive.
   The custom universe is backed up. Use this back up to update the custom universe link after you install and configure the CA Service Management products.

Import CA Business Intelligence Content

To import CA Business Intelligence 3.3 content to 4.1 server, use the Post Installation utility. Run this utility on the server where CA Business Intelligence Release 4.1 SP3 is installed.

Note: If you have installed CA Business Intelligence Release 4.1 SP3 using custom distributed, ensure that you run the utility in the web tier and Intelligence tier environment. Run the utility in the web tier environment only if you have Custom Action Framework enabled. For more information, see the post installation utility (https://wiki.ca.com/display/CABI41SP3/CA+Business+Intelligence+Platform+Post+Installation+Utility).

Follow these steps:

1. Log in to the Central Management Console installed windows machine as a CA Business Intelligence installed user.
2. Go to <CABIDVD>\utilities\PostInstall direcory from the command prompt.
3. Place the biar files that are created during the backup of the custom universe in the 3.x folder along with their corresponding properties files. Place the properties file at <CABIDVD>\utilities\PostInstall\3.x location.
4. Consider the following points:
   - Properties files are optional. Properties file must have the BIAR name. An example of the properties file for CA Service Desk Manager biar file that uses ODBC is as follows:
     - RDBMS=Generic ODBC datasource
     - DatabaseServer=casd_sdm_host
     - NetworkLayer=ODBC
     - UserName=ServiceDeskUser
     - Password=ServiceDeskPassword
     - Database= sdm_host
     - ArrayBindSize=10
     - ArrayFetchSize=10
     - PoolMode=Pooling

- PoolTime=10
- LogTimeOut=60

- Some of the properties for CA Service Catalog must be changed, as follows:
  - RDBMS= <Specify the MS SQL Server version> or For Oracle, RDBMS=<Generic ODBC datasource>
  - DatabaseServer=<DB server Name>
  - NetworkLayer=ODBC
  - UserName=sa or For Oracle, UserName=mdbadmin
  - Password=<Database password>
  - Database =caslcm_cabi_dsn
  - Some of the properties for CA Asset Portfolio Management must be changed as follows:
  - RDBMS=<Specify the name of your RDBMS>
  - DatabaseServer=<DB server Name>
  - NetworkLayer=OLE DB
  - UserName=uapadmin
  - Password=<Database password>
  - Database=<Name Of the NSN created in the datasource parameters>

5. Execute **PostInstall.bat** to run the utility from the <CABIDVD>\utilities\PostInstall path.
6. Enter **n** for Do you want to migrate data from CABI 3.x.
7. Enter **n** for Do you want to install CA Sample Templates.
8. Enter the CA Business Intelligence 4.1 SP3 Administrator password and press Enter.
   This step takes some time and after completion of the process a success message is displayed.
9. Verify the installation logs in the <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0 \logging\postinstall.log directory.
10. Import the *CA Service Desk* universe from the Universe Design tool where the CABI Client tools is installed, and then, click **File**, **Close**, to close the universe.
11. From the Universe Design tool, import any Custom (Derived) universes, and then, click **File**, **Close**, to close the universe.
12. From the Central Configuration Manager, restart the Server Intelligence Agent.

13. (Only for CA Service Desk Manager) From the CA Business Intelligence Release 4.1 SP3 Server machine, run the CA Service Management installer to configure CA Business Intelligence (see page 549).

> **Note:** After you install the CA Service Management products and integrate any of those with CA Business Intelligence 4.1, the Universe and Reports for CA Service Management 14.1 are overwritten on the previous version of out of the box Universe and Reports. Scheduled Instances are retained from the previous releases, if they exist.

You have successfully migrated CA Business Intelligence to Release 4.1 SP3.

After migrating reports from CA Business Intelligence (CABI) 3.x to CABI 4.x, if you are using CA Service Desk Manager out of the box reports using the Reports tab, the following error may appear:

```
An Error occurred : could not find the document
```

This error message appears because in CABI 3.x, CA SDM out of the box reports are located at All Folders, CA Reports, CA Service Desk folder of CA Business Intelligence. In CABI 4.x, CA SDM out of the box reports are located at All Folders, CA Reports, CA Service Management, CA Service Desk folder of CA Business Intelligence. A CABI report is exposed in the CA SDM Reports tab using a CA SDM Web Form (Security and Role Management, Role Management, Web Forms, type=Report). Such Web Form detail screen has a Resource with a value similar to the following:

```
$BOServerURL?sPath=[CA+Reports],[CA+Service+Management],[CA+Service+Desk],
[Asset]&sDocName=Asset+List&sViewer=html
```

[CA+Service+Management] folder may not exist if the CA Business Intelligence 3.x content is migrated to 4.x. To resolve this issue, perform one of the following actions:

- Edit each such Resource values of the web forms and remove the ", [CA+Service+Management]" string. Save and retest.
- Complete the following steps to create a new folder in CABI 4.x:
  a. Using a web browser, access the Central Management Console, Folders, All Folder, CA Reports.
  b. Create the "CA Service Management" folder.
  c. Move the CA Service Desk folder from All Folders, CA Reports to All Folders, CA Reports, CA Service Management. This can be performed by right clicking on CA Service Desk, Organize, Move To option.
  d. Retest

If the problem persists, contact CA Technologies Technical Support.

14. Import the *CA Service Desk* universe from the Universe Design tool where the CABI Client tools is installed, and then, click **File**, **Close**, to close the universe.

15. From the Universe Design tool, select **File**, **Open**, and navigate to the previously saved Custom (Derived) Universe (created in Step 11 above), to open the Universe.

16. Click **File**, **Parameters**.

17. Click the **Change Source** tab.

18. Select the *CA Service Desk.unv* on the file system (created in step 14 above), and then, click **OK** .

19. Save and export the universe.

20. Exit the Universe Design tool.

Review the Best Practices to Use CA Business Intelligence

Follow these best practices when maintaining and using CA Business Intelligence:

- Install and maintain one universe per CA Technologies product.
- Do *not* modify the default universe. Instead, copy it and modify the copy. Otherwise, your changes can be erased when you apply service packs, patches, and other updates. Back up all your changes and then apply the patches to your customized universe.
- Reports:
  - Verify that the services in Central Configuration Manager (CCM) are running, when the reports stop running.
  - Do not overwrite predefined reports.
  - Always use a predefined report as a base to build a custom report and maintain consistent formatting in all reports.
  - Administrators *can modify all the reports and can create* new reports that are based on the existing universe. However, administrators must not add any reports to the existing folders.
  - Both administrators and end users *must not* change pre-defined reports. Any changes to those reports are applied to all other users using the same CA Business Intelligence instance. Instead, both administrators and end users must create their own custom folders, copy the reports there, rename them, and customize them.
  - Both administrators and end users must add new reports that they create to their custom folders.

Install CA Process Automation

CA Process Automation integrates with the CA Service Management products to automate the workflow business processes.

Important! If you use CA Process Automation, we recommend that you do *not* install the CA Process Automation domain orchestrator and CA Process Automation components on the same computer.

You can also configure CA Process Automation to use CA EEM as an authentication server.

Note: If you have installed CA EEM and CA Process Automation and integrate one or more CA Service Management products with these common components, ensure that you provide the same CA EEM information that you provided while installing CA Process Automation for auto-integration to be successful.

Follow these steps:

1. From the product download page (https://support.ca.com/irj/portal/DownloadCenter) use the following DVDs for installation:
    a. CA Process Automation 4.2 SP02 (4.2.2) Third Party Prerequisites - DVD 1 - DVD07090259E.iso
    b. CA Process Automation 4.2 SP02 (4.2.2)Product Installation - DVD 2 - DVD07090455E. iso
2. Follow the Installation wizard to complete the installation process.

Note: For information about implementing multi-tenancy with CA Process Automation, see the CA Process Automation installation and configuration documentation.

Step 4 - Install or Upgrade

Complete the following for installing CA Service Management or upgrading from an earlier release version to CA Service Management 14.1:

- If you are an existing customer and want to upgrade to CA Service Management 14.1, follow the procedures described in Upgrade to CA Service Management (see page 293).
- If you are new customer, follow the procedures described in Install CA Service Management (see page 296).

Upgrade to CA Service Management

The CA Service Management installer automatically detects the existing version of the products and upgrades them with minimal or no user intervention. You can upgrade the following products:

- Upgrades Supported for CA Asset Portfolio Management (see page 294)
- Upgrades Supported for CA Service Catalog (see page 295)
- Upgrades Supported for CA Service Desk Manager (see page 295)
- Upgrades Supported for Unified Self-Service (see page 295)

Important! You must install CA Business Intelligence Release 4.1SP3 (see page 285) before you upgrade CA Service Management.

Note: If you are planning to upgrade a product that was integrated and configured with Active Directory in an earlier release, before upgrading to CA Service Management 14.1, ensure to create the CasmAdmin user and OpenSpaceAdminGroup. Associate the CasmAdmin to the OpenSpaceAdminGroup in the Active Directory.

To upgrade the products, follow these steps:

1. Review the upgrade considerations and verify the upgrade prerequisites for the products. For more information, see the Upgrade CA Service Catalog (see page 579), How to Upgrade CA SDM (see page 399), Migrate CA APM Using the Migration Tool Kit (see page 325), and Upgrade Unified Self-Service (see page 295).

2. Launch the CA Service Management installer on the servers that you want to upgrade. The installer automatically detects the installed product release version and upgrades it to 14.1.

After you have upgraded, perform additional steps to finalize the integration with the common components (see page 546) and finalize the integration with the products (see page 559) depending upon the products you have upgraded.

Important! At the end of deployment, the services must be restarted for the integration changes to come to effect.

Upgrades Supported for CA Asset Portfolio Management

Upgrades from CA Asset Portfolio Management (CA APM) releases 11.3.4, 12.6, 12.8, and 12.9 are supported. Ensure to follow the onscreen instructions on the installation wizard while upgrading as upgrade instructions for CA ITAM release 11.3.4, 12.6, 12.8 may vary from CA ITAM 12.9.

Note:

- If you are upgrading CA Asset Portfolio Management from an earlier release to CA Service Management 14.1, ensure to set the database compatibility level to MS SQL Server 2008.
- If you are upgrading CA ITAM from an earlier release to 14.1, the changes you made to configuration files from an earlier release is not automatically merged with 14.1. Refer to the backup files located in *%Temp%\ITAM* directory and manually merge these changes with the current installed version.

Upgrades Supported for CA Service Catalog

Upgrades from CA Service Catalog releases 12.6, 12.7, 12.8, and 12.9 are supported.

Upgrades Supported for CA Service Desk Manager

Upgrades from CA Service Desk Manager releases 11.2, 12.1, 12.5, 12.6, 12.7, and 12.9 are supported.

Upgrades Supported for Unified Self-Service

Upgrades from CA Open Space releases 2.0, 2.0 SP1, and 3.0 are supported.

Pre-upgrade tasks

Complete the following tasks before you upgrade to Unified Self-Service:

- Back up the existing LAR file to retain any customization you made. Upgrading to Unified Self-Service updates the existing LAR file which overwrites any existing customization.
- Stop the existing CA Open Space server. On the computer where you installed CA Open Space, select Start, All Programs, CA, Open Space, Stop.

Post-upgrade tasks

After you run the installer and upgrade to Unified Self-Service, complete the following steps:

- If you have backed up the previous LAR file, apply the customizations in the new LAR file that has been created after the installation.
- Open the existing onboarded tenant page, if any, to verify the successful upgrade.

  Note: If you upgraded from Open Space 2.0 or Open Space 2.0 SP1, the Start menu does not contain the Default Tenant - Web Client option.

- If you want the Unified Self-Service users to view the assets requested from CA Service Catalog, you must enter the My Resources offering ID from CA Service Catalog. You can obtain this ID from CA Service Catalog.
  For example, log in to CA Service Catalog , navigate to Catalog, Offerings, IT Support Services,

Service Management, My Resources, and obtain the ID from the Details page. Ensure that the CA Service Catalog server is imported with the Service Management content pack. For more information about the content pack, see the CA Service Catalog documentation.

Install CA Service Management

You can use the CA Service Management Installer to install, upgrade, configure, and integrate the CA Service Management products in the solution. The installer performs the prerequisite checks and mandatory validations before installing the products.

Important! If you plan to use CA EEM that is configured with Active Directory, before installing CA Service Management 14.1, ensure to create the CasmAdmin user and OpenSpaceAdminGroup. Associate the CasmAdmin to the OpenSpaceAdminGroup in the Active Directory.

Ensure that you have also identified your installation scenario (see page 274) and planned for your installation (see page 280) accordingly, before you proceed with this section.

Note: For Windows SQL Server database, mdbadmin is the default user across all CA Service Management products.

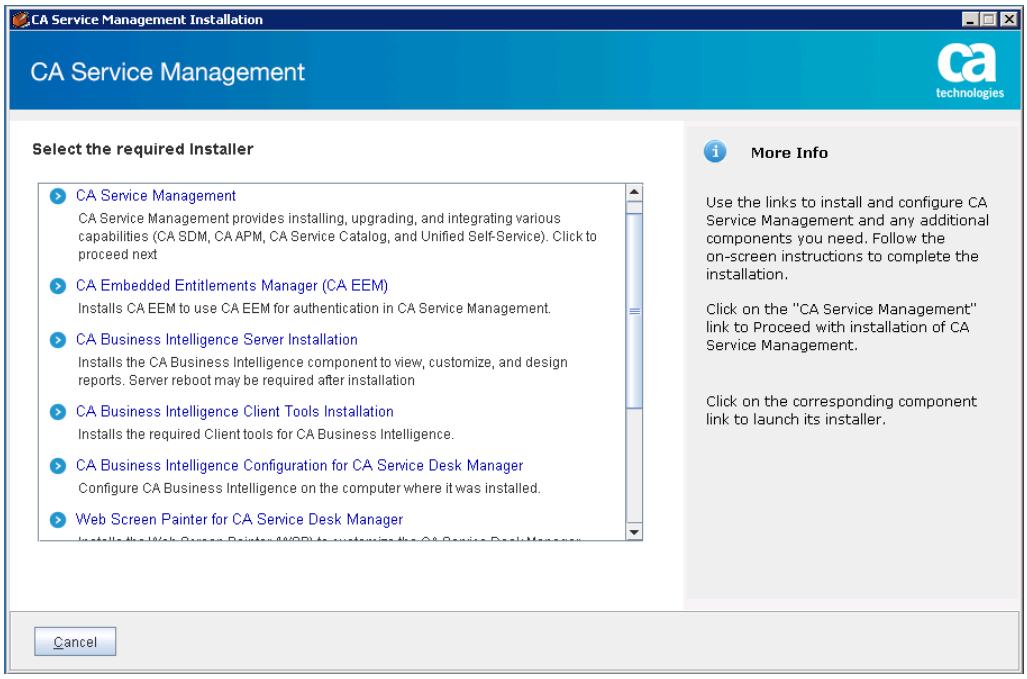
Follow these steps:

1. Launch the CA Service Management Installer.

   Note: If the Installation wizard does not open automatically, start the installation by double-clicking the setup.exe file, located at the root of the installation folder.

2. Click **Select Language** to select a language from the list.

3. Select **CA Service Management** in the **Select the required installer** screen. This option lets you install the products such as CA Service Desk Manager, CA Service Catalog, CA Asset Portfolio Management, and Unified Self-Service that are part of the the solution.



Select the required installer

4. Review and Accept the License Agreement Information.

5. Select SQL Server or Oracle as the database type in the Database Configuration screen. Enter the following information as per the selected database:
   If you have selected SQL Server, the following fields require explanation:

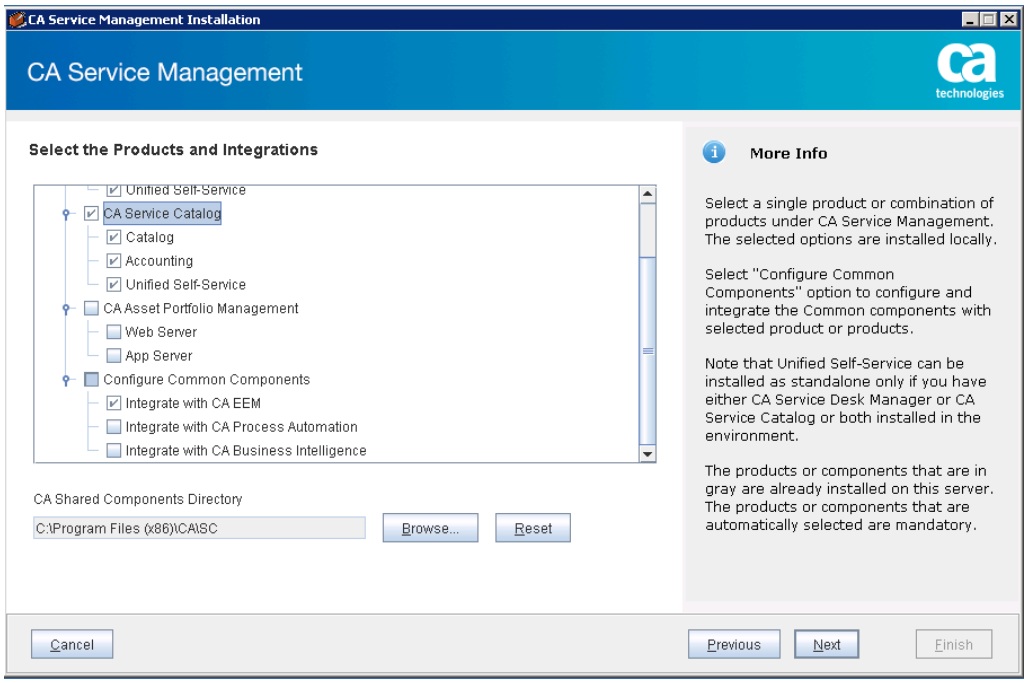
   - **Database Server**: The host name of the database server. If the target instance is part of a clustered instance, the virtual host name of the cluster must be used.
   - **Database Name**: Specifies the Database name (mdb), the name of the target DBMS. The default value is mdb.
   - **Database Port**: Specifies the port identifier for the target DBMS.
   - **Database Server Instance**: The database instance name. Leave this field blank if you are using the default instance.
   - **Database Admin User**: For SQL Server, “sa” is the default value. This is the admin user with permission to create user and schema.
   - **Database Admin Password**: Specifies the database password of user specified by database admin user. There is no default value for this parameter.
   - **mdbadmin Password**: Specify the password for the user specified for the mdbadmin user.
   - **Confirm mdbadmin Password**: Confirm the mdbadmin user password.

   If you have selected Oracle , the following fields require explanation:

- **Database Server**: The host name of the Oracle database server. If the target instance is part of a clustered instance, the virtual host name of the cluster must be used.
- **Oracle Service Name**: Specifies the Oracle Service name.
- **Listener Port**: Specifies the listener port for the database.
- **Net Service Name**: Identifies the Net Service Name of the Oracle database where the database resides. If the database is remote, use the Net Service Name defined within the Oracle client on the local computer. CA SDM and CA APM access the database using a local installation of the Oracle client, which may specify a Net Service Name that is different than the service name on the Oracle server.
- **DBA User Name**: Identifies the name of an Oracle user with DBA access. The default value for DBA user is SYS.
- **DBA User Password**: Identifies the password for the DBA user.
- **mdbadmin Password**: Specify the password for the user specified for the mdbadmin user.
- **Confirm mdbadmin Password**: Confirm the mdbadmin user password.
- **Tablespace Path (on DB Server)**: Specifies the tablespace path on the database server.
- **Oracle Home Path**: Specifies the Oracle client 32-bit path.
- **Data Tablespace Name**: Specifies the name of the data tablespace. The default value is MDB_DATA.
- **Index Tablespace Name**: Specifies the index Tablespace Name: Default value is MDB_INDEX.

6. Select any or combination of products in the **Select the Product and Integrations** screen**.**

Note: Ensure that you have verified the prerequisites and reviewed the planning considerations before proceeding with installing any or combination of these products.



Select the Products and Integrations

For example, if you have selected CA Service Catalog, you install CA Service Catalog (see page 590). Similarly, you can install CA Service Desk Manager (see page 479) and install CA Asset Portfolio Management (see page 301).

Note: CA Asset Portfolio Management App Server uses the reserved port 9080 and CA Service Catalog uses the reserved port 7777. Reserved ports are set internally and are not configurable during CA Service Management products installation. You must not configure any other services on these reserved ports.

Note: If you are installing CA Asset Portfolio Management capabilities on the same server, ensure to select your required options (either both App Server and Web Server options or any one of these options). The CA Service Management installer does not allow you to add these options later, on the same server.

7. Click **Browse** to locate the installed Common Components (see page 283)as per your installation requirement.
   Configures and integrates CA EEM, CA Process Automation, and/or CA Business Intelligence with the selected CA Service Management product or products.

8. Review the Installation Prerequisites report and take corrective measures to proceed with the installation.

9. Enter the required server details in the selected Common Component Details page. For example, if you have selected CA Process Automation as the common component, enter the server details in the **CA Process Automation Details** screen. Use the **Reintegrate CA Process Automation on local server** option to reintegrate common components (CA EEM, CA Process Automation, and CA Business Intelligence) on a system even after completing the CA Service Management installation. It allows you to reconfigure the common components again.
   For example, if while upgrading to CA Service Management, you have already integrated CA Service Desk Manager and CA EEM and then you decide to change the CA EEM server details and want to reintegrate these common components, you should select this option to reintegrate these products. Note this option only reintegrates the common components for CA Service Management.

10. Review the **PreInstallation Configuration Summary**.

11. Review the **Installation progress** information and click **Install** to install the selected product /products.

12. Review the log files stdout.txt and stderr.txt in the C:\ directory, If the installation failed. Fix the errors and click **Retry Install**.

13. Review the Installation Guidance Report summary to ensure that the installation succeeded.

You have successfully installed CA Service Management. Perform additional steps to finalize the integration with the common components (see page 546) and finalize the integration with the products (see page 559) depending upon the products you have installed.

Important! At the end of deployment, the services must be restarted for the integration changes to come to effect.

Note: As part of your CA Service Management product installation, if you have first selected and installed CA Service Catalog followed by other products (CA ITAM and/or CA SDM) and you try to integrate these products with CA process Automation, after installation it is observed that CA Process Automation configuration is not updated with CA ITAM and CA SDM host names under the CA Service Catalog and CA SDM dataset respectively.

After the installation of all CA Service Management products, launch the CA Service Management installer from the CA Service Catalog server from where you first installed or upgraded the application. On the **Select the Required Installer** page, scroll to the last option **Integrate pre-installed solution components** and follow the installation wizard instructions to complete the Redo Integration successfully.

Implementing CA IT Asset Manager

This topic contains the following information:

Important! Review the CA Service Management Release Notes (see page 69). Do not start your installation until you have read and understood the information.

Understand the CA Asset Portfolio Management Architecture

This article describes the CA Asset Portfolio Management components, and architecture.

CA Asset Portfolio Management Components

CA Asset Portfolio Management consists of the following components:

Web Server

The Web server is the main server that hosts the web application and builds the CA APM user interface. This server communicates with the user and the application server.

The following fields require explanation:

Web Server or Load Balancer IP/Host

The CA APM installation, by default, sets this field to the web server host name.

- In a single web server environment, you can enter the web server host name, or the web server IP address.
- In a multiple web server environment, you can enter either the web server host name, or the IP address of the Load Balancer.

Note: The web server can be registered with a different name in the Domain Name System (DNS) than what is registered as the web server host name. In this situation, specify the different name in this field.

You can configure additional web server components after you install the product.

Application Server

The application server is the server that connects the database server and the web server for CA APM. The business and data access logic reside on the application server. To allow for scalability, the application server and web server are on two distinct servers.

You can have more than one application server. The Export Service component and the Storage Management Service component must be installed on one of the application servers, but not necessarily on the same server.

The following fields require explanation:

Application Server or Load Balancer IP/Host

The CA APM installation, by default, sets this field to the application server host name.

- In a single application server environment, you can enter the application server host name, or the application server IP address.
- In a multiple application server environment, you can enter either the application server host name, or the IP address of the Load Balancer.

The application server can be registered with a different name in the Domain Name System (DNS) than what is registered as the application server host name. In this situation, specify the different name in this field.

You can configure more application server components after you install the product.

CA EEM

CA APM uses CA EEM for authentication. Other products that need CA EEM for authentication can use the same CA EEM server that CA APM uses.

- To manage security centrally for multiple CA Technologies products, specify the name, location, and login credentials for the existing CA EEM server.
- To manage CA APM security independently from other CA Technologies products, install CA EEM on any single application or web server other than the one where the existing CA EEM is installed.

CA Business Intelligence

CA Business Intelligence administers, monitors, and configures the reporting environment. CA APM uses CA Business Intelligence to integrate, analyze, and present information required for effective enterprise IT management.

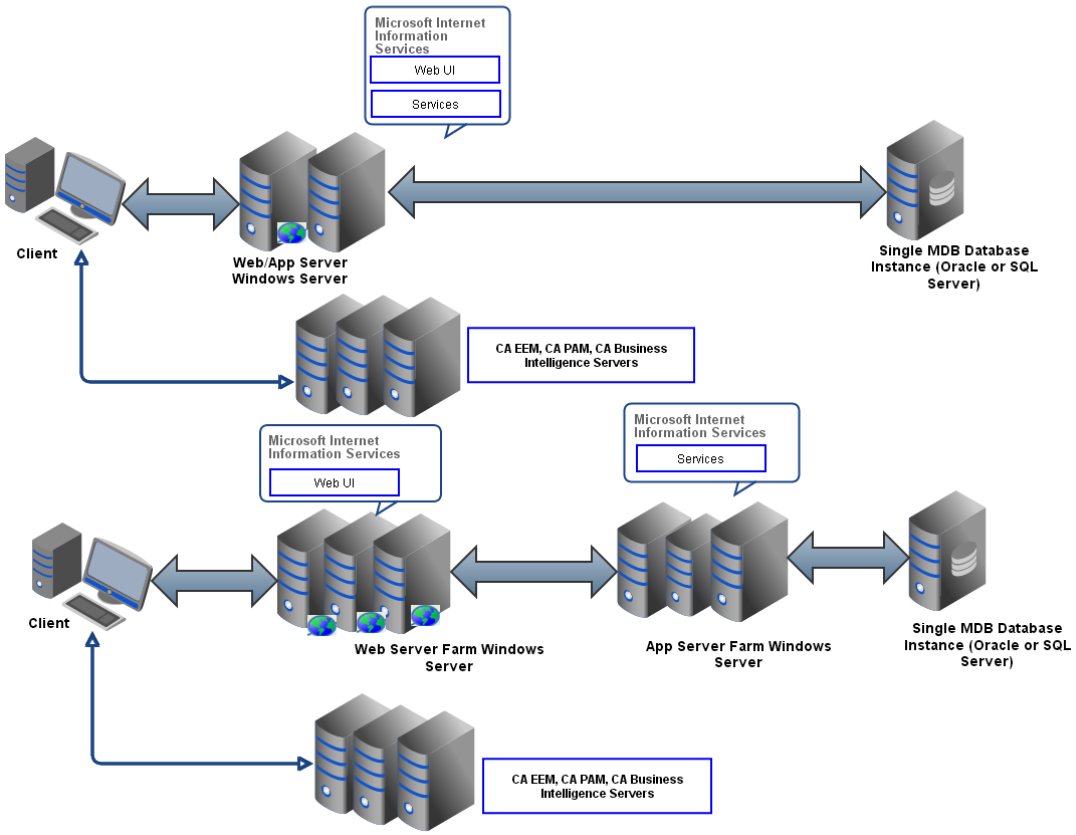
For information about the login credentials and connection information that you enter for the CA Business Intelligence component, see How to Integrate CA APM and CA Business Intelligence.

CA Process Automation Manager

CA APM and CA Process Automation integrate to let you set up and configure a notification process that delivers notifications to specific recipients after a defined event occurs. CA APM provides email notification processes with the product. These processes are delivered in files that are included on the product installation media. You import the files into CA Process Automation and specify process parameters in CA Process Automation and CA APM.

CA Asset Portfolio Management Architecture

The following figure shows the architecture for CA Asset Portfolio Management:



How to Install CA APM

This article describes the process of installing the CA APM

- Step 1: Verify the Installation Prerequisites and Checklist (see page 304)
- Step 2: Install CA APM (see page 309)
- Step 3: Upgrade to JRE 1.8.0_45 (see page 312)
- Step 4 (Optional): Update the Apache Tomcat Configuration File (see page 314)
- Step 5: Start the Services (see page 314)
- Step 6: Start the Web Interface (see page 315)
- Step 7: Verify the Installation (see page 317)

- Step 8 (Optional): Secure Network Communication Configuration (see page 318)
- Step 9: Configure Product Components (see page 319)

Tip! Before you install, ensure that you have performed the prerequisite tasks that are described in Step 1: Verify the Installation Prerequisites and Checklist (see page 304)

Step 1: Verify the Installation Prerequisites and Checklist

We recommend that you complete the prerequisites and checklist before you proceed with the installation and setup of CA APM.

- Verifying System Requirements (see page 304)
  - Hardware Requirements (see page 304)
  - Software Requirements (see page 305)
- Perform the Pre-Installation Tasks (see page 306)
  - Verify the Internet Information Services Installation (see page 306)
  - Remove CA iTechnology iGateway (see page 306)
  - Install Pentaho Data Integration (Kettle) (see page 307)

Verifying System Requirements

Ensure that your computer meets the requirements that are described in this topic.

Hardware Requirements

The following hardware requirements assume that you have between 80 and 100 concurrent users. For assistance with deployment architectures exceeding 100 concurrent users, contact CA Support (http://www.ca.com/us/support.aspx).

Component	Web Server and Application Server	Your Entry
Processor	3 GHz (dual core processor)	
RAM	8 GB	
Free Disk Space	5 GB	
Hard Drive Space	--	

Component	Database Server	Your Entry
Processor	3 GHz (dual core processor)	
RAM	8 GB	
Free Disk Space	--	
Hard Drive Space	4 GB	

Important! CA APM has time-sensitive processes. Verify that all servers are set to their correct date and time with their respective time zones.

Software Requirements

Component	Version	Comments	Your Entry
Java Runtime Environment (JRE)	1.7 (32-bit)		
CA EEM		Install CA EEM (see page 283) 12.51 CR02 using the CA Service Management Installation Media or upgraded an earlier installed version of CA EEM to CA EEM 12.51 CR02.	
JDBC Drivers			
Microsoft SQL or Oracle database server			
Internet Information Server (IIS)	7.5	Install IIS (see page 304)for CA SAM implementation.	
Microsoft .NET Framework	4.0		
Microsoft .NET Feature 3.5 for Windows Server 2012			
Windows Installer	5.0		
Microsoft Web Services Enhancements (WSE)	3.0		
CA Software Asset Manager		Download CA SAM from CA Support (http://www.ca.com/us/support/ca-support-online/product-content/recommended-reading/technical-document-index/ca-software-asset-manager-solutions-patches-catalogs-index.aspx). Required to manage software assets.	
CA SCM		CA SCM (and any cumulative releases) before installing CA APM to integrate CA SCM Release 12.6 with CA Asset Portfolio Management.	
Pentaho Data Integration (Kettle)	4.4	**(Optional)** Required if you are migrating from UAPM 11.3.4 to CA Asset Portfolio Management 14.1	
CA Business Intelligence		**(Optional)** Install CA Business Intelligence (see page 285) to configure reports.	

Component	Version	Comments	Your Entry
CA Process Automation		**(Optional)** Install CA Process Automation (see page 292) for event notification processing.	

Review the Supportability Matrix (see page 119) to understand the supported versions.

Perform the Pre-Installation Tasks

Perform the following pre-installation tasks to prepare the server for CA APM installation.

Verify the Internet Information Services Installation

Before you install CA APM, verify that Internet Information Services (IIS) is installed on all application and web servers. If the service is not on a server, add the service before you begin the installation.

Follow these steps:

1. For each application and web server, log in to the server.
2. Open the Control Panel (Administrative Tools, Services).
3. Verify that the IIS Admin service is on the server.

Install IIS version 7.5

1. From Server Manager, select Roles.
2. In the Roles Summary area, click Add Roles and click Next.
   The Select Server Roles dialog appears.
3. Select Application Server from the Roles list and click Next twice.
   The Select Role Services dialog for the Application Server role appears.
4. Select Web Server (IIS) Support and, under Windows Process Activation Service Support, select HTTP Activation.
5. If you are prompted to install more role services and features, click Add Required Role Services and click Next twice.
6. Verify that the summary of selections is correct and click Install.
7. Click Close after the installation completes.

Remove CA iTechnology iGateway

CA iTechnology iGateway, which is installed with CA EEM, is a shared component that various CA Technologies products use. CAiTechnologyiGatewayis a web server that sends requests and receives replies using the http protocol. CAiTechnologyiGatewaycan be installed with other products also.

If CA iTechnology iGateway exists on the computer where you are installing CA EEM, determine if it is 32-bit or 64-bit. If CAiTechnologyiGatewayand your CA EEM 12.51 server are both 32-bit or both 64-bit, no action is necessary. However, if the two products do not match (for example, one is 32-bit and the other is 64-bit), remove CA iTechnologyiGatewayand start the CA EEM installation. The correct version ofCA iTechnology iGatewayis installed when you complete the CA EEM installation.

Note: Various CA Technologies products or components install the 64-bit version of CA iTechnology iGateway, including the 64-bit CA Technologies eTrustITM agent.

Follow these steps:

1. On the computer where you are installing CA EEM, remove CA iTechnology iGateway.

   Note: To uninstall CA iTechnology iGateway successfully, first uninstall all products that are dependent on CA iTechnology iGateway.

   a. Open the Control Panel. Double-click Add or Remove Programs.
   Select CAiTechnologyiGateway and click Remove.

2. Remove theiGatewayandiTechnologyregistry key folders from the following location:

   `HKEY_localmachine\SOFTWARE\ComputerAssociates\`

3. Delete the IGW_LOC environment variable.

   a. From the Start menu, right-click My Computer and select Properties. Click the Advanced tab.
   Click Environment Variables. Select IGW_LOC in the System variables list, click Delete, and click OK.

4. Restart the computer.

5. Install CA Asset Portfolio Management.

6. When the CA Asset Portfolio Management installation is complete, reinstall the uninstalled componentsonthe computer where CA EEM is installed.

   Note: We do not recommend the installation of the CA Asset Portfolio Management components, except the Management Database, on a 64-bit computer that hosts a 64-bit Oracle database server.

Install Pentaho Data Integration (Kettle)

Install Pentaho Data Integration (Kettle) on the local computer where you install CA APM. Kettle is required only if you are upgrading from Release 11.3.4 to Release 14.1 or if you previously upgraded from Release 11.3.4 to Release 12.9.

Note: You can install Kettle before or after installing CA APM. However, we recommend that you install Kettle before you install CA APM.

Follow these steps:

1. Log in as the administrator to the computer where you are installing CA APM.
2. Download Kettle from the CA Support website and install Kettle on the server where you install CA APM Release 12.9.
    a. Click the following link (ftp://ftp.ca.com/pub/ca_itam/ca_apm/apm12_8/pentaho-kettle-4.4.0.zip)
    b. Savepentaho-kettle-4.4.0.zip in the desired directory.

       Example: C:\Program Files (x86)\CA\ITAM\
    c. Extract the contents ofpentaho-kettle-4.4.0.zip.

       A new folder that is named Kettle is created. Note the path of the folder.
3. Create an environment variable for Kettle by completing these steps.
    a. Click Start, Run, and type sysdm.cpl to access System Properties.
    b. Click the Advanced tab.
    c. Click Environment Variables.
    d. Click New in the System variables section and enter the following details:
       Variable Name
       KETTLE_HOME
       Variable value
       Path of the Kettle folder.

       Note: Ensure that the path is set to the parent folder that contains the “data-integration” folder, for example, C:\Program Files (x86)\CA\ITAM\Kettle.
    e. Click OK and exit System Properties.

Step 2: Install CA APM

Launch the CA Service Management Installer (see page 296) and complete the following steps to install CA APM:

Follow these steps:

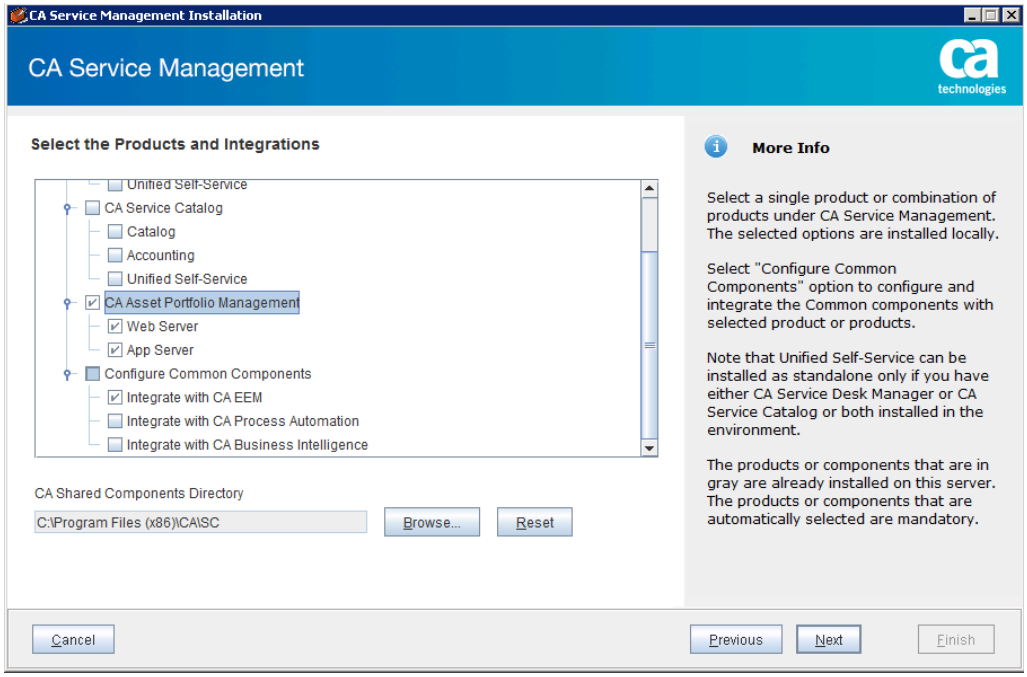
1. Select a language from the **Language Selection** screen.
   The installer provides additional information about the selected options on the right pane.

2. Accept the license agreement.

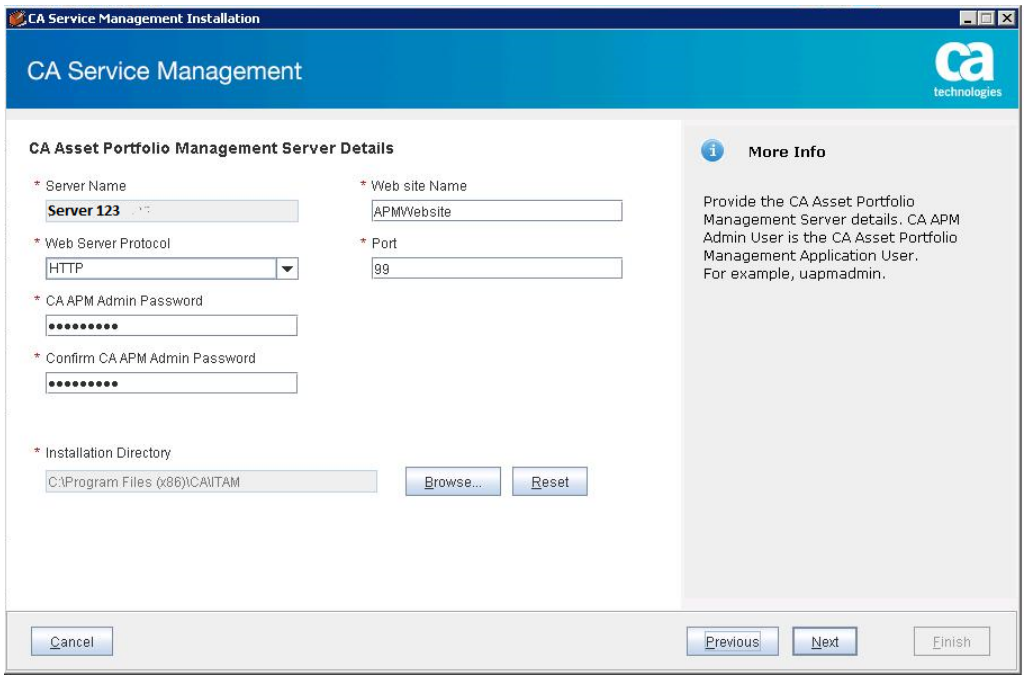
3. Enter the database information correctly.

> **Note:** Verify that you are providing a valid tablespace path if you have an Oracle database. The database installation fails if this path is invalid. The following path is an example of a valid Oracle tablespace path: C:\app\Administrator\oradata\Oracle_Service_Name.

4. Select **CA Asset Portfolio Management** from **Select the Products and Integrations** screen.

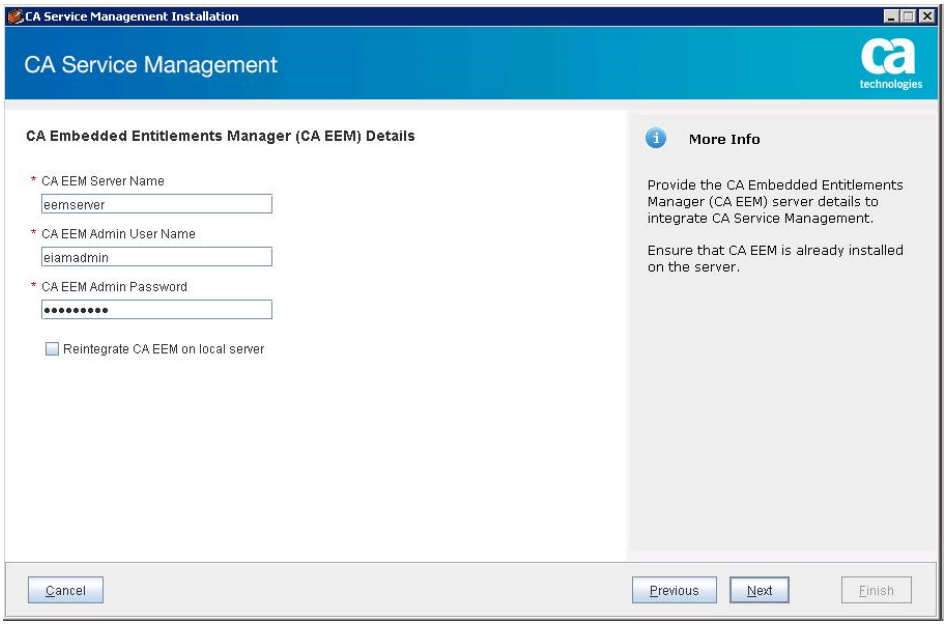


5. Provide the CA Asset Portfolio Management Server Details:



6. Select the Configure Common Components to integrate CA Asset Portfolio Management with CA EEM, CA Process Automation, or CA Business Intelligence.

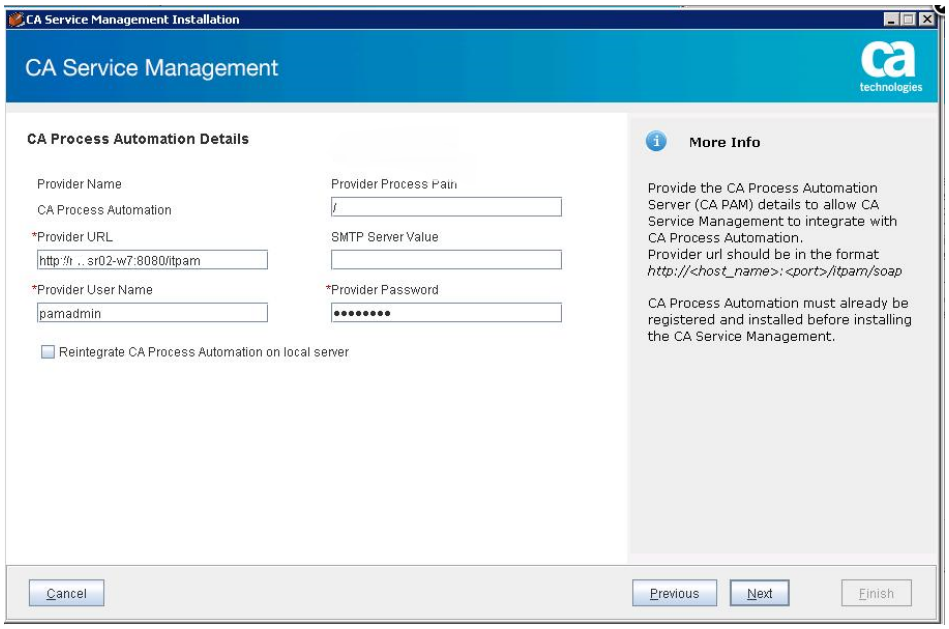
    a. Providee the CA EEM server details for authentication and authorization. For more information, see Install CA EEM (see page 283)

    CA Embedded Entitlements Manager (CA EEM) Details

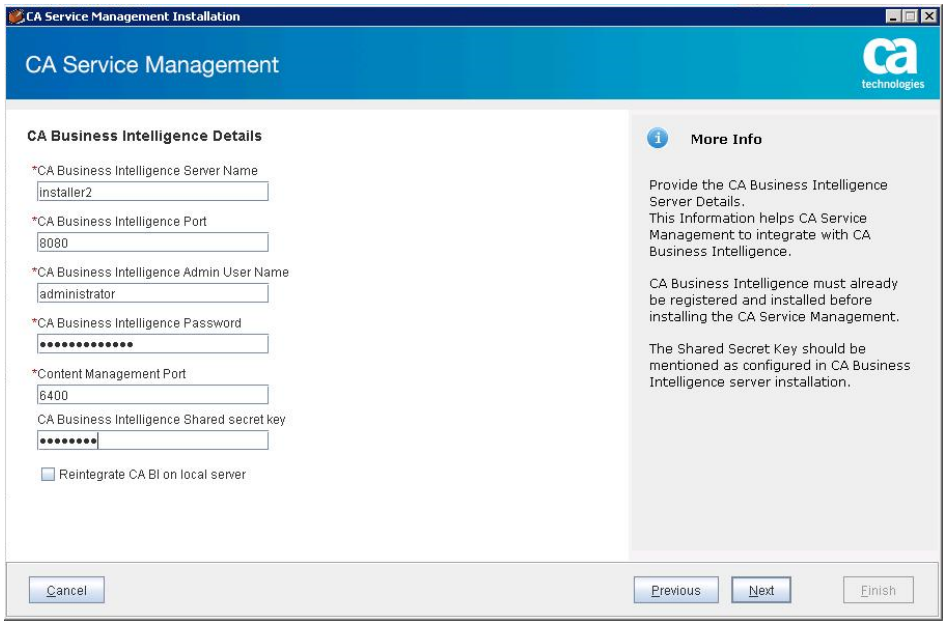
    Click **Next**.

    b. Integrate with CA Process Automation for event notification processing. For more information, see Install the CA Process Automation. (see page 292)



Click **Next**.

c. (Optional step). Install CA Business Intelligence for generating and viewing reports.



CA Business Intelligence Details

Note: In a web farm setup, the CA Business Intelligence and CA EEM panels do not appear if these common components are already installed on one of the servers in the web farm.

Click **Next**.

7. Review the Installation Progress Screen. Click **Install** to begin installation.

8. After the installation is complete, click **Finish**.

Step 3: Upgrade to JRE 1.8.0_45

This article describes the process of upgrading to JRE 1.8.0_45 to successfully implement CA IT Asset Manager.

- Upgrade CA CASM JRE to JRE 8 (see page 312)
- Upgrade AMS JRE7 to JRE8 (see page 313)

Upgrade CA CASM JRE to JRE 8

Follow these steps:

1. Stop the CA CASM service.

2. Navigate to http://tomcat.apache.org (http://tomcat.apache.org/) to download Tomcat 8.0.21. Extract the contents and rename the folder to Tomcat.

3. Navigate to http://www.oracle.com/technetwork/java/javase/downloads to download JRE 8u45.

4. Install JRE8u45 in a temporary location.

5. Copy the Tomcat and JRE 8 folders from the temporary location.

6. Navigate to CASM installation folder and backup the existing Tomcat and JRE folders.

7. Paste the folders that you copied in step 5.

8. Rename the “JRE 8” folder to “JRE”.

9. From the Tomcat backup, copy the following folders to the new Tomcat folder:

   - common
   - server
   - shared
   - webapps/balancer
   - webapps/casm

10. Navigate to SharedComponents\AMS, copy “AMSService.bat” to CASM folder and rename it to “CASMService.bat”

11. Edit “CASMService.bat” file to set JRE_HOME variable to point to JRE.

12. Open the command prompt, navigate to SharedComponents, CASM and execute the following command:

    ```
    CASMService install <service name>
    ```

    For Example:

    ```
    CASMService install CASM
    ```

13. Navigate to new Tomcat, conf.

14. Open server.xml and change the default port 8080 to existing port.

15. Start the service.

16. Delete the old service “CA CASM”.

Upgrade AMS JRE7 to JRE8

Follow these steps:

1. Stop the AMS service “Apache Tomcat 7.0 AMS”

2. Navigate to http://tomcat.apache.org (http://tomcat.apache.org/) to download Tomcat 8.0.21. Extract the contents and rename the folder to Tomcat.

3. Navigate to http://www.oracle.com/technetwork/java/javase/downloads to download JRE 8u45.

4. Install JRE8u45 in a temporary location.

5. Copy the Tomcat and JRE 8 folders from the temporary location.

6. Navigate to SharedComponents\AMS (AMS Installation folder) and backup the existing Tomcat and JRE 7 folders.

7. Paste the Tomcat and JRE8 folders that you copied in step 5.

8. From the Tomcat backup, navigate to webapps, copy the AMS folder, and paste it in the new Tomcat – webapps folder.

9. Navigate to SharedComponents\AMS, and edit the "AMSService.bat" to set JRE_HOME variable to point to JRE 8.

10. Open the command prompt, navigate to SharedComponents\AMS and execute the following command:

    ```
    AMSService install <service name>
    ```

    For Example:

    ```
    AMSService install AMS
    ```

11. To configure the port number in the server.xml, navigate to new Tomcat, conf.
12. Open server.xml and change the default port 8080 to existing port.
13. Start the service.
14. Delete the old service “Apache Tomcat 7.0 AMS”.

Step 4 (Optional): Update the Apache Tomcat Configuration File

This step is required only when you want to change the AMS port. The Common Asset Viewer lets you view discovered and owned data for an asset that has been linked through reconciliation. This data includes system configuration, operating system, system devices, and file systems. The Common Asset Viewer requires the Apache Tomcat server, which is included with the CA APM installation. You first update the port in the Apache Tomcat configuration file. Then, you change the port in the product (Administration tab, System Configuration, Common Asset Viewer).

Note: The Tomcat port number for CA APM defaults to 9080. If another product that is integrated with CA APM uses this port number, change the port number in CA APM so that you do not have a conflict.

Follow these steps:

1. On the application server where the Common Asset Viewer is installed, navigate to one of the following folders, depending on your server:
   C:\Program Files\CA\SC\AMS\Tomcat\conf (for 32-bit operating systems)
   C:\Program Files (x86)\CA\SC\AMS\Tomcat\conf (for 64-bit operating systems)
2. Select and open the server.xml file.
3. Navigate to the following section of the server.xml file:
   <Connector port="9080" protocol="HTTP/1.1"connectionTimeout="20000" redirectPort="
   8443" />
4. Update the Tomcat port number with the same number that CA APM uses (Administration tab, System Configuration, Common Asset Viewer).
5. Save the server.xml file.

Step 5: Start the Services

After the installation is complete, start all services.

Note: In certain circumstances, after the product installation, you can receive a message that CA Business Intelligence was installed but requires you to restart the web server. Restart the web server before verifying that the CA Business Intelligence services are started.

Follow these steps:

1. Open the Control Panel (for example, click Start, Settings, Control Panel).
2. Double-click Administrative Tools.
3. Double-click Services.
4. Locate and start each of the following services:

- Apache Tomcat 7.0 Application Management Suite (AMS) Service
- CA Asset Portfolio Management - Data Importer Engine
- CA Asset Portfolio Management - Event Service
- CA Asset Portfolio Management - Export Service
- CA Asset Portfolio Management - Registration Service
- CA Asset Portfolio Management - HW Reconciliation Engine
- CA Asset Portfolio Management - LDAP Import Service
- CA CASM

  Note: For performance reasons, we recommend that you do not start the CA CASM service when you do not use multi-tenancy.

- CA iTechnology iGateway 4.6

5. To verify CA Business Intelligence services with the Central Configuration Manager, select Start, Programs, BusinessObjects XI Release, BusinessObjects Enterprise, Central Configuration Manager. The Central Configuration Manager opens.
If any service is not started, right-click the service and select Start.

Step 6: Start the Web Interface

After the installation is complete, you can start the web interface to verify that CA APM is ready to use. After you verify that the web interface starts, provide all administrators with the URL and login credentials to log in and prepare the product for users. Administrators can then set up security, configure the user interface, set up hardware reconciliation, and, if necessary, configure the product components. After the administrators prepare the product, they can provide users with the URL and login credentials.

After you install IIS and ASP.NET on the computer where you plan to install CA APM, ensure that you register ASP.NET with IIS, before you start the web interface.

Follow these steps:

1. Depending on your Windows server, complete one of the following steps:

   - (On Windows Server 2008) Complete the following steps:

     a. In the command prompt, navigate to the appropriate Microsoft.NET framework folder. For example, C:\Windows\Microsoft.Net\Framework64\v4.0.30319 or C:\Windows\Microsoft.Net\Framework\v4.0.30319.

     b. Run the executable file, aspnet_regiis.exe/i
     ASP.NET is now registered with IIS.

   - (On Windows Server 2012) Complete the following steps:

     a. i. Open the Server Manager.

     ii. Under the Manage menu, select **Add Roles and Features**.
     The Add Roles and Features Wizard opens.

     iii. Follow the on-screen instructions and select the installation type and the destination server.

     iv. In the Select server roles pane, under **Roles**, expand **Application Server**, and select the appropriate ASP.NET version and click **Next**.

     v. Follow the on-screen instructions and complete the installation.

     ASP.NET is now registered with IIS.

2. Start the web interface using one of the following methods:

- Open a supported web browser and enter the appropriate URL in the following format:

  `http://servername:port/itam`

  - Replace servername and port with the name of the server and the port that are hosting the CA APM web servers.

Note: If the Internet Explorer browser security is set to high, a content warning message appears when you start the web interface. To avoid this message, add the web site to your trusted sites or lower your security settings.

- A Start menu shortcut is created on your web server that references the URL location. Click Start, Programs, CA, Asset Portfolio Management, Asset Portfolio Management.

  To log in to CA APM, enter the following default credentials:

- **User Name**
  uapmadmin
- **Password**
  uapmadmin

> **Note:** : If you changed the password during the installation, use the password that you created.

In some situations, a browser error or a user name error appears. You can resolve these errors by following the troubleshooting instructions in the message.

Step 7: Verify the Installation

After you have completed all installation procedures, you can verify that CA APM was installed successfully.

Follow these steps:

1. Log in to the servers where you installed CA APM.
2. (Windows Server 2008 or Windows Server 2012) From the Start menu, select Control Panel, Programs and Features.
3. Verify that the following component is available on all applicable servers:
   CA Asset Portfolio Management

   You have completed the installation verification.

> **Note:** If you backed up the Storage folder contents before installing, restore the contents now. Use the Storage folder contents that you copied and paste them into the following location:
>
> [ITAM Root Path]/Storage/

If you receive a prompt about folders that already exist, merge the folders.

Additional Products Installed

The following products are installed when you install CA APM:

- Common Asset Viewer
- CORA 12.5.0.34
- Common Administration for Service Management (CASM)

- Migration Toolkit

Step 8 (Optional): Secure Network Communication Configuration

After the installation is complete, configure CA APM for non-secure or secure network communication. For secure network communication (https), first configure IIS on the product servers to support the Secure Socket Layer (SSL) protocol. Then, set the CA APM configuration parameters for secure network communication.

Complete the following actions:

1. Configure IIS for secure network communication (see page 318).
2. Configure CA APM for secure network communication (see page 318).

Configure IIS for Secure Network Communication

Configure IIS on the product servers to support the Secure Socket Layer (SSL) protocol.

Follow these steps:

1. Launch the Internet Information Services (IIS) Manager on the CA APM web server.
2. Select Server Certificates.
3. Click Create Self-Signed Certificate and specify a certificate name.
4. Select the web site (on the left) where CA APM is installed (for example, Default Web Site).
5. Click Bindings under Actions on the right.
   The Site Bindings dialog opens.
6. Click Add.
7. Select https for the Type.
8. Specify the port and the SSL certificate name.
9. Perform these same steps on the CA APM application server.

Configure CA APM for Secure Network Communication

Configure CA APM on the product servers to support the Secure Socket Layer (SSL) protocol.

Follow these steps:

1. Log in to the product and navigate to Administration, System Configuration.
2. Click Web Server on the left.
3. Change the server protocol to https and click Save.
4. Click WCF Service on the left.

5. Change the server protocol to https and click Save.

6. Click Application Server on the left and select the Show Advanced Options check box to see all configuration parameters.

7. Change the server protocol to https.

8. Change the server port and the component server port to the port of the https protocol (by default, 443) and click Save.

9. Reset IIS on the web server and the application server.

You can now start the product web interface using secure network communication. Open a supported web browser and enter the following URL:

```
https://servername/ITAM/Pages/UserLogin.aspx
```

Replace *servername* with the name of the server that is hosting the CA APM web server.

Step 9: Configure Product Components

After installing CA APM, you can change the component configurations and configure additional product components. You can configure the following components:

- Recycle Settings in the Application Pool (see page 320)
- Database Server (see page 320)
- Web Server (see page 321)
- Application Server (see page 321)
- Hardware Reconciliation Engine (see page 322)
- CA EEM (see page 322)
- CA Business Intelligence (see page 322)
- CA Process Automation Manager (see page 322)
- Export Service (see page 322)
- Data Importer Engine Service (see page 322)
- Import Driver (see page 323)
- LDAP Data Import and Sync Service (see page 323)
- Storage Manager Service (see page 323)
- CA APM Registration Service (see page 323)
- Common Administration for Service Management (CASM) (see page 323)
- Event Service (see page 323)
- Common Asset Viewer (see page 324)
- WCF Service (see page 324)
- Software Asset Management (see page 324)
- CA Service Desk Manager (see page 325)

Follow these steps:

1. Log in to CA APM as the administrator.

2. Click Administration, System Configuration.

3. On the left, click the product component that you want to configure.

4. Configure the settings and click Save.

5. Recycle the settings in the application pool.
   For more information, see Recycle Settings in the Application Pool (see page 320).

6. Restart the services.
   For more information, see Start the Services (see page 314).

Note: You cannot configure the database server from the System Configuration page. Update the corresponding configuration files for any database server configuration settings.

For more information about changing the component configurations and adding servers, see Manage Product Components (see page 1585).

Recycle Settings in the Application Pool

After you configure a product component through System Configuration, recycle the settings in the Application Pool.

Follow these steps:

1. From the Start menu, open the Control Panel.

2. Double-click Administrative Tools and then double-click Internet Information Services (IIS) Manager.

3. In the Connections pane, expand the server name and click Application Pools.

4. In the Application Pools pane, select ITAM.

5. In the Actions Pane, click Stop and then click Start.

Database Server

The database server is a product component that hosts the Oracle or SQL Server database management system for CA APM. The CA MDB is installed on the database server. The application server, Hardware Reconciliation Engine, and other product components retrieve data from and store data in the CA MDB.

The following fields require explanation:

- **MS SQL Server Instance**
  Defines the name of the MS SQL Server instance that is being configured. Enter the instance name only when multiple SQL Server named instances exist. Leave the field blank if there is only one (default) instance.

Note: You can change the component configurations and configure additional components for your enterprise after you install the product. For more information about changing the component configurations and adding servers, see Managing Product Components (see page 1585).

Web Server

The web server is the main server that hosts the web application and builds the CA APM user interface. This server communicates with the user, the application server, and the database server.

The following fields require explanation:

Web Server or Load Balancer IP/Host

The CA APM installation, by default, sets this field to the web server host name.

- In a single web server environment, you can enter the web server host name, or the web server IP address.
- In a multiple web server environment, you can enter either the web server host name, or the IP address of the Load Balancer.

Note: The web server can be registered with a different name in the Domain Name System (DNS) than what is registered as the web server host name. In this situation, specify the different name in this field.

You can configure additional web server components after you install the product.

Application Server

The application server is the server that connects the database server and the web server for CA APM. The business and data access logic reside on the application server. To allow for scalability, the application server and web server are on two distinct servers.

You can have more than one application server. The Export Service component and the Storage Management Service component must be installed on one of the application servers, but not necessarily on the same server.

The following fields require explanation:

Application Server or Load Balancer IP/Host

The CA APM installation, by default, sets this field to the application server host name.

- In a single application server environment, you can enter the application server host name, or the application server IP address.

- In a multiple application server environment, you can enter either the application server host name, or the IP address of the Load Balancer.

The application server can be registered with a different name in the Domain Name System (DNS) than what is registered as the application server host name. In this situation, specify the different name in this field.

You can configure more application server components after you install the product.

Hardware Reconciliation Engine

The Hardware Reconciliation Engine is the service that matches discovered assets to their corresponding owned assets from different logical repositories. You can manage the assets based on your business practices. The Hardware Reconciliation Engine retrieves data from and stores the results in the CA MDB. You can install the Hardware Reconciliation Engine on one or more servers.

You can configure more Hardware Reconciliation Engine components after you install the product.

CA EEM

CA APM uses CA EEM for authentication. Other products that need CA EEM for authentication can use the same CA EEM server that CA APM uses.

- To manage security centrally for multiple CA Technologies products, specify the name, location, and login credentials for the existing CA EEM server.
- To manage CA APM security independently from other CA Technologies products, install CA EEM on any single application or web server other than the one where the existing CA EEM is installed.

CA Business Intelligence

CA Business Intelligence administers, monitors, and configures the reporting environment. CA APM uses CA Business Intelligence to integrate, analyze, and present information required for effective enterprise IT management.

For information about the access credentials and connection information that you enter for the CA Business Intelligence component, see How to Integrate CA APM and CA Business Intelligence.

CA Process Automation Manager

CA PAM can be integrated with CA Asset Portfolio Management to automate workflow business processes. For more information see Installing Common Components (see page 283).

Export Service

The Export Service exports data from CA APM and saves the results in formats such as a comma-separated value (CSV) file. To accomplish this task, the Export Service interacts with the Storage Manager Service so that you can specify where the exported files are stored.

Data Importer Engine Service

The Data Importer Engine Service imports bulk product information into the CA MDB through column and field mapping.

Import Driver

The Import Driver processes discovered hardware data exports from CA SAM. CA APM uses the discovered hardware data to link ownership and discovery data. CA APM exports ownership data back to CA SAM.

LDAP Data Import and Sync Service

The LDAP Data Import and Sync Service imports data into CA APM from CA EEM or external data sources (LDAP or CA SiteMinder). Install the LDAP Data Import and Sync Service on one of the Data Importer servers.

Storage Manager Service

The Storage Manager Service stores exported files, attachment files, data import data and map files, and log files for data import and mass change. If your current product release is any version of Release 12.6, 12.7, or 12.8, you must back up the contents of the Storage folder before you uninstall your current release. After you have completed the Release 12.9 installation, restore the contents of the folder.

CA APM Registration Service

The CA APM Registration Service consolidates individual CA APM CORA services into one main service. You can have installations of other CA Technologies products that also use the CORA API. The changes that you make to the CORA API in your CA APM environment do not affect the use of the CORA API by other CA Technologies products.

Common Administration for Service Management (CASM)

The Common Administration for Service Management (CASM) provides administrative functionality, such as multi-tenancy administration, to CA APM. Multi-tenancy is the ability for multiple independent tenants (and their users) to share a single implementation of CA APM.

Note: For more information about implementing multi-tenancy, see How to Implement Multi-Tenancy (see page 990).

Event Service

The Event Service manages the events and notifications process in CA APM. Events are important activities or data changes that you want to track and that you define in CA APM. After a defined event has occurred, notifications are sent to alert appropriate users and administrators about the event.

To perform the notification function, the Event Service interacts with a workflow provider (for example, CA Process Automation) using the Web Service. A workflow provider manages automated processes. If your workflow provider is CA Process Automation, you can specify the existing instance of CA Process Automation during the installation. You can also share CA Process Automation with CA Service Desk Manager and CA Service Catalog.

Common Asset Viewer

The Common Asset Viewer lets you view discovered and owned data for an asset that has been linked through reconciliation, including system configuration, operating system, system devices, and file systems. You can view this data on the Asset Details page by clicking the Owned Information or Discovered Information link.

The Common Asset Viewer requires the following components to install and execute successfully:

- Apache Tomcat server, which is included with the CA APM installation. The default value for the Apache Tomcat server port is 9080. You can change this value after the installation. You first update the port in the Apache Tomcat configuration file (see page 314). Then, you change the port in the product (Administration tab, System Configuration, Common Asset Viewer).

- Java Development Kit (JDK). Before you begin the CA APM installation, install the JDK on the application server on which you are installing the Common Asset Viewer.

After you install the Common Asset Viewer, the component is configured for non-secure network communication (http). You can configure the component for secure network communication (https) by first configuring the Apache Tomcat server (where the Common Asset Viewer is installed) to support the Secure Socket Layer (SSL) protocol. Then you need to change a setting for the Common Asset Viewer component in the web configuration file.

The Tomcat port number for CA APM defaults to 9080. If another product that is integrated with CA APM uses this port number, change the port number in CA APM so that you do not have a conflict.

WCF Service

The Windows Communications Foundation (WCF) service implements the web services in CA APM. The web services let you use a standards-based interface to build client applications that integrate with CA APM.

The web services let you create, search, update, copy, and delete CA APM objects from your external client application. Your assigned user role determines whether you have permission to access the web services in CA APM. Your role also restricts the objects and data (classes and attributes) that you can view or modify.

Specify the server name for the WCF Service component. You can modify the WCF Service protocol setting. You can change the configuration of the WCF Service component after you install the product.

Software Asset Management

The Software Asset Management component allows you to enable software asset management capabilities through CA SAM. If you implement both CA APM and CA SAM, you can coordinate the management of both hardware and software assets in your organization. CA APM maintains hardware asset data and CA SAM maintains software asset and license data. Common data that both products require is shared.

The product installation does not configure the Software Asset Management component. Configure this component through System Configuration after you install the product.

Note: You can change the component configurations and configure additional components for your enterprise after you install the product. For more information about changing the component configurations and adding servers, see Managing Product Components (see page 1585).

CA Service Desk Manager

CA Service Desk Manager component is used for integrating CA APM and CA SDM. Refer to Integrating CA ITAM and CA Service Desk Manager (see page 3251).

Migrate CA APM Release 11.3.4 to the Current Release

To migrate CA APM data, perform these steps:

1. Review the Prerequisites (see page 328)
2. Start the CA APM Migration Toolkit (see page 332)
3. Run the Pre-Migration Reports (see page 332)
4. Use the pre-migration report data for reference and corrective action (see page 339)
5. Specify the Duplicate Asset Rename Configuration (see page 344)
6. Run the Migration Utility (see page 345)
7. Start the CA APM Web Interface (see page 351)
8. Run the Post-Migration Reports for Manual Migration (see page 368)
9. Perform Manual Migrations (see page 351)
10. Perform Post-Migration Verification (see page 367)

As a system administrator, you perform the data migration when you want to move CA APM data from Release 11.3.4 to the current release . After you install the current release of CA APM, the CA Management Database (CA MDB) structures are upgraded and you are prompted to migrate your data.

Note: Use the current release of CA APM to migrate objects that were not migrated with Release 14.1. These objects are costs and payments extensions and audits, custom relationships and audits, and relationship extensions and audits. With this release, all relationships are migrated, including custom relationships and relationships that were not product-provided. If you previously migrated your data from Release 11.3.4, you can migrate the data for just these objects. You do not need to perform the complete data migration again.

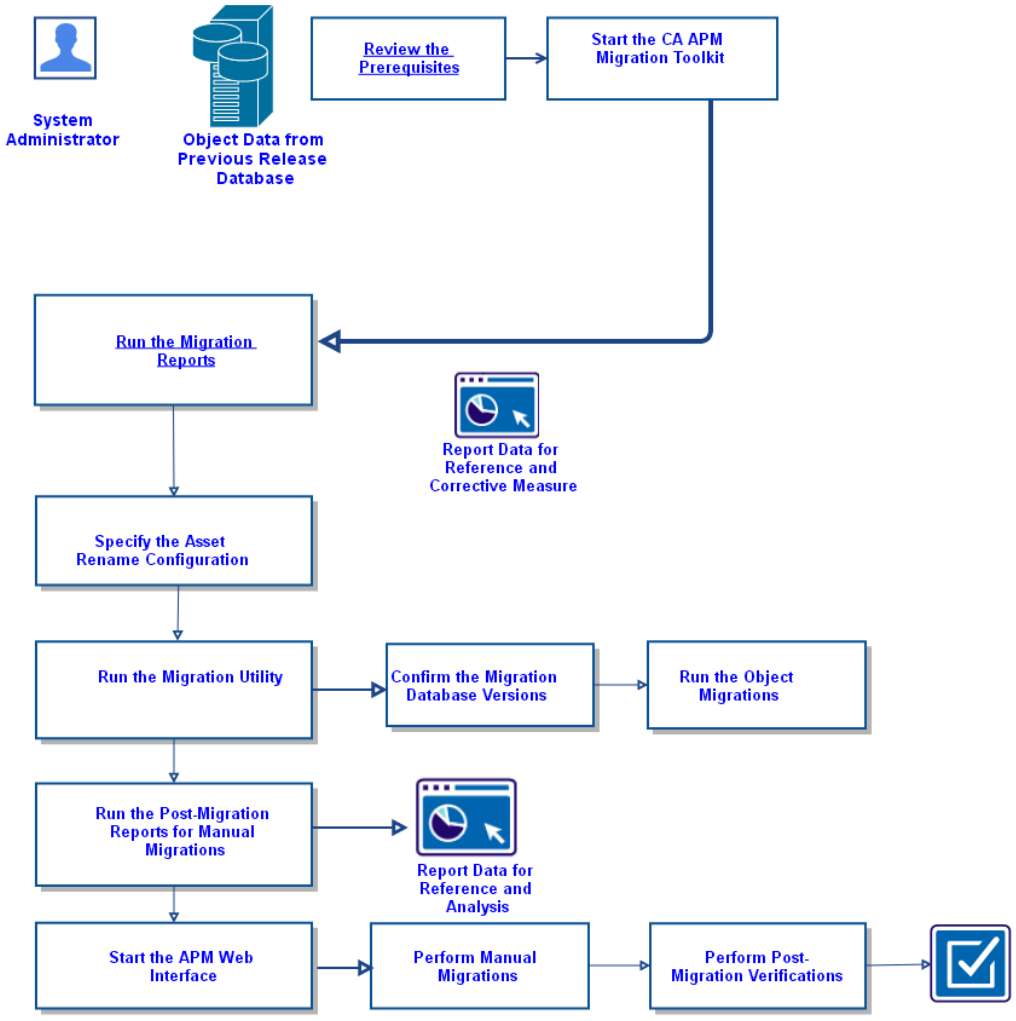
Installing the upgrade and migrating your data are separate processes:

- **Upgrade**: Updates the application and database structures to a newer version.
- **Migrate**. Transforms or moves the data from previous database structures to new database structures, which were created during the upgrade.

The CA APM Migration Toolkit contains the following tools to assist you with migrating your data from Release 11.3.4 database structures to the current release database structures:

- **Migration Documentation**: Provides the instructions for generating the migration reports, running the Migration Utility, and manually migrating objects.
- **Migration Reporting**: Generates reports that help you during the migration process. Generate the pre-migration reports (see page 332) *before* you run the Migration Utility (see page 345) to avoid potential problems during the migration. You can generate the post-migration reports (see page 368) *after* you run the Migration Utility. The post-migration reports help you manually migrate legacy database structures that cannot be migrated using the Migration Utility.
- **Duplicate Asset Name Configurator**: Specifies the renaming configuration to apply to duplicate Asset Names.
- **Migration Utility**: Provides automated steps to move the selected objects in your legacy database structures to new database structures.

The following diagram illustrates how a system administrator migrates data.



Example: Migrate CA APM Data from Release 11.3.4 to Current Release

Miriam is the CA APM system administrator at Document Management Company. She wants to upgrade CA APM Release 11.3.4 to the current release and migrate the data from legacy data structures to the upgraded data structures. Miriam reviews the prerequisites to start the migration and upgrades to the new release.

Miriam starts the CA APM Migration Toolkit. First, she generates and reviews the pre-migration reports. The reports help identify objects that she has to correct in the legacy data structures before successfully running the Migration Utility. She sets some of the reports aside to use later to configure new names for assets that have the same name and to perform manual migrations.

After Miriam makes the corrections to the legacy data structures, she reviews the Duplicate Asset Name Report to identify non-unique Asset Names. Miriam opens the Duplicate Asset Name Configurator and selects a renaming configuration for duplicate Asset Names. These assets are renamed when Miriam runs the Migration Utility.

Miriam opens the Migration Utility. She tests the database connection, which confirms that the correct CA APM legacy database version is being migrated to the correct new release database version.

Miriam selects the objects to migrate and runs the Migration Utility. She monitors the migration process by reading the progress and status messages. When all of the objects are migrated, the Audit History object becomes available for migration. She selects the Audit History object and reruns the Migration Utility.

When the Migration Utility process finishes, Miriam generates the post-migration reports. The reports specify the data that was successfully migrated and the data that was not migrated. Miriam has to migrate manually the data that was not migrated.

Manual migrations are performed using the upgraded CA APM current release web interface. Miriam starts the web interface. She performs the manual migrations using the post-migration report information. She verifies the migrated data to complete the migration process.

Review the Migration Prerequisites

This article contains the following topics:

Verify that you have completed these prerequisites in the following order to ensure that you can successfully migrate the data:

Note: Many of the migration prerequisites are completed while installing CA APM.

1. Review the following information:
   - Known Issues available on the Release Information (see page 69).
   - Relationship Differences Between Release 11.3.4 and the Current Release (see page 328).
2. Ensure that the current Release 11.3.4 patch level is cumulative patch 14 or higher. If the current patch level is unknown, or not cumulative patch 14 or higher, download and apply the latest CA APM Release 11.3.4 cumulative patch from the CA Support website.
3. Stop the following services and the scheduled tasks for CA APM and other integrated Service Management products:
   - CA Unicenter Asset Portfolio Management (CA APM)
     - CA APM Cache Service
     - CA APM Notification Service

- Automated reconciliation tasks
- CA Service Catalog Release 12.8 and 12.9
  - CA Service Catalog
  - CA Service Accounting
- CA Service Catalog Release 12.7
  - CA Service Accounting
  - CA Service Fulfillment
  - CA Service Repository Agent
  - CA Service View
- CA Service Desk Manager
  - CA Service Desk Manager Server
- CA Client Automation
  - For CA Client Automation Enterprise Managers and Domain Managers that directly share the CA MDB being migrated, stop the CA Client Automation Service using *caf* stop.
  - For other servers running supplemental Engine processes against the CA MDB being migrated, stop the CA Client Automation Service using *caf* stop.
  - For any Engine processes executing the Database Synchronization tasks to the CA MDB being migrated, stop the Database Synchronization jobs using the DSM Explorer.
  - Stop the Engine replication tasks to the Enterprise using the DSM Explorer for each CA Client Automation Domain Manager that reports to the Enterprise.

4. Back up the CA APM Release 11.3.4 database.
5. Locate the CA Migration Health Check Utility in the Health Check Utility folder on the CA APM installation media. Execute the utility on the CA APM Release 11.3.4 database.

   Important! For information about running the utility, see the *CA Migration Health Check Utility User Guide*, which is available on the installation media.

6. Review the Microsoft SQL Server Transaction Log Sequence settings for the CA MDB, and ensure that the settings are positioned for bulk loading. Complete the following steps to locate the information:

a. In a web browser, open the Microsoft website (http://www.microsoft.com) and search for "Transaction Log Management".

b. Follow the instructions in the article.

7. Install CA Service Management 14.1 against the Release 11.3.4 database.

> **Note:** If you previously migrated Release 11.3.4 data to Release current release, you need to perform some steps to retain the migration status of the migrated objects. For more information about how to retain the migration status, see Installation Planning.

8. Verify that no current release services are running. These services can still be running if you exited the CA APM Migration Toolkit before you ran the Data Migration Utility or generated the reports for manual migrations.

Relationship Differences Between CA APM Release 11.3.4 and the Current Release

CA APM Release 11.3.4 includes product-provided relationships and allows you to add new custom relationships. The support for relationships has changed in the current release.

Relationships that Are not Product Provided in CA APM

The following relationships and associated links that are provided in Release 11.3.4 are not product provided in the current release. However, these relationships are migrated to custom relationships in the current release:

- Activity Summary
- Contacts (Budget manager, Supported by, User)
- Dependencies (Depends on)
- Product Evolution (Evolved into)
- Product Upgrade (Upgraded to)
- User Allocation (Allocated to)
- SW Allocation (Allocated on)

Product-Provided Relationships in CA APM

The following Release 11.3.4 relationships are product provided in CA APM:

- Asset Entitlement (Licensed to)
- Company Acquisition (Acquired By)

- Company Entitlement (Licensed to)
- Contact Entitlement (Licensed to)
- Governing Document (Governed by)
- Image Partitions (Partitioned CPU)
- Legal Amendment (Amends)
- Location Entitlement (Licensed to)
- HW Asset Configuration (Generic component, Specific component)
- HW Model Configuration (Generic component)

The data structures to store the relationship information have changed. To move the relationship information from Release 11.3.4 to the current release, the Migration Utility must identify the relationships by Relationship Template name and Relationship Template Link name.

What You Must Do: Before you run the Migration Utility, change the modified names in Relationship Template or Relationship Template Link to the values in the original Release 11.3.4.

User Interface Changes

In CA APM Release 11.3.4, relationships and links are displayed and modified in separate sections in the user interface. In the current release, relationships and links are combined into a single entity that is displayed and modified in the same section in the user interface.

Some of the menu items for relationship names in the current release are different from Release 11.3.4. The following chart lists each Release 11.3.4 relationship and its associated current release relationship menu item. Some relationship menu items have a different label when viewing the relationship from the reverse direction. For example, the Company Entitlement relationship is displayed as Company Allocation when viewed from the software asset and Software Allocation when viewed from the company.

CA APM Release 11.3.4 Relationship	CA APM Release 14.1 Entity	CA APMRelease 14.1 Relationship
Asset Entitlement	Asset (software)	Asset Allocation
Asset Entitlement	Asset (hardware)	Software Allocation
Company Acquisition	Company	Company Acquisition
Company Entitlement	Asset (software)	Company Allocation
Company Entitlement	Company	Software Allocation
Contact Entitlement	Asset (software)	Contact Allocation
Contact Entitlement	Contact	Software Allocation

CA APM Release 11.3.4 Relationship	CA APM Release 14.1 Entity	CA APMRelease 14.1 Relationship
Governing Document	Legal Document	Governing Legal Document
Image Partitions	Asset	Image Partitions
Legal Amendment	Legal Document	Legal Amendment
Location Entitlement	Asset (software)	Location Allocation
Location Entitlement	Location	Software Allocation
HW Asset Configuration (Generic component)	Asset	Model Configuration
HW Asset Configuration (Specific component)	Asset	Asset Configuration
HW Model Configuration	Model	Model Configuration

Start the Migration Toolkit

During the upgrade of Release 11.3.4 to Release 14.1, the CA APM Migration Toolkit is installed on the same computer that is performing the upgrade. We recommend that you migrate your CA MDB data to the new release data structures immediately after the upgrade is complete.

Note: If multiple servers are deployed in your environment, the Migration Utility will be installed only on the first Server.

Start the CA APM Migration Toolkit on the same computer where you performed the upgrade.

Follow these steps:

- Click Start, All Programs, CA, Asset Portfolio Management, CA APM Migration Toolkit.

Run the Pre-Migration Reports before Migrating the Data

This article contains the following topics:

- Task Add Asset Report (see page 339)
- Customized Search Report (see page 339)
- Translation List Obsolete Report (see page 339)
- Translation List Unconverted Report (see page 339)

Before you migrate the CA MDB, you run the pre-migration reports. The pre-migration reports identify the following types of data:

- Data that can cause problems during data migration. You correct the data in the CA MDB *before* you run the Migration Utility. For example, if you renamed a relationship template that was provided with Release 11.3.4, this change could cause a problem during the migration of relationships. The Relationship Report identifies the renamed templates, which you change back to the original product-provided template names, before migration.

- Data that requires analysis for migration configuration decisions.

- Data that is not migrated with the Migration Utility, but can be migrated manually with updated product features. You reference this data during manual migration, *after* you run the Migration Utility. You must capture the data in these reports before you migrate your legacy data, because this data is not migrated to the current release. database structures. You save these reports and reference their information later, during manual migration for the current release.

- Data that is supported in Release 11.3.4 but is not supported in the current release. You cannot migrate this data with the Migration Utility or add it using the current release version. These reports identify unsupported data and provide legacy reference information.

Follow these steps:

1. On the CA APM Migration Toolkit main window, click Migration Reporting.
   The following Pre-Migration Reports area check boxes are selected:

   - Custom Index
   - Duplicate Asset Name
   - Reconciliation
   - Relationships

   Note: If you do not want to generate all reports, select only those report types that you want.

2. In the Report Output Folder area, click Browse and select the output folder where you want to save the reports.

3. Click Generate Reports.
   The status messages appear in the Messages area to help you monitor the report generation process.
   You are prompted to open the report output folder to view the reports.

4. Click Yes.
   Windows Explorer opens. The Reporting tool creates a folder for each report check box that you selected previously.

5. Navigate to, and open, a report folder.
   The reports appear in comma-separated value (CSV) format.

6. Right-click a report and select Open with, Excel, to open and view the report in a table format.
   The report data (see page 334) is presented in a table format. The table headings are in the first row.

   Note: You can click open the report to view in a text editor in CSV format.

Pre-Migration Report Data for Reference and Corrective Action

The Reporting tool generates reports in CSV format that you can open with a text editor. The report field names and field values are separated with commas. You can also open a report with Excel, which presents the data in a table format. When you open a report with Excel, the field names are the column headings, and the field values appear in the rows below the headings.

The following pre-migration reports give you information about data that you must change in the CA MDB *before* migration. The related objects can then be migrated successfully to the current release CA MDB data structures.

- Custom Index Report
- Relationship Report

The following reports identify data that you analyze for migration configuration decisions:

- Duplicate Asset Name Report
- Reconciliation Report:
  - Main Translation List Query Report

The following pre-migration reports identify data that you use *after* you run the Migration Utility, when you perform manual migrations. Save these reports and reference them during manual migration.

- Reconciliation Reports:
  - Main Task Query Report
  - Task Add Asset Report
  - Customized Search Report

The following reports identify data that is not supported in the current release and that provide legacy reference information:

- Reconciliation Reports:
  - Translation List Obsolete Report
  - Translation List Unconverted Report

Custom Index Report

The Custom Index Report identifies indexes that were added to fields in Release 11.3.4 (or previous releases) for customization. These indexes can create performance issues in the current release version. We recommend that you remove custom indexes from your database. The report provides SQL statements that you run to remove the custom indexes.

Remove Custom Indexes from Database

We recommend that you remove custom indexes from your database to avoid performance issues. Remove the indexes *before* you run the Migration Utility. The Custom Index Report provides the information that you use to remove the custom indexes.

Follow these steps:

1. Locate the Custom Index Report.
2. Copy the SQL statements from the Drop SQL column on the report.

   Note: Delete the quotation marks at the beginning and end of the statements.

3. Paste the SQL statements to your preferred tool, for example, Microsoft SQL Server Management Studio and Oracle SQL Developer, and run the statements.
   The following items are removed:
   - Custom indexes
   - Index definitions from the arg_index_member table
   - Index information from the arg_index_def table

Relationship Report

The Relationship Report identifies the relationship templates that were renamed from the original product-provided Release 11.3.4 names. Change this data in the CA MDB *before* migration.

The tool generates the Relationship Report in different languages. Use the appropriate report for the language that the Release 11.3.4 was configured to.

The report shows the following status for the relationship template or the relationship template link:

- **Customized**
  Indicates that the relationship templates or relationship template links are added or renamed by the user in Release 11.3.4.

  - If the relationship was added in Release 11.3.4, it is not a product-provided relationship in the current release. However, it is migrated to a custom relationship.

  - If the relationship is product provided in Release 11.3.4 and in the current release, you can migrate the relationship to the product-provided relationship in the current release. First, rename the relationship templates or relationship template links to their original values.

- **Migrated by Migration Utility**
  Indicates that the relationship templates or the relationship template links are supported in the current release and will be migrated by the utility.

- **No Longer Supported**
  Indicates the relationship templates or relationship template links that are not product provided in the current release. The Migration Utility migrates these relationships to custom relationships.

- **Not Found**
  Indicates the product-provided relationship templates or relationship template links in Release 11.3.4 that are not found in the database of the user. If the relationship templates or relationship template links were renamed and are product-provided in the current release, rename the relationship templates or relationship template links to their original values to migrate the relationship to the current release.

- **Rename to migrate**
  Indicates the renamed relationship templates or relationship template links in Release 11.3.4 that you have to change to the original name before migrating.

Complete the following actions if you want to include the renamed product-provided Relationship Templates in the migration:

- Change the renamed Relationship Template to the original product-provided name.

- Change the renamed Relationship Template Link to the original product-provided name.

Change the Renamed Relationship Template to the Original Product-Provided Name

Before you run the Migration Utility, you change the renamed Relationship Template names to the original product-provided Relationship Template names from Release 11.3.4.

You execute a SQL statement to change the Relationship Template Name. Perform these steps for each entry in the report with status ‘Rename to migrate’ and a value that is specified under ‘Relationship Template Rename’.

Follow these steps:

1. Execute the following SQL statement from your preferred tool (for example, Microsoft SQL Server Management Studio or Oracle SQL Developer):

> **Note:** The brackets and the text within the brackets are placeholders. The placeholder names represent the column names on the Relationship Report.

```
UPDATE arg_actiondf
SET adtext = '{Relationship Template Rename}'
WHERE adtext = '{Relationship Template Name}'
    AND ad1obty IN (SELECT slentry
        FROM arg_strlst
        WHERE slid = 9
        AND slvalue1 = '{Relationship Object Type}')
```

2. Replace the placeholders with the values in the same-named columns on the Relationship Report. For example, the report Relationship Template Rename column identifies the product-provided name Activity Summary. You replace {Relationship Template Rename} with Activity Summary.

Change the Renamed Relationship Template Link to the Original Product-Provided Name

Before you run the Migration Utility, you change the renamed Relationship Template Link Names to the original product-provided Relationship Template Link Names from Release 11.3.4.

You execute a SQL statement to change the Relationship Template Link Name. Perform these steps for each entry in the report with status ‘Rename to migrate’ and a value that is specified under ‘Link Rename’.

Follow these steps:

1. Execute the following SQL statement from your preferred tool (for example, Microsoft SQL Server Management Studio or Oracle SQL Developer):

> **Note:** The brackets and the text within the brackets are placeholders. The placeholder names represent the column names on the Relationship Report.

```
UPDATE arg_linkdef
SET ndtext = '{Link Rename}'
WHERE ndtext = '{Link Name}'
    AND nd2obty IN (SELECT slentry
        FROM arg_strlst
        WHERE slid = 9
        AND slvalue1 = '{Link Object Type}')
```

2. Replace the placeholders with the values in the same-named columns on the Relationship Report. For example, in the report, the Link Rename column identifies the product-provided template link name as Approved by. You replace {Link Rename} with Approved by.

Duplicate Asset Rename Report

The Duplicate Asset Name Report identifies non-unique asset names.

Note: Only the assets that share the same asset name and have no values set for the following registration fields are affected:

- Serial Number
- Alt Asset ID
- Host Name
- DNS Name
- Mac Address
- Serial Number

During migration, the CA APM Migration Toolkit can automatically configure a unique Asset Name for each duplicate Asset Name in your CA MDB. Use the Duplicate Asset Name Report to help you decide how to specify the asset rename configuration (see page 344).

Reconciliation Reports

The Reporting tool generates the following reconciliation reports:

- Main Translation List Query Report
- Translation List Obsolete Report
- Translation List Unconverted Report
- Main Task Query Report
- Task Add Asset Report
- Customized Search Report

Main Translation List Query Report

The Main Translation List Query Report identifies legacy translation list data for companies, operating systems, and models. You analyze the data on this report to determine whether to run the Migration Utility (see page 345) to migrate legacy translation lists to the current release normalization rules or migrate the lists manually.

If you decide to migrate the translation lists manually, use the data on the Main Translation List Query Report.

Main Task Query Report

The pre-migration Main Task Query Report identifies data that you use *after* you run the Migration Utility. The report provides information about the legacy reconciliation tasks from Release 11.3.4. Save the report and reference it during manual migration of Hardware Reconciliation tasks to create reconciliation rules in the current release.

Task Add Asset Report

The Task Add Asset Report provides data that you use *after* you run the Migration Utility, when you perform manual migrations (see page 351). The report identifies the legacy reconciliation tasks that add owned assets from Release 11.3.4. Save the report and reference it during manual migration of Hardware Reconciliation tasks.

Customized Search Report

The Customized Search Report provides data that you use *after* you run the Migration Utility, when you perform manual migrations. The report identifies the legacy hardware reconciliation customized searches from Release 11.3.4. The current release version of CA APM provides predefined hardware reconciliation reports. You can customize these reports using the CA Business Intelligence, which is also provided in the current release. Save the report and reference it during manual migration of hardware reconciliation searches.

Translation List Obsolete Report

The Translation List Obsolete Report identifies the Hardware Reconciliation legacy translation lists from Release 11.3.4 that are obsolete and not supported in the current release. This report is for your reference. No action is required.

Translation List Unconverted Report

The Translation List Unconverted Report identifies the Hardware Reconciliation legacy translation lists from Release 11.3.4 that have missing or invalid entries that will not be migrated to the current release. The translation list will be migrated, but some of the entries in the list will not be migrated, because supporting data is not present in the legacy database.

Use the data on the Translation List Unconverted Report and on the Main Translation List Query Report to add the missing entries to the normalization lists after migration.

Use the Migration Report Data for Reference and Analysis

This article contains the following topics:

The Reporting tool generates reports in CSV format that you can open with a text editor. The report field names and field values are separated with commas. You can also open a report with Excel, which presents the data in a table format. When you open a report with Excel, the field names are the column headings, and the field values appear in the rows below the headings.

The post-migration reports give you information about data that you enter in Release 14.1 *after* migration. This data could not be migrated using the Migration Utility.

The following post-migration reports provide information that you use to perform manual migrations (see page 351):

- Advanced Search Report (see page 340)
- Attachments Report (see page 341)
- Basic Search Report (see page 341)
- Event Reports (see page 341)
- Filtering Reports (see page 343)
- Role Security (Field and Functional Permissions) Reports (see page 343)

Advanced Search Report

The Advanced Search Report provides a summary of each advanced search and location information for the detail reports for each advanced search (see page 341). The Detail column of the report provides the location and name of each Advanced Search Detail Report.

The following report fields require an explanation:

- **Export Type**
  Indicates the Export Format for search results.
- **Refresh Interval**
  Identifies the start time and frequency for an Export Schedule.
- **Object Type**
  Indicates Role Access when the Security Search setting has one or more roles.
- **Assignment**
  Identifies the role name or contact that has permission to access the search.
- **Creator**
  Identifies the name of the last user to update the search. Use this information to delegate the manual migration (re-creation) of the advanced search. You do not assign this field to a setting in the advanced search.
- **Creator ID**
  Identifies the name of the last user to update the search. Use this information to delegate the manual migration (re-creation) of the advanced search. You do not assign this field to a setting in the advanced search.

Use the Advanced Search Report to migrate the advanced searches to Release 14.1 manually.

Advanced Search Detail Reports

Each Advanced Search Detail Report identifies the data for one advanced search. Review the information about advanced searches that were created in Release 11.3.4.

Use the Advanced Search Detail Reports to migrate these advanced searches to Release 14.1 manually.

Attachments Report

The Attachments Report identifies information that you use to migrate file attachments manually. The Migration Utility migrates the complete Web URL link attachments and the metadata for remote server and local file attachments. After migration, you move the physical file attachments to the Storage Manager Service.

The Attachments Report provides the file location and description and the following information for each attachment:

- **UUID**
  Universally Unique Identifier identifies an object and distinguishes between two objects that have the same name.

- **Object Type**
  Identifies the type of object to which the file is attached.

- **Assignment**
  Identifies the name of the object to which the file is attached.

Basic Search Report

Use the Basic Search Report to view the following information about searches that were created in Release 11.3.4 and to migrate these basic searches to Release 14.1 manually:

- Object Type that the search returns.

- Role, if any, permitted to view the search return fields.

- Search Return Fields, which were named Display Fields in Release 11.3.4.

Event Reports

The Notification History Event Report (see page 341) provides history information from Release 11.3.4, for you to review. The following Event Reports identify data that you use *after* you run the Migration Utility, when you perform manual migrations. Reference these reports during manual migration of events (see page 351):

- Date Event Report (see page 342)

- Watch and Change Event Report (see page 342)

Notification History Event Report

The Notification History Event Report provides history information from Release 11.3.4 for you to review. No action is required.

This report identifies events that were processed in the last year. The following fields require explanation:

- **Event Enabled**
  Indicates that the event is enabled and not inactive when the value is TRUE. Indicates that the event is inactive when the value is FALSE.

- **Event Field Name**
  The event is based on the value of this object field.

- **Event Recipient**
  The email address of the current event notification.

- **Event Notification Definition Text**
  The email message text of the current event notification.

- **Notification Type**
  Indicates the type of notification that the recipient receives. "Initial Event" indicates the recipient of the first notification. "Escalation" indicates the recipient of unacknowledged notifications.

- **Notification Text**
  The email message text of the past event notification.

- **Notification Recipient**
  The email address of the past event notification.

See CA Process Automation Integration for information about workflow provider process parameters that are specified in CA Process Automation. For information about notification process parameters, see your workflow provider documentation.

Date Event Report

The Date Event Report identifies data that you use *after* you run the Migration Utility, when you perform manual migrations. This report identifies date events and notifications. Reference the report during manual migration of events.

The Integrate with CA Process Automation Integration for a Notification Process Manually (see page 3489) section provides information about workflow provider process parameters that are specified in CA Process Automation. For information about notification process parameters, see your workflow provider documentation.

Watch and Change Event Report

The Watch and Change Event Report identifies data that you use *after* you run the Migration Utility, when you perform manual migrations. This report provides information about watch events and notifications and about change events and notifications, from Release 11.3.4. Reference the report during manual migration.

Note: Manual events were available in Release 11.3.4, but are not supported in Release 14.1. Manual events are not included on the Watch and Change Event Report.

The Integrate with CA Process Automation Integration for a Notification Process Manually (see page 3489) section provides information about workflow provider process parameters that are specified in CA Process Automation. For information about notification process parameters, see your workflow provider documentation.

Filtering Reports

The Filtering Report provides a summary of each filter and location information for the detail reports for each filter. The Detail column of the report provides the location and name of each Filter Detail Report.

Contact Filtering Detail Report

Each Filtering Detail Report identifies the data for one filter. Use the Filtering Detail Reports to view the information about filters that were created in Release 11.3.4 and to migrate filters manually.

Role Security (Field and Functional Permissions) Reports

Each Role Security Report identifies the data for one field, functional, or viewable linked object security setting. The Migration Toolkit generates the following types of role security reports:

- **Field Security Reports.** Generates one Field Security Report for each object that has role security settings. The report identifies the role, the object, the object field, and the permission that is assigned to the role for the field. The Update Permission report column label and the Add New Permission report column label refer to Release 11.3.4 functionality. Release 14.1 does not differentiate permissions for updating and creating objects.

- **Functional Security Reports.** Generates one Functional Security Report for each object that has role security settings. The report identifies the role, the object, the function related to the object, and the permission that is assigned to the role for the function.

- **Field Security Linked Object Viewable Report.** Generates one Field Security Linked Object Viewable Report for each object that has role security settings. The report identifies the role, the objects, and the assigned fields for the object.

Use the Role Security Reports to view the information about role security settings that were created in CA APM Release 11.3.4 and to migrate role security settings manually.

The following objects, fields, and functions are not supported in Release 14.1. They appear on the Release 11.3.4 database reports for reference only:

- Asset Version

- Asset Version Status History

- Model Version

- Keywords

Specify the Duplicate Asset Rename Configuration

CA APM Release 14.1 registration includes asset name, serial number alt asset ID, host name, DNS name, and mac address. A *unique* asset name is required for each asset object. Release 11.3.4 did not have this requirement, so your CA MDB could have asset names that are not unique for asset registration. The CA APM Migration Toolkit can automatically configure a unique asset name for each duplicate asset name in your CA MDB during migration.

The CA APM Migration Toolkit uses a configuration to rename the duplicate asset names. You choose the configuration on the CA APM Migration Utility Duplicate Asset Name Configuration dialog. When you run the Migration Utility, the duplicate assets are renamed in the current release database.

Note: A unique asset name is a requirement for asset registration by the Common Registration API (CORA) for the current CA APM release. If you do not have CORA enabled, asset registration does not occur.

Follow these steps:

1. Review the Duplicate Asset Name Report.
2. On the CA Asset Portfolio Management Migration Toolkit main window, click Duplicate Asset Name Configurator.
3. Select one of the following rename configurations:

   - **Replacement**
     Replaces the duplicate asset names with the value in another field. You select this field in the drop-down list.

     Note: The fields in the drop-down list are the same fields that are the headings on the Duplicate Asset Name Report.

     The Incrementation configuration is automatically selected and locked. If the Replacement configuration results in a duplicate asset name, adding Incrementation to the configuration ensures that the rename is unique.

   - **Concatenation**
     Appends the values of one or more fields onto the end of the duplicate asset names. You select up to four fields in the drop-down lists.

     Note: The fields in the drop-down lists are the same fields that are the headings on the Duplicate Asset Name Report.

The Incrementation configuration is automatically selected and locked. If the Concatenation configuration results in a duplicate asset name, adding Incrementation to the configuration ensures that the rename is unique.

- **Incrementation**
  Appends a unique integer value to the end of the duplicate asset names and increments the integer by one for each subsequent duplicate asset name. You enter the starting integer in the Integer Base Line Value.

- **NONE**
  Duplicate asset names are not renamed. You can select this option if you do not have CORA enabled or if you want to correct the assets manually after migration.

4. (Optional) Enter a one-character Field Delimiter that appears between each field and between a field and an incrementation integer in the Incrementation and Concatenation configurations.

5. Click Save.

Note: Depending on the number of records, it takes some time for the configuration to save. The progress bar indicates the status of completion.

6. Click Exit.

Run the Migration Utility

This article contains the following topics:

The Migration Utility migrates audits, objects, and events from one CA APM release to the upgraded database structure of another.

The hierarchical structure of the objects in the selection area on the CA APM Migration Utility window allows you to select all objects within a hierarchy level or to select individual objects within a level. A status icon displays the migration status for each object or object level.

The icon key in the top area of the window indicates the statuses. When an object status is Complete, you cannot select the object.

The Messages and Summary tabs allow you to monitor the migration process and to review the migration run.

Important: In addition to the services and the scheduled tasks detailed in Prerequisites, ensure the current release services are not running before you run the Migration Utility.

The first time that you open the window, you are prompted to confirm the migration database versions. After you complete this task, you can run the object migrations.

Note: With CA APM 14.1, you can migrate objects that were not migrated with Release 12.9. These objects are costs and payments extensions and audits, custom relationships and audits, and relationship extensions and audits. With this release, all relationships are migrated, including custom relationships and relationships that were not product-provided. If you previously migrated your data from Release 11.3.4, you can migrate the data for just these objects. You do not need to perform the complete data migration again.

You can migrate the following objects and associated events with the Migration Utility:

- Assets
  - Unique Asset Names for CORA
  - Asset Current Status History
- Cost and Payments
  - Billing Codes
  - Pricing Types
  - Cost Types
  - Currency Types
- Cost and Payment Extensions (and the associated audits)
- Legal Documents
  - Legal Definitions
  - Document Locations
  - Legal Status
  - Legal Document Status Histories
- Notes
  - Note Types
- OOTB Relationships (Original Product-Provided Relationships)

- Custom Relationships (and the associated audits)
- Extensions
  - Simple Extensions
  - List Extensions
  - Location Hierarchies
- Relationship Extensions (and the associated audits)
- Attachments
- Roles
- Reconciliation Translation Lists (supported types only)
  - Operating System Translation List
  - System Model Translation List
  - Manufacturer Translation List
- Legacy audits to audit archive tables. The Audit History object is enabled after you migrate other objects and the Audit Generation for Events shows the status as Complete.

Note: To ensure that events work properly in the product, select Audit Generation for Events from the list of Migration Objects. Audit Generation for Events establishes baseline audit records.

Confirm the Migration Database Version

You confirm the migration database versions by testing the database connection. The first time that you run the Migration Utility, the CA APM Migration Utility Configuration dialog automatically opens. The dialog fields are populated with the database configuration settings that you specified during installation.

Note: After you confirm the migration database versions, click Configure on the Migration Utility window.

When you test the database connections, the Migration Utility detects the product release version *from* which you are migrating data and the release version *to* which you are migrating data. The utility populates the From Version and To Version fields on the dialog with the detected product release versions. You cannot change the release versions on the dialog.

The detected From Version must be Release 11.3.4 and the detected To Version must be CA Service Management 14.1. If the Migration Utility detects a different release version, you cannot proceed with the migration.

Follow these steps:

1. Enter the Database Password.

2. Click Test Connection.
   A confirmation message indicates that the connection test succeeded or failed.

3. Click Save on the CA APM Migration Utility Configuration dialog if the confirmation message indicated that connection testing succeeded.
   The dialog closes.

4. If the confirmation message indicated that the database connection test failed, determine why the Migration Utility could not connect to the database configuration. After you resolve the problem, repeat the connection test.

> **Note:** If the Product Release Versions on the CA APM Migration Utility Configuration dialog do not match the release versions that you are trying to connect to the Migration Utility, the database connection test fails. You cannot proceed with the migration.

If you want to change the database configuration settings later, see Configure the Migration Database.

Configure the Migration Database

You do not need to configure the migration database during the migration. The database is configured to the settings that were specified during installation.

Later, if you change the location of the CA MDB, configure the migration database to the new location before you run the Migration Utility.

Follow these steps:

1. Click Configure on the Migration Utility window.

2. Enter the configuration settings.

3. Click Test Connection.
   A confirmation message indicates that the connection test succeeded or failed.

4. Click Save on the CA APM Migration Utility Configuration dialog if the confirmation message indicated that the connection test succeeded.
   The CA APM Migration Utility Configuration dialog closes.

5. If the confirmation message indicated that the database connection test failed, determine why the Migration Utility could not connect to the database configuration. After you resolve the problem, repeat the connection test.

Run the Object Migrations

Note: In addition to the services and scheduled tasks , ensure the Release 14.1 services are not running before you run the Migration Utility.

The CA APM Migration Utility window lists the migration objects in a hierarchical structure in the CA APM Objects area. You select the objects that you want to migrate. You can migrate the data in stages. The hierarchical structure allows you to select all objects within a hierarchy level or to select individual objects within a level.

When you select an object to migrate, all objects within the hierarchy of that object are also selected. These objects are called secondary objects. The secondary objects within the hierarchy migrate first, and the top-level object that you selected migrates last. For example, if you select the Cost and Payments top-level object, the Billing Code, Pricing Type, and Cost Type secondary objects within the Cost and Payments object hierarchy are also selected. Expand the top-level object to see its secondary objects. During migration, Billing Code, Pricing Type, and Cost Type migrate first. The top-level object Cost and Payments migrates after its secondary objects.

You can clear the check boxes next to the objects that you do not want to migrate. You can select one object, a group of objects, or all objects to migrate.

Objects that have already been migrated have a status of Completed, and their check boxes are disabled. In this way, the Migration Utility prevents you from trying to migrate an object that has already been migrated.

Right-click an object to view options that you can select to perform. The options that are available depend on the status of the object. The following options are available for you to select when you right-click an object:

- Clear the check boxes for the secondary objects
- Move to Completed
- Move to Not Started

The Audit History object is disabled initially. You start with migrating the non-audit objects. The audit history object is enabled when the migration is successful and the Audit Generation of Events shows the status as Complete. You can migrate the Audit History objects anytime once the option is enabled, and all the applications and services are back online.

Important! Depending on the size of the data, Audit History objects can take a long time to migrate. If the audit history has approximately 1 million records, it is recommended to migrate it during off peak hours.

Follow these steps:

1. On the CA APM Migration Utility window, select the check boxes next to the objects that you want to migrate.

   Note: To ensure the events work properly in the product, select Audit Generation for Events from the list of Migration Objects. Audit Generation for Events establishes baseline audit records.

2. Click Start.
   Look at the information in the Messages tab to monitor the migration progress.
   When the migration is successful, the objects in the selection area of the window have a status of Completed.

   Note: If the migration fails, view the details in the object migration log files in the following location:

   ```
   [ITAM Root Path]\Migration Toolkit\migration-utility\logs
   ```

3. (Optional) If the migration is successful, select the Audit History object and repeat Step 2.

4. Click Exit.
   The CA APM Migration Utility window closes.

When the migration completes, restart the services for the following Service Management products:

- CA Service Catalog
- CA Service Desk Manager
- CA Client Automation
- CA APM Release 14.1

Monitor the Migration Process

The Messages tab on the CA APM Migration Utility window shows the progress of the current migration process. You monitor the migration process by viewing the messages. The messages indicate the changing status of each object that is being migrated.

When the migration is finished, you can view a summary of the successful, pending, and failed migrations on the Summary tab. The Summary tab shows the migration status for all migrations that ran during your session.

You can view the object migration log files from the following location:

```
[ITAM Root Path]\Migration Toolkit\migration-utility\logs
```

For any failure messages appearing in the log files, contact CA Support.

Start the CA APM Web Interface

You start the CA APM web interface to run CA Service Management 14.1 upgraded product and manually migrate data to this database. Complete the Migration Utility automated migrations and run the post-migration reports (see page 368) *before* you perform manual migrations (see page 351).

To start the web interface, open a web browser and enter the following URL:

```
http://servername/itam
```

Replace *servername* with the name of the server that is hosting the CA APM web servers.

Note: If the Internet Explorer browser security is set to high, a content warning message appears when you start the web interface. To avoid this message, add the web site to your trusted sites or lower your security settings.

A Start menu shortcut is created on your web server that references the URL location.

To log in to CA APM after you open the URL, enter the following default credentials:

- **User Name**
  uapmadmin
- **Password**
  uapmadmin

Note: In some situations, a browser error or a user name error appears. You can resolve these errors by following the troubleshooting instructions (see page 374).

Perform Manual Migration from CA APM 11.3.4 to the Current Release

You can perform the manual migration of data to the current release after you complete the following tasks:

- You migrated data using the Migration Utility.

- You generated the post-migration reports.

When you migrate data manually, you use the CA APM current release version to enter the data in the new-release data structures. The migration reports specify the fields and values that you enter.

Important: Exit the Migration Toolkit and start the web interface (see page 351) before you can perform the manual data migrations.

Perform the following manual migrations:

- Migrate Basic Searches (see page 352)
- Migrate Advanced Searches (see page 354)
- Migrate File Attachments (see page 358)
- Migrate Events (see page 360)
- Migrate Filters (see page 360)
- Migrate Role Security (Field and Functional Permissions) (see page 362)
- Migrate Hardware Reconciliation Tasks and Rules (see page 364)
- Migrate Hardware Reconciliation Translation Lists (see page 365)
- Migrate Hardware Reconciliation Searches (see page 366)

Migrate Basic Searches

In Release 11.3.4, the search return fields that a user can see are set in the Security feature by role. The current release version of CA APM enhances the Basic Search functionality so that it is more closely aligned to the Advanced Search. All fields are available in the Basic Search. In the current release version of CA APM, you set the search return fields that a user can view in the search feature. When you create a search and save the configured search, you can apply security to the search by selecting specific user roles and configurations.

By default, the security for the searches you create makes them available only to the creator. You assign roles and configurations to your searches to grant access to the users who are assigned to those roles and configurations.

Note: For information about searching, see Searching (see page 2431).

These changes cannot be migrated with the Migration Utility. Use the Basic Search Report data during the manual migration.

Follow these steps:

1. Identify the Object Type for the search on the Basic Search Report.
2. In CA APM, click the tab and optional subtab for the object that you want to find.
3. On the left, click New Search.
   The Add Fields dialog appears.

   Note: For some object types, you are prompted to select templates, families, or other attributes to narrow the search.

4. Using the report Search Return Fields, select the fields to add to the search. In Release 11.3.4, these fields were labeled Display Fields.
5. In the Add Fields(s) To area at the bottom of the dialog, select Search Criteria and Search Results.
6. Click OK.
   The fields are added to both the search criteria and search results. The Add Fields dialog closes.
7. At the top of the page, click CONFIGURE SEARCH: OFF.
   The configuration of the search is complete.
8. In the Search Information area, enter the search title and any other descriptive information, for example, Category and Description.
9. (Optional) Open the Search Security area.
10. (Optional) In the Search Security area, select the user roles for which the search is available.

    Note: We recommend that you select the user role that is identified on the Basic Search Report (see page 339).

11. (Optional) In the Search Security area, select the configuration for which the search is available.

    Note: If you do not select either a role or a configuration, the search is available only to the search creator.

12. Locate the Search Criteria area and the criteria fields that you entered.

13. For each Search Criteria field, enter the field value. You can click the search icon to search for a value.

14. (Optional) Open the Additional Settings area, and add other settings, for example, sorting settings.

15. Click Save.
    The search is saved.

16. If you selected user roles in the Search Security area, perform the following steps for each role:

    a. Click Administration, User/Role Management.

    b. On the left, expand the Role Management menu.

    c. Click Role Search.

    d. Search for and select the role.
       The role details appear.

    e. In the Default Searches area, click Select New.

    f. Search for the search that you just created.

    g. Assign the search as a default search for the role.

    h. Click Save.
       The updated role is saved.

Migrate Advanced Searches

In CA APM Release 11.3.4, the search return fields that a user can see are set in the Security feature by role. In this release, searches support an added level of security. You set the search return fields that a user can view in the search feature. When you save the configured search, you can apply security to the search by selecting specific user roles and configurations.

By default, the security for the searches you create makes them available only to the creator. You assign roles and configurations to your searches to grant access to the users who are assigned to those roles and configurations.

Note: For information about searching, see Searching (see page 2431).

These changes cannot be migrated with the Migration Utility.

When you migrate Advanced Searches, you complete the following steps:

- Create the Advanced Search (see page 355)

- Schedule a Search and Export Results (see page 357)

Create an Advanced Search

Use data from the Advanced Search Report (see page 339) and the Advanced Search Detail Report (see page 339) during the manual migration.

Follow these steps:

1. Identify the Object Type for the search on the Advanced Search Detail Report.
2. In CA APM, click the tab and optional subtab for the object that you want to find.
3. On the left, click New Search.
   The Add Fields dialog appears.

   Note: For some object types, you are prompted to select templates, families, or other attributes to narrow the search.

4. On the detail report, identify the fields that are in *both* the Return Fields and the Selected Criteria Fields.
5. On the Add Fields dialog, select the common fields that you identified on the report.
6. In the Add Fields(s) To area at the bottom of the dialog, select Search Criteria and Search Results.
7. Click OK.
   The fields that are both Search Criteria and Search Results fields are added to the search, and the Add Fields dialog closes.
8. Click Add Fields.
   The Add Fields dialog appears.
9. Select the Return Fields that are not common to the Return Fields and the Selected Criteria Fields on the detail report.
10. In the Add Fields(s) To area at the bottom of the dialog, select Search Results Only.
11. Click OK.
    The Search Results Only fields are added to the search, and the Add Fields dialog closes.
12. Click Add Fields.
    The Add Fields dialog appears.
13. Select the Selected Criteria Fields that are not common to the Return Fields and the Selected Criteria Fields on the detail report.
14. In the Add Fields(s) To area at the bottom of the dialog, select Search Criteria Only.

15. Click OK.
    The Search Criteria Only fields are added to the search, and the Add Fields dialog closes.

16. At the top of the page, click CONFIGURE SEARCH: OFF.
    The configuration of the search is complete.

17. In the Search Information area, enter the search title and any other descriptive information from the report. For example, Category and Description.

18. (Optional) Expand the Search Security area.

19. (Optional) In the Search Security area, perform the following steps to select the user roles for which the search is available:

    a. Click Select New in the Role Access area.
       The Role Search dialog opens.

    b. Enter the Role Name that is identified in the Assignment field on the Advanced Search Report. Role Name can be the name of a role or a contact name.

    c. Enter a Description, if you want.

    d. Select whether to include Inactive records in the search for the new role.

    e. Click Go.
       The search results appear.

    f. Select the roles or contacts for which the search is available.

    g. Click OK.
       The Role Search dialog closes.

20. (Optional) In the Search Security area, select the configuration for which the search is available.

    Note: If you do not select either a role or a configuration, the search is available to all users and configurations.

21. Locate the Search Criteria area and the criteria fields that you selected.

22. Click Advanced.
    The advanced Search Criteria area opens.

23. For each Search Criteria, perform the following steps:

    a. Click the Edit Record icon next to a Search Criteria.

    b. Locate the Criteria information about the report.

c. Enter the Operator, Value, Connector, and parenthesis, as indicated on the detail report.

d. Click the Complete Record Edit icon.

24. (Optional) Open the Additional Settings area, and add other search settings, for example, sorting.

> **Note:** In the Search Results Sorting area, select the Selected Field and Sort Direction values, as identified on the detail report Sort Order area.

25. Click Save.
The advanced search is saved.

Schedule a Search and Export Results

You can schedule a search to process periodically and export the search results to a CSV file or a database view.

Follow these steps:

1. In CA APM, click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.
3. Search for and select the search that you saved.
4. On the left, click New Export.
5. Enter the basic export information that is based on the detail report export information.
6. The following fields require explanation:

- **Export name**
Specifies the export name.
- **Export Format**
Specifies the format for the exported search results.
- **View Name**
Specifies the database view name.

> **Note:** The view name is required if you select Database View for the Export Format. The name must be a valid database view name.

- **Description**
  Specifies a description for the exported search results.

- **Retention Days**
  Specifies the number of days that the exported search results are retained before the results are purged.

- **Folder Name**
  Specifies the folder for the exported CSV file search results.

- **Never Expires**
  Specifies that the CSV file or database view is never purged.

7. Schedule the search in the Export Schedule area. Use the detail report Refresh Interval value to schedule the search.
   The following fields require explanation:

   - **Run Time**
     Specifies the time of day to process the search, in the local time zone on the CA APM application server.

   - **Interval Type**
     Specifies the type of interval for the search, for example, Day, Month, Quarter, Week, or Year.

   - **Interval Day**
     Specifies the day during the interval to process the search. For example, if the Interval Type is Month and the Interval Day is 1, the search is processed on the first day of the month.

   - **First Run Date**
     Specifies the date when the first search starts to process.

   - **Interval**
     Specifies how often the search processes, which are based on the selected Interval Type. For example, if the Interval Type is Weekly and the Interval is 2, the search processes every two weeks.

   - **Last Day of Interval**
     Specifies that the search processes on the last day of the selected Interval Type.

8. Specify whether all roles and configurations that are assigned to the search receive the exported search results.

9. Click Save.
   The search is saved. The search processes at the scheduled time and the search results are exported.

Migrate Attachments

In the current release, the Storage Manager Service handles all attachment files. You can specify two types of attachments:

- **Web URL link.** Provides direct access to the page specified in the URL. When you add this type of attachment, include the prefix *http://* for the link to work correctly.
- **File path.** Provides direct access to a file. The file opens using the default program for the file type. At the time that you create this attachment type, the file is copied from your file system to the file system on a CA APM server.

  Note: If you add multiple attachments (to one object or to different objects), the name and file path or URL for each attachment must be unique for all objects.

In Release 11.3.4, file attachments were stored in a common share folder.

The Migration Utility migrates the complete Web URL link attachments and the metadata for remote server and local file attachments. The metadata includes the attachment description information and file path location information. The Migration Utility changes the file path location to the Storage Manager Service. After migration, you move the physical file attachments to the Storage Manager Service.

After you run the Migration Utility, you copy the Release 11.3.4 file attachments from the share folder and your local server to the current release Storage Manager Service. Web URL link attachments are migrated by the Migration Utility.

Note: For more information about file attachments, see Manage an Attachment (see page 2349).

Use the Attachments Report (see page 339) data during the manual migration.

Follow these steps:

1. Navigate to the file attachment location that is identified on the report.
2. Copy and paste the file attachment to the following location on the Storage Manager Service on the application server:

   - *[ITAM Root Path]*\Storage\Common Store\Attachment*attachment.extn*

   Replace *attachment.extn* with the attachment filename and extension.
   Enter the complete path to the file attachment, for example:
   C:\Program Files (x86)\ITAM\Storage\Common Store\Attachment\legaldoc1.docx
3. Repeat these steps for each remote server or local file attachment on the report.

   Note: Files that are not moved to the Storage Manager Machine location are not available in the product.

4. If you deleted an attachment from the remote server or your local machine, but not from CA APM, the Migration Utility migrates the metadata for the attachment. If the report identifies attachments that no longer physically exist, use the current release version of CA APM to delete the attachment metadata.

Migrate Events

You can use the user interface to define date, change, and watch events. You can set up notifications using hard-coded text and the CA APM object values. For example, you can specify that the subject of a notification include the words "Acknowledgment required for" followed by the value of the CA APM legal document identifier object. When an event occurs, email notifications can be sent to specific recipients. Notifications that are not acknowledged can be escalated.

Use the Date Event Report (see page 339) data and the Watch and Change Event Report (see page 339) data during the manual migration of events and notifications.

Follow these steps:

1. Follow the instructions for creating events and notifications i*n Administration (see page 1568)*.

2. Use the information in the Date Event Report and the Watch and Change Event Report to create the events and notifications.

Note: See CA Process Automation Integration (see page 3489) for information about workflow provider process parameters that you specify in CA Process Automation. For information about notification process parameters, see your workflow provider documentation.

Migrate Filters

In CA APM Release 11.3.4, the filters that a user can see are set in the Security feature, by role. In this release, filters support an added level of security. You set the filters that a user can view in the filters feature. When you configure a filter, you can apply security to the filter by selecting specific user roles and users who have permission to see the filter.

By default, the security for the filters you create makes them available to all roles and users. By applying unique security to your filters, you ensure that certain users cannot view sensitive information in a filter.

These changes cannot be migrated with the Migration Utility. Use the Filter Detail Reports (see page 339) data during the manual migration.

Follow these steps:

1. Identify the object for the filter on the Filtering Detail Report.

2. In CA APM, click the Administration tab and the Filter Management sub tab.

3. Click New Filter.
   The Filter Details page opens.

4. In the Filter Information area, perform the following steps, using the information in the Filtering Detail Report:

   a. Enter the Filter Name and the Object that you want to filter.

   b. (Optional) Enter a Description.

   c. (Optional) Select Assign Filter to All Users, if you want all users to be able to view the filter data. If you want to apply security to the filter, complete the Filter Security area, as described in the following steps.

5. In the Filter Security area, perform one or more of the following actions:

   - To enter roles that can see the filter:
     - Click Select New in the Roles area.
       The Role Search dialog opens.
     - Search for and select the roles that are permitted to see the filter.
     - Click OK.
   - To enter users who can see the filter:
     - Click Select New in the Users area.
       A search dialog opens.
     - Search for and select the users who are permitted to see the filter.
     - Click OK.

6. Click Add Fields.
   The Add Field(s) dialog opens.

7. Select the fields that appear on the report in the Selected Criteria Fields section.

8. Click OK.
   The Add Field(s) dialog closes and the fields that you selected appear in the Filter Criteria area.

9. Using the information in the Criteria area of the detail report, perform the following steps for each Filter Criteria:

   a. Click the Edit Record icon next to a Filter Criteria.

   b. Enter the Operator, Value, Connector, and parenthesis, as indicated on the report.

   c. Click the Complete Record Edit icon.

10. Click Save.
    The filter is saved.

Migrate Role Security

The Migration Utility migrates user roles, but not the role security settings. You migrate the role security (field, functional, and viewable linked object permissions) manually.

A user role is the primary record that controls security and user interface navigation. Each role defines a focused view of the product by exposing only the functionality necessary for users to perform the tasks that are typically assigned to their roles in their business organization. The default role for a user, together with the user interface configuration, determines what the user sees when logging in. A user can belong to only a single role.

You configure user roles to apply functional and field-level repository access rights. You determine and assign the level of access that is required for each role. Role assignment prevents the users from performing unauthorized tasks, such as adding or deleting data.

Field security defines the role permissions for an object field, for example, full control. Functional security defines the role permissions for functions on an object, for example, copy an asset. Viewable Linked Object Security defines the fields for the object.

You create the security permission settings for an object in the object local configurations. Then, you assign one of the object configurations to a role. The field and functional security permissions for a role are determined by the object configurations that are assigned to that role. The object configuration for each role is identified on the Role Security Reports for the object.

You perform the following manual migrations to migrate the role security:

- Migrate Role Field Security (see page 362)
- Migrate Role Functional Security (see page 363)
- Migrate Role Viewable Linked Object Security (see page 364)

Use the information in the Role Security Reports to migrate the role field security, role functional security, and role viewable linked field security manually.

Migrate Role Field Security

Use the information in the Role Security Reports (see page 339) to migrate role field security manually.

Follow these steps:

1. For role field security permissions, on the Field Security Report for the object, locate a field and the role permission for the field.
2. Create and name a local configuration for the object field. The following field security configurations are available:
   - **Full Control.** The field is editable by the role.

- **Hidden.** Hidden and removed from the user interface for the role.
- **Read Only.** The field is read only for the role.

> **Note:** For information about configuring the user interface, see How to Configure the User Interface (see page 1520).

Migrate Role Functional Security

Use the information in the Role Security Reports to migrate role functional security manually.

Follow these steps:

1. For role functional security permissions, on the Functional Security Report for the object, locate a function and the role permission for the function.
2. Create and name a local configuration for the object function. Functional security configurations can be one of many functions, for example, allow users to change the asset model. Functional security configurations have a permission of Granted Permission or Denied Permission.

> **Note:** For information about configuring the user interface, see the How to Configure the User Interface (see page 1520).

3. Save the object configuration.
4. Click Administration, User/Role Management.
5. On the left, expand the Role Management area.
6. Click Role Search.
7. Search for the role indicated on the Security Report.
8. Click the role name link in the Search Return area.
   The Basic Information area opens.
9. On the left, click Role Configuration.
   The Role Configuration area appears.
10. Click Select New.
    The list of saved configurations appears.
11. Select the object configuration that you want to assign to the role.

12. Click OK.
    The object configuration is assigned to the role.

Migrate Role Viewable Linked Object Security

Use the information in the Role Security Reports to migrate role viewable linked object security manually.

Follow these steps:

1. For role viewable linked object security permissions, on the Field Security Linked Object Viewable Report, locate a linked object and the role for the object.
2. Create and name a local configuration for the object. Link the fields that are defined as Assigned Fields for the Object in the report.
3. Save the object configuration.
4. Click Administration, User/Role Management.
5. On the left, expand the Role Management area.
6. Click Role Search.
7. Search for the role indicated on the Security Report.
8. Click the role name link in the Search Return area.
   The Basic Information area opens.
9. On the left, click Role Configuration.
10. Click Select New.
11. Select the object configuration that you want to assign to the role and click OK.

The object configuration is assigned to the role. Repeat the steps for each role in the report.

Migrate Hardware Reconciliation Tasks and Rules

The hardware reconciliation process involves the following steps:

1. Establish data normalization rules to map data values between discovery repositories and the product.
2. Define a reconciliation rule to specify how to limit the data being processed and how to process the records that were found.

> **Note:** The reconciliation rules in this step replace the Release 11.3.4 reconciliation tasks. You create reconciliation rules that are based on the Release 11.3.4 tasks from the Main Task Query Report (see page 332) and the Task Add Asset Report (see page 332), during the manual migration.

3. (Optional) Define reconciliation update options to specify the owned-asset fields that you want the Hardware Reconciliation Engine to update automatically with changes found in the corresponding discovered assets.

4. Define asset matching criteria to match owned and discovered assets for a reconciliation rule.

5. View the reconciliation results in the message queue.

Use the Main Task Query Report and Task Add Asset Report data during the manual migration of tasks to reconciliation rules.

Follow these steps:

1. Follow the instructions for defining reconciliation rules in *Define a Reconciliation Rule (see page 2417)* section.

2. Use the information in the Main Task Query Report and Task Add Asset Report to create the reconciliation rules.

Migrate Hardware Reconciliation Translation Lists

If you choose *not* to migrate the Hardware Reconciliation translation lists using the Migration Utility, you migrate the lists manually. You analyze the Main Translation List Query Report to make this decision.

The current release of CA APM replaces multiple translation lists of the same type with normalization rules for Model, Manufacturer, and Operating System.

Use the Main Translation List Query Report (see page 332) data during the manual migration of translation lists to normalization rules.

Follow these steps:

1. Follow the instructions for creating normalization rules in the Data Normalization (see page 351) section.

2. Use the information in the Main Translation List Query Report to create the normalization rules.

> **Note:** Merge all of the lists of the same type, eliminate duplicate entries, and migrate the combined list to the corresponding normalization rules.

Migrate Missing Entries from Hardware Reconciliation Translation Lists

The Translation List Unconverted Report identifies the Hardware Reconciliation legacy translation lists from CA APM Release 11.3.4 that have missing or invalid entries that are not migrated to the current release. The translation list is migrated, but some of the entries in the list are not migrated, because supporting data is not present in the legacy database.

The product replaces multiple translation lists of the same type with normalization rules for Model, Manufacturer, and Operating System.

Use data from the Translation List Unconverted Report (see page 332) and the Main Translation List Query Report (see page 332) to add missing entries on the legacy translation lists to the current release normalization rules.

Follow these steps:

1. Follow the instructions for updating normalization rules in the Data Normalization (see page 2407) section.

2. Use the information in the Translation List Unconverted Report to update the normalization rules in with the missing entries identified in the report.

> **Note:** Merge all of the lists of the same type, eliminate duplicate entries, and migrate the combined list to the corresponding normalization rules.

Migrate Hardware Reconciliation Searches

You migrate the hardware reconciliation custom searches from CA APM Release 11.3.4 to the current release hardware reconciliation reports. The product provides predefined hardware reconciliation reports that are generated by CA Business Intelligence software. You can customize these reports using CA Business Intelligence, which is also provided.

Hardware reconciliation reports provide the following information:

- Owned assets that have been reconciled to a discovered asset, including both discovered inventory and network discovery records.
- Billed assets (an active or received asset having a valid bill code) not matched to a discovery record.
- Discovered assets not reconciled to an owned asset.
- Discovered assets not processed due to missing or invalid data.
- Counts of the current discovery data volume.
- Owned assets matched to discovery records.
- Owned assets not matched to discovery records.

- Matches between network discovery data and agent discovery data.
- Potential lost revenue, including assets not being billed, but discovered. This report exposes revenue opportunities that are based on the number of assets being billed. Use the information in this report to provide proof that an asset is active and discovered.
- Network discovery records that have not been matched to a corresponding discovered inventory. Network discovery provides limited data to identify an asset on the network. Discovery provides detailed hardware and software information about an asset.

Use the Release 11.3.4 search information in the Customized Search Report (see page 332) to determine which hardware reconciliation reports to generate and possibly customize.

Follow these steps:

1. Follow the instructions for generating hardware reconciliation reports in the Reconciliation Reports (see page 2428) section.
2. Use the information in the Customized Search Report to locate the related hardware reconciliation report and enter the search criteria.

Note: To add unreconciled assets by generating and exporting the results of a report and then importing the report results through Data Importer, see Add Assets from Unreconciled Discovered Records (see page 2425).

Perform Post-Migration Verification for CA SDM and CA Service Catalog Integration

If you integrated CA Service Desk Manager and CA Service Catalog before performing the data migration, perform the post-migration verification of these integrations. You perform this verification after you have completed migrating all data to CA APM 14.1.

Follow these steps:

1. Click Run and execute services.msc.
2. Select and start the service, if the CA Service Desk Manager service is not running.
3. Go to the CA Service Desk Manager directory.
   If the CA Service Desk Manager PDM Tomcat service is not running, select and start the service.
4. Log in to CA Service Catalog. Go to Administration and click Configuration.
5. Click the CA APM Web Services hyperlink and enter the CA APM web server name.Enter the port number and click Save.
6. Log out and start the CA Service View service in services.msc.
   Verify that the CA APM integrations with CA Service Desk Manager and CA Service Catalog work.

Run the Post-Migration Reports for Manual Migration

After you run the Migration Utility, run the post-migration reports, which you use during manual migrations. The post-migration reports identify object data that you have to enter into the current release. The utility could not migrate some data because the feature associated with the data changed.

Follow these steps:

1. On the CA APM Migration Toolkit main window, click Migration Reporting.
2. Clear all of the check boxes in the Pre-Migration Reports area and select the following reports in the Post-Migration Reports area:
   - Advanced Searches
   - Attachments
   - Basic Search Return Fields
   - Events
   - Filters
   - Role Security (Field and Functional Permissions)

   Note: If you do not want to generate all post-migration report types, select only those report types that you want.
3. In the Report Output Folder area, click Browse, and select the output folder where you want to save the reports.
4. Click Generate Reports.
   The status messages appear in the Messages area to help you monitor the report generation process.
   You are prompted to open the report output folder to view the reports.
5. Click Yes.
   Windows Explorer opens. The Reporting tool creates a folder for each Post-Migration Reports check box that you selected previously.
6. Navigate to, and open, a report folder.
   The reports appear in comma-separated value (CSV) format.
7. Right-click a report and select Open with, Excel, to open and view the report in a table format.
   The report data (see page 339) is presented in a table format. The table headings are in the first row.

Note: You can open a report and view in a text editor, in CSV format.

CA APM Migration Utility Patch

Complete the following steps to apply the CA APM Migration Utility Patch:

Verify the Prerequisites

This CA APM Migration Utility Patch can be applied on CA APM Release 12.9 or CA APM Release 14.1.

Install the Patch

Follow these instructions to install the patch.

Download and Extract the Patch.

Follow these steps:

1. Download the CA APM Migration Utility patch from CA Support Online to the CA APM web server in a temporary folder.
2. Unzip the CA APM Migration Utility patch.
3. After unzipping, verify the availability of the following files:
   - Database.exe
   - healthcheck-version-1_0_0_737.exe
   - version-1_0_0_737.exe
4. Run the ‘Database.exe’ file, and verify availability of the following folders:
   - 12.9MDB
   - 14.1MDB
5. Run the 'healthcheck-version-1_0_0_737.exe' file, and verify availability of the following folders:

- com
- lib

6. Run the 'version-1_0_0_737.exe' file, and verify availability of the following folder:
   - Migration-CoraConfigurator
   - migration-documentation
   - Migration-launchUI
   - migration-reporting
   - migration-utility

Run the Health Check Utility.

From the extracted 'healthcheck-version-1_0_0_737' folder, run the Health Check Utility.

To run the Health Check utility, see the 'CA Migration Health Check Utility User Guide.docx' available within the 'healthcheck-version-1_0_0_737' folder.

Upgrade the Database.

Follow these steps:

1. Perform the following steps on the web server:
   a. For APM 12.9, from the command prompt, go to the [Extracted Database Folder] \Database\12.9MDB\mdb folder
   b. For APM 14.1, from the command prompt, go to the [Extracted Database Folder] \Database\14.1MDB\mdb folder
2. For **SQL Server**, execute the following command:

```
setupmdb.bat -DBVENDOR=mssql -DBNAME=<mdb_name> -DBHOST=<database_hostname> -
DBUSER=<database_username> -DBPASSWORD=<database_password> -
MANIFEST=Unicenter_Asset_Portfolio_Management -WORKSPACE=UAPM
```

DBVENDOR
Specifies the database vendor name. Enter mssql for SQL Server.

DBNAME
Specifies the existing CA APM Release 12.9 or CA APM Release 14.1 MDB database name.

DBHOST
Specifies the database server system host name.

DBUSER
Specifies the existing CA APM Release 12.9 or CA APM Release 14.1 MDB database user name.

DBPASSWORD
Specifies the existing CA APM Release 12.9 or CA APM Release 14.1 MDB database password.

Important! The -DBUSER and -DBPASSWORD parameter values must match your existing CA APM Release 12.9 or CA APM Release 14.1 database user name and password.

MANIFEST
Specifies the name of the manifest file. Do not change the default value for this parameter.

WORKSPACE
Specifies the name of the workspace. Do not change the default value for this parameter.

3. For **Oracle Server**, execute the following command:

```
setupmdb.bat -DBVENDOR=oracle -DBNAME=<oracle_service_name> -
DBHOST=<database_hostname> -DBUSER=<database_username> -
ORA_TBLSPACE_PATH=<tablespace_path> -DBPASSWORD=<database_password> -
MDB_ADMIN_PSWD=<mdb_administrator_password> -
MANIFEST=Unicenter_Asset_Portfolio_Management -WORKSPACE=UAPM
```

DBVENDOR
Specifies the database vendor name. Enter oracle for Oracle.

DBNAME
Specifies the existing Oracle Service name.

DBHOST
Specifies the database server system host name.

DBUSER
Specifies the existing Oracle database user name.

ORA_TBLSPACE_PATH
Specifies the path to the Oracle tablespace.

DBPASSWORD
Specifies the existing Oracle database password

Important! The -DBUSER and -DBPASSWORD parameter values must match your existing CA APM Release 12.9 or CA APM Release 14.1 database user name and password.

MDB_ADMIN_PSWD
Specifies the existing MDB administrator password.

MANIFEST
Specifies the name of the manifest file. Do not change the default value for this parameter.

WORKSPACE
Specifies the name of the workspace. Do not change the default value for this parameter.

Verify MDB Installation

Open the install_<databasename>.log file with a text editor.

Note: In the log file name, database name is replaced with the name of the database. For example, if the database name is test, the log file name is install_test.log.

Verify that a message similar to the following message appears at the end of the log file:

'*MDB setup completed successfully*'

Upgrade to CA APM Release 12.9 or CA APM Release 14.1

Upgrade to CA APM Release 12.9 or CA APM Release 14.1.

For more information, see Migrate CA APM Release 11.3.4 to the Current Release (see page 325).

Run the Migration Utility.

Follow these steps:

1. Generate Pre-Migration Reports:
    a. Log in as an administrator
    b. Navigate to the folder 'version-1_0_0_737'\migration-reporting'.
    c. Run the 'migration_reporting.bat' file.
    d. Select the option for Pre-Migration reports.

    Note: When the CA APM Migration Utility for Reporting is launched, configure the database manually.

2. If the Health Check Utility reports a duplicate asset name, perform the following steps:
    a. Log in as an administrator
    b. Navigate to the folder 'version-1_0_0_737\Migration-CoraConfigurator'.
    c. Run the 'Migration-CoraConfigurator.bat' file.

> **Note:** When the CA APM Migration Utility for Duplicate Asset Name Configuration is launched, configure the database manually.

3. Run the Migration Utility:
    a. Log in as an administrator
    b. Navigate to the folder 'version-1_0_0_737'\Migration Utility'.
    c. Run the 'Migration-Utility.bat'

> **Note:**When the CA APM Migration Utility is launched, configure the database manually.

4. Generate Post-Migration Reports:
    a. Log in as an administrator
    b. Navigate to the folder 'version-1_0_0_737'\migration-reporting'.
    c. Run the 'migration_reporting.bat' file.
    d. Select the option for Post-Migration reports.

> **Note:** When the CA APM Migration Utility for Reporting is launched, configure the database manually.

Fixes

The following defects have been fixed in the CA APM Migration Utility patch:

Title	Description
Cost and Payment Issue	Cost and Payments Node failed due to duplicate records. Cost and Payments Node failed due to an invalid reference fields cost center.
App filter and extensions Issue	Asset saves failed due to missing iscikey attribute in metadata. Asset extensions were not migrating due to an error in the upgrade scripts.
Heap fixes Issue.	Relationship audit history that is failed with a heap error. Asset audit history that is failed with a heap error.

Title	Description
Health Check Utility Issue	Health Check Utility processing MDB 1.5 definitions for Table Reference Diagnosis. This is invalid as it runs against MDB 1.4 database.

Enhancements

The CA APM Migration Utility patch includes the following enhancements:

1. If the upgrade script fails, the database installation stops.
2. Roll back schema objects is available in upgrade scripts when the MDB script fails.
3. A security warning dialogue box appears when you try to run the Health Check Utility again. You can click **Yes** to continue or **No** to discard.

Troubleshoot the CA APM Migration Utility

This article contains the following topics:

Web Servers Named with Underscore Characters

Symptom:

Using underscore characters in web server host names cause problems when you log in to the product or when you use CA EEM for user configuration.

Solution:

If you are using a virtual or ghosted system, configure a new host name by creating another image without the underscore character. For a production system, add a host name to your internal Domain Name System (DNS) so that the product can be accessed with a different URL.

Audit History Migration Fails

Symptom:

After you execute the Migration Utility, the status icon for Audit History shows “Error” indicating the migration has failed and the migration utility logs shows the following message:

```
Audit History migration has aborted due to a history data conflict with the Group Separator. Contact CA Support to determine a unique Group Separator.
```

Solution:

Contact CA Support.

Migration Utility Class Error

Symptom:

When you try to launch the Migration Utility from the toolkit or command prompt, you get the following error message:

```
Could not find the main class: com.ca.core.gui.Appplication
```

Solution:

The error occurs if you have configured an incorrect path for the KETTLE_HOME. Ensure that the KETTLE_HOME environment variable is set to the path of Kettle which contains the folder “data-integration”. For example: C:\Program Files\Pentaho\Kettle\.

Duplicate Asset Name Configurator link fails to launch

Valid on Windows 2008 Operating System

Symptom:

You cannot execute the Duplicate Asset Name Configurator with User Access Control (UAC) turned ON.

Solution:

To execute the Duplicate Asset Name Configurator with UAC turned ON, launch the UI as an administrator.

- Right-click LaunchUI.bat and click Run as Administrator.

Implementing CA SAM with CA APM

This section contains the following articles:

CA SAM and CA APM Overview

CA APM coordinates with CA SAM to allow you to perform software asset management functions. CA SAM is the next evolution of software asset and compliance management, superseding CA Software Compliance Manager (CA SCM). See the product support site on CA Support Online for more information about the plans for CA Software Compliance Manager.

Note: We do not recommend that you manage software assets in CA APM. To take advantage of the enhancements that CA APM provides, we recommend that you use CA SAM to manage your software assets and licenses.

Important! If CA APM is integrated with CA SAM in your solution deployment, consider the following:

- To install/upgrade to CA SAM 3.6.5 or later, you must install/upgrade to CA APM 14.1.01 or later to be fully compatible with CA SAM.
- For older versions of CA APM (14.1 or older), you must not upgrade CA SAM to version 3.6.5 or later.

CA SAM provides the following advantages:

- Supports the process of determining your software license compliance position by comparing the number of available licenses with the number of used licenses.
- Integrates a software license import function into the CA SAM user interface.
- Facilitates the creation and maintenance of a software license catalog with detailed commercial information about the licenses.
- Assigns installation and usage data to defined products in the software license catalog.
- Performs software product recognition.
- Permits financial analysis of product prices, license costs, and contract payments (this function is available through an additional module).

If you implement both CA APM and CA SAM, you can coordinate the management of both hardware and software assets in your organization. CA APM maintains hardware asset data and CA SAM maintains software asset and license data. Common data that both CA APM and CA SAM require is shared.

CA APM and CA SAM Data Synchronization

The article contains the following topics:

When you implement CA APM with CA SAM, CA APM and CA SAM share data that is required for hardware and software asset management. To maintain the integrity of the data and of the asset management process, data must be synchronized between CA APM and CA SAM. Data synchronization ensures that objects that are the same in both CA APM and CA SAM contain the same data values. This data synchronization occurs in the following ways:

- Automatic - When you create, update, or delete the following objects in CA APM (through the user interface, web services, or Data Importer), the objects are automatically synchronized in CA SAM. Create, update, or delete the following objects in CA APM only.
  - Company
  - Location
  - Cost center
  - Division
  - Contact

Important! The CA SAM Administrator must designate these objects as read-only in CA SAM to prevent any unauthorized change and to ensure that data is synchronized correctly. For more information about this requirement, see Data Management Recommendations. For more information about designating objects as read-only in CA SAM, see the CA SAM documentation.

Note: These objects use the same labels in CA APM and CA SAM, except Contact. In CA SAM, the Contact object is labeled "User".

For Contact, Company, and Location, the automatic synchronization occurs for specific data types only as shown in the following table:

Object	Automatically Synchronize when Type Is
Contact	User
Company	Internal
Location	NULL

- Manual - When you create or update the following objects in CA APM or CA SAM, synchronize the objects manually. Create or update the following objects in CA APM or CA SAM.
  - Country
  - Region

For example, if you create a Country object in CA SAM, manually create the same object in CA APM. If you update a Region object in CA APM, manually update that object in CA SAM.

Note: For more information about manual data synchronization, see the Data Management Recommendations.

- Data Loading - When you upgrade to CA APM Release 12.9 from a previous CA APM Release 12.6 installation, you can load your existing CA APM data for Company, Location, Cost center, Division, and Contact into CA SAM. For more information about data loading, see Load CA APM Data into CA SAM (see page 389).

Note: If you are implementing CA APM with an existing instance of CA SAM, there is existing CA SAM data that has not yet been synchronized. Before you start the automatic synchronization process, synchronize the existing CA SAM data with the CA APM data. For more information, see the following article on the CA SAM product page (https://support.ca.com/irj/portal/prddtlshome?prdhmpgform=p&productID=8572) on CA Support, Recommended Reading section: "How to Synchronize CA APM Data with an existing CA SAM Instance".

How to Configure Data Synchronization

You can configure the automatic data synchronization of CA APM and CA SAM data to suit your particular business needs. You can configure the type and attributes of the objects that are synchronized. You can also configure the criteria that are used to select the data rows for synchronization. To configure the data synchronization, edit the configuration file SAMDataSynchConfig.xml.

Important! The product installation saves the data synchronization configuration file SAMDataSynchConfig.xml with default settings for the data attributes and criteria. You modify this file *only* if you want to customize the default settings.

You can find the data synchronization configuration file in the following Event Service and Application Server folders:

```
<InstallFolder>\CA\ITAM\EventService\SAMDataSynchConfig.xml
<InstallFolder>\CA\ITAM\Application Server\SAMDataSynchConfig.xml
```

Note: If you change the configuration file in one of the folders, make the same changes to the configuration file in the other folder.

Example SAMDataSynchConfig.xml Configuration File Structure

The following example shows a section of the configuration file with the following changes to the default attributes and criteria:

- APMCriteria statements (highlighted) - Analyst was added as a criterion for the CA APM contact attribute (contacttype.value). User is the default criterion.

- SamField statements (highlighted) - CA APM contact (contactid) was mapped to the CA SAM user (import_user_id). The default statement (commented out in the example) mapped the CA APM asset owner (resourceownerid) to the CA SAM user (import_user_id).

```
<SamTable apmsyncclass="contact" samsynctable="users" >
   <SamField apmattribute="individualid" samattribute="import_id" />
   <SamField apmattribute="emailid" samattribute="login" />
   <SamField apmattribute="costcenterkey" samattribute="import_level_2_id" />
   <SamField apmattribute="lastname" samattribute="last_name" />
   <SamField apmattribute="firstname" samattribute="first_name" />
   <SamField apmattribute="emailid" samattribute="email" />
   <APMCriteria>
    <Criteria apmattribute="contacttype.value" value="User" />
    <Criteria apmattribute="contacttype.value" value="Analyst" />
   </APMCriteria>
</SamTable>
<SamTable apmsyncclass="asset" samsynctable="devices" >
   <SamField apmattribute="costcenterkey" samattribute="import_org_level_2_id" />
   <SamField apmattribute="locationid" samattribute="import_location_id" />
   <!--<SamField apmattribute="resourceownerid" samattribute="import_user_id" />-->
   <SamField apmattribute="contactid" samattribute="import_user_id" />
</SamTable>
```

The following terms in the example require explanation:

- **SamTable**
  Specifies the XML node that represents the mapping of the CA APM and CA SAM data objects or table.

- **Apmsyncclass**
  Specifies the name of the data synchronization object in CA APM.

- **Samsynctable**
  Specifies the name of the database table that the CA APM objects map to in CA SAM.

- **SamField**
  Specifies the XML node that represents the mapping of CA APM and CA SAM attributes.

- **Apmattribute**
  Specifies the CA APM attribute of the data synchronization object. To generate the name of the attribute, log in to the CA APM database using a database client tool and execute the following query:

  ```
  select attribute_name, class_name, table_name, field_name from arg_attribute_def where class_name='object_name';
  ```

  Use the value of the attribute_name column as the value for the Apmattribute XML attribute in the configuration XML.

- **Samattribute**
  Specifies the field name in the database table that the CA APM attributes map to in CA SAM. For the list of CA SAM objects and attributes, see the *CA Software Asset Manager Administration Manual.*

- **APMCriteria**
  Specifies the XML node that holds one or more child criteria nodes.

- **Criteria**
  Specifies the XML node that represents the criteria that is applied with the OR connector in the CA APM database table.

Data Synchronization Configuration Limitations

The following limitations apply to the changes that you can make to the data synchronization configuration file:

- You can change the mapping of attributes within a data object. You cannot change the mapping at the object level. For example, you cannot map the CA APM Location with the CA SAM User. You can map the CA APM Location with the CA SAM Location only.

- You can add columns under criteria. For example, the Contact object has User as the default Contact Type. As a result, all the data rows in the Contact object with Contact Type of User are selected for data synchronization. You can add other criteria. The following statements show a sample of how to add criteria:

```
<APMCriteria>
    <Criteria apmattribute="contacttype.value" value="User" />
    <Criteria apmattribute="contacttype.value" value="Analyst" />
    <Criteria apmattribute="costcenter.value" value="NewCostCenter" />
</APMCriteria>
```

  These statements specify the following selection criteria for data synchronization:

  - All Contacts with a Contact Type equal to User or Analyst
  - All Contacts with a Cost Center equal to New Cost Center

- Each criteria XML node can have only one value. For example, the default criteria value for Contact Type is User. More values (for example, “Analyst” or “Employee”) can be added (or removed). However, you cannot have “Analyst, Employee” as the criteria value. Create a criteria XML node for each unique value.

Add an Attribute

You can add an attribute to the data synchronization configuration file. You can also change an existing attribute in the file by editing an existing statement.

Follow these steps:

1. Create a SamField node by adding the following statement under the existing SamField nodes:

   ```
   <SamField apmattribute="attribute_name" samattribute="attribute_name" />
   ```

Note: Perform the following steps to identify the values that are needed for this statement.

2. Execute the following query on the CA APM database using a database client tool:

```
select class_name, attribute_name, table_name, field_name
from arg_attribute_def where class_name='object_name';
```

3. In the query results, copy the attribute_name value that was generated in the previous step. Paste this value in your new SamField node statement as the apmattribute value.

4. Access the *CA Software Asset Manager Administration Manual,* Data Imports chapter, and locate the field tables in the Formats section.

5. Copy the appropriate field name and paste it in your new SamField node statement as the samattribute value.

Note: For help with selecting the appropriate CA SAM fields, contact CA Services.

Add Criteria

You can add criteria to the data synchronization configuration file to expand the data values that are selected for data synchronization.

Follow these steps:

1. Create a criteria node by adding the following statement under the existing criteria nodes:

```
<Criteria apmattribute="value" value="value" />
```

Note: Perform the following steps to identify the values that are needed for this statement.

2. Execute the following query on the CA APM database using a database client tool:

```
select class_name, attribute_name, table_name, field_name
from arg_attribute_def where class_name='object_name';
```

3. In the query results, copy the attribute_name value that was generated in the previous step. Paste this value in the new criteria node statement as the apmattribute value.

4. Provide the criteria values by completing the following steps:

    a. Execute the following query:

```
Select field_name, table_name from arg_attribute_def where class_name =
'<apmsyncclass value>' and attribute_name = <apmattribute value>.
```

b. In the query results, select the field_name from the table_name.

c. Copy the field value and paste it in the *value="value"* parameter from Step 1.

Note: Create a separate criteria node for each unique value that you want to synchronize.

How to Implement CA SAM with CA APM

Perform the following steps to implement CA SAM with CA APM:

1. Review the prerequisites (see page 382).
2. Configure the CA APM Event Service for CA SAM (see page 383).
3. Configure the SAM Import Driver (see page 384).
4. Schedule the Windows task for the Hardware Import (see page 385).
5. Start the CA APM Event Service (see page 386).
6. Enable the software asset management capabilities (see page 386).
7. Load CA APM data into CA SAM (see page 389).

Note: To implement CA SAM, you also need to download the latest version of the CA SAM Catalog from CA Support Online and apply the Catalog in CA SAM. You can perform the Catalog download before or after you implement CA SAM with CA APM. For information about the CA SAM Catalog, see the CA SAM documentation (https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=fd1d7034-8f4f-4f28-9de8-3a9f503e9b2a&productID=8572).

Review the Prerequisites

Review the following prerequisites to ensure that you can successfully implement CA SAM with CA APM.

- You installed CA APM.

Important! Verify that the CA APM workflow provider URL is accessible and the corresponding login credentials are valid.

> **Note:** If your CA APM environment integrates with CA Service Desk Manager (CA SDM), verify that you have enabled the CA SDM audit history.

- You installed CA SAM from the CA SAM installation media. For information about installing CA SAM, see the CA SAM documentation (https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=fd1d7034-8f4f-4f28-9de8-3a9f503e9b2a&productID=8572).

  > **Important!** Microsoft .NET Framework 4.0 must be installed also on the CA SAM server.

  If you are using CA SAM to manage software assets for more than 250,000 hardware assets, we recommend the following installation configuration for improved system performance:

  - Install a CA SAM staging server for processing discovery data only. Implement the staging server on a MySQL database for improved performance and scalability.
  - Install the CA SAM production server on either a SQL Server or an Oracle database.
  - Transfer the discovery data to the CA SAM production server when processing is complete on the staging server.

- You installed CA SAM version 3.5.1 or later.
- (Optional) You verified and uninstalled CA SAM Import and Export Service.
  CA SAM Import and Export Service is no longer required to implement CA SAM with CA APM. If you are upgrading from CA APM 12.7, 12.8, or 12.9, we recommend that you uninstall the CA SAM Import Export Service.

Configure the CA APM Event Service for CA SAM

Configure the CA APM Event Service by validating or editing the parameters on the CA APM Administration tab.

Follow these steps:

1. Log in to CA APM on the web server as the administrator.
2. Navigate to Administration, System Configuration, Event Service page.
3. Click Show Advanced Options.
   The parameters that apply to CA SAM appear.
4. Validate or edit the values in the following parameters:

- **Interval between Event Occurrence check (in milliseconds)**
  The amount of time, in milliseconds, that CA APM waits between database checks for field changes related to defined events.
  If SAM capabilities are enabled, verify that this parameter is set to 30000. If SAM capabilities are not enabled, verify that this value matches the setting in the Event Service configuration

file.
Default (without CA SAM implementation): 3600000 (1 hour)
Default (with CA SAM implementation): 30000 (30 seconds)

- **Interval between triggering events check (in milliseconds)**
  Amount of time, in milliseconds, that CA APM waits between database checks for triggered events that need to be sent to the workflow provider.
  If SAM capabilities are enabled, verify that this parameter is set to 60000. If SAM capabilities are not enabled, verify that this value matches the setting in the Event Service configuration file.
  Default (without CA SAM implementation): 3600000 (1 hour)
  Default (with CA SAM implementation): 60000 (60 seconds)

- **Interval between triggered events status update (in milliseconds)**
  The amount of time, in milliseconds, that CA APM waits between updates to the status of triggered events that were sent to the workflow provider.
  If SAM capabilities are enabled, verify that this parameter is set to 60000. If SAM capabilities are not enabled, verify that this value matches the setting in the Event Service configuration file.
  Default (without CA SAM implementation): 3600000 (1 hour)
  Default (with CA SAM implementation): 60000 (60 seconds)

- **Interval between asset contact update (in milliseconds)**
  The amount of time, in milliseconds, that CA APM waits between updates to asset contacts in the CA CMDB.
  Default: 43200000 (12 hours)

- **CA SAM Status Update Frequency**
  The frequency for updating the status of CA SAM import jobs in the MDB (in milliseconds).
  Default: 120000 (120 seconds)

- **On Demand Max Threads**
  The maximum number of threads for processing the data synchronization between CA APM and CA SAM. The default (zero) indicates that the system creates the required number of threads, depending on the system hardware configuration. Any value other than the default value uses the same number of threads, regardless of the system configuration.
  Default: 0

- **CA SAM Events Notification Email**
  The CA APM administrator email address for receiving notifications about the CA SAM data synchronization.

- **Query Top**
  The number of triggered events that are processed at one time.
  Example: This value is set to 1000 and 1500 events are triggered. The first processing pass processes the first 1000 records, and the next processing pass processes the remaining 500.
  Default: 1000

Configure the SAM Import Driver

Configure the SAM Import Driver by validating or editing the parameters on the CA APM Administration tab.

Follow these steps:

1. Log in to CA APM on the web server as the administrator.
2. Navigate to Administration, System Configuration, SAM Import Driver page.
3. Validate or edit the values in the following parameters:
   - **ITAM Root Path**

     The path to the root location where the product is installed.
   - **File Path**

     The path to the root location where CA SAM export files are imported.

     Example: [ITAM Root Path]\ITAM\Import Driver\Input
   - Import Processor Executable Path

     The path to the Data Importer Processor executable file (ImportProcessor.exe)

     Example: [ITAM Root Path]\ITAM\Import Processor\ImportProcessor.exe

Schedule the Windows Task for the Hardware Import

Use the Windows Task Scheduler to schedule a task to import into CA APM the discovered hardware data from CA SAM. The following procedure schedules the import to run once every day.

Note: While this procedure describes the use of the Windows Task Scheduler, you can also use another task scheduler or process orchestration tool.

Follow these steps for Windows Server 2008:

1. From the Start menu on the CA APM application server, open the Windows Task Scheduler. For example, on Windows Server 2008, go to Control Panel, System and Security, Administrative Tools, Schedule Tasks.
2. Click Create Task.
3. On the General tab, enter a name for the task.
4. Select the check box for “Run whether user is logged in or not”.
5. Navigate to the Actions tab and click New.
6. In the Action field, select Start a program.
7. In the Program/script field, browse to locate the Import Driver Program folder, select the ImportDriver.exe file, and click OK.

8. Navigate to the Triggers tab and click New.
9. In the Settings field, select Daily.
10. In the Start field, select 12:00:00 AM.
11. Select Recur every 1 day and click OK.
12. On the Create Task dialog, click OK.
    You have completed scheduling the Windows task to import discovered hardware data.

Start the CA APM Event Service

If you are upgrading from a previous CA APM release, you start the CA APM Event Service to complete the implementation of CA SAM with CA APM:

Follow these steps:

1. From the Start menu on the CA APM application server, open the Control Panel, Administrative Tools, Services.
2. Locate the entry for the CA Asset Portfolio Management - Event Service.
3. Right-click the service and select Start.
   The service is started.

Enable Software Asset Management Capabilities

After you install and configure all CA APM components, you then enable the software asset management capabilities.

If you currently have an integration between CA APM and CA Software Compliance Manager (CA SCM), uninstall CA SCM before you enable software asset management capabilities. For information about uninstalling CA SCM, see How to Uninstall CA Software Compliance Manager (see page 395). For more information about how and when to uninstall CA SCM, contact your CA Services representative.

Note: If you enabled software asset management capabilities in a previous release and you are now upgrading, skip the following steps. However, update the web.config configuration file on the CA APM web server to refer to the CA SAM section of the common home page. Update the following statement:

```
<add key="CASAMWebClientUrl" value="http://CA_SAM_server_name/prod" />
```

Example:

```
<add key="CASAMWebClientUrl" value="http://itamsam/prod" />
```

Follow these steps:

1. Log in to CA APM on the web server as the Administrator.

2. Navigate to Administration, System Configuration, Software Asset Management.

3. Complete the requested information. The following fields require explanation:

   CA SAM Web Client URL
   Specifies the URL for the CA SAM home page.
   Note: You can copy the web client URL from the CA SAM home page after you log in.

   Enable SAM Capabilities
   Specifies that software asset management capabilities are enabled. If you previously had CA SCM fields on the CA APM user interface, they are removed after you select this check box.

   CA SAM Web Service WSDL URL
   The URL for the CA SAM Web Service Definition Language (WSDL). This URL is used to access the CA SAM web service. Use the following format:

   ```
   http://[CA SAM System Name]:[Port Number]/prod/soap/dyn_server.php
   ```

   Replace [CA SAM System Name] with the name of the CA SAM server.
   Replace [Port Number] with the port number where the CA SAM Web Service is hosted.

   CA SAM Web Service Login
   Login name for the CA SAM web service.
   Note: Verify that this login name and the CA SAM Web Service Password match the login name and password in the config_soap.inc file. This file is found in the following CA SAM installation folder path:

   ```
   app\includes\prod\st\config_soap.inc
   ```

   Important! The default content of the config_soap.inc file is commented. Remove the comment delimiters (/* */) and configure the login name and password.

   CA SAM Web Service Password
   Login password for the CA SAM web service.

   CA SAM Database Type
   Specifies the Database type of SAM server.
   Default: SQL Server

   CA SAM Data exchange directory
   Specifies the name of the Data Exchange directory on SAM server used for Data synchronization.
   Example: external
   Default: superuser

   CA SAM SSO Encryption Algorithm
   Specifies the encryption algorithm to be used for single sign-on access to CA SAM from the CA Asset Portfolio Management common home page.
   This entry must match the entry in CA SAM System Configuration for the

security_auth_token_cipher field.
For more information about CA SAM single sign-on, see the description of single sign-on in the *CA Software Asset Manager Administration Manual*.

CA SAM SSO Encryption Algorithm
Specifies the encryption algorithm to be used for single sign-on access to CA SAM from the CA Asset Portfolio Management common home page.
This entry must match the entry in CA SAM System Configuration for the security_auth_token_cipher field.
Note: For more information about CA SAM single sign-on, see the description of single sign-on in the *CA Software Asset Manager Administration Manual*.

CA SAM SSO Authentication Mechanism
Specifies the mechanism to be used for logging in to CA SAM.
This entry must match the entry in CA SAM System Configuration for the security_auth_method field.
Note: We recommend that you select auth_token_password for this mechanism. The auth_token mechanism disables the login for other CA SAM users.

CA SAM SSO Field to Authenticate User
Specifies the type of unique identifier (import ID or email address) that is used to authenticate the user.
This entry must match the entry in CA SAM System Configuration for the security_auth_token_user_identifier field.

CA SAM SSO Secret Key
Specifies the key that CA APM and CA SAM share and that is used to encrypt and decrypt the user authentication. This key ensures that CA APM users who do not have the proper authentication cannot access CA SAM.
This entry must match the entry in CA SAM System Configuration for the security_auth_token_key field.

4. Click Save.

5. Restart the Apache Tomcat Common Asset Viewer service.

Note: Also restart the Apache Tomcat Common Asset Viewer service if you change the entries in any of the following fields at a later time:

6. Restart Internet Information Services (IIS) on the CA APM web servers and application servers by executing the iisreset command.

7. Software asset management capabilities are enabled, and CA SCM fields are removed from the CA APM user interface.

The Load Data button is enabled if CA APM data exists (for example, if you had an existing CA APM 12.6 installation and you are upgrading). You can then load existing CA APM data for selected objects into CA SAM. For information about loading data, see Load CA APM Data into CA SAM (see page 389). This button is not enabled if you are performing a new installation of CA APM. You do not have existing data with a new installation.

Common Home Page Single Sign-On

When the CA SAM implementation is complete, the CA IT Asset Manager common home page displays Hardware and Software Asset Management dashboards. These dashboards contain links that open pages in CA APM and CA SAM. After you log in to CA APM and open the common home page, you can access CA SAM pages without logging in to CA SAM.

To implement the single sign-on, verify that the following steps are completed:

1. The user ID in CA APM exists as a user ID in CA SAM, also.
2. The user email address and Import ID in CA SAM match the user email address and Contact ID in CA APM.
3. The CA SAM user is authorized to perform CA SAM functions.
    a. Access the CA SAM user details page by selecting Organization, User, and then editing an existing user record or creating a user record.
    b. Select the check box for CA Software Asset Manager authorization.

Load CA APM Data into CA SAM

After you enable software asset management capabilities in CA APM, you can load existing CA APM data for selected objects into CA SAM. This data load allows you to synchronize the data so that objects that match in CA APM and CA SAM have the same data values. The CA APM data that you can load includes the following objects:

1. Location
2. Division
3. Company
4. Cost Center
5. Contact

If you had a previous installation of CA APM, you have existing CA APM data for these objects. If you are performing a new installation of CA APM, you do not have any existing data.

Note: Before you load CA APM data into CA SAM, verify that your CA APM data meets CA SAM requirements. These requirements are defined in Field Requirements for Automatic Data Synchronization.

Follow these steps:

1. On the Administration, System Configuration, Software Asset Management page, verify that the Load Data button is enabled.

> **Note:** The Load Data button is enabled if CA APM data exists (for example, if you had an existing CA APM 12.6 installation and you are upgrading).

2. Click Load Data.
   The data load copies the Location, Division, Company, Cost Center, and Contact object values to CA SAM. A status table displays the progress of the data load.
   If some of the objects fail to synchronize with CA SAM, the error records are written to a log file. You can view this log file by clicking the Get Error Records button. The Get Error Records button is available only after you enable SAM capabilities.

3. Click Get Error Records to verify if any data synchronization errors occurred.
   You are prompted to open or save a CSV file. If errors exist in the CSV file, the errors are grouped by object in the following order:

   a. Location

   b. Division

   c. Company

   d. Cost Center

   e. Contact

4. Review the errors and explanations in the CSV file and correct the CA APM object data.
   The corrected objects are synchronized with CA SAM during the next data synchronization.

How to Implement Multi-tenancy with CA SAM

If you implemented multi-tenancy and your tenants require to perform software asset management functions, you can integrate each tenant with CA SAM. For example, you manage 20 tenants and only 12 of them require software asset management functions. You can integrate each of these tenants with CA SAM separately.

To implement multi-tenancy, create a CA SAM instance for each tenant on CA APM. For example, if you manage ten tenants using CA APM, you must install CA SAM on ten different computers. Each installation of CA SAM corresponds to a single tenant.

If you configured multiple tenants in CA APM to a single instance of CA SAM, discovered asset information is updated based on the matching asset details. However, if the discovered asset is a new asset, CA APM creates a new asset but is not assigned to any tenant.

Important! You cannot integrate a tenant group with CA SAM.

When you integrate a tenant with CA SAM, CA APM creates a data synchronization configuration file with the name SAMDataSynchConfig-*<Tenant Name>*.xml. For example, if the name of the tenant is Tenant1, data synchronization configuration file is named SAMDataSynchConfig-Tenant1.xml.

For more information on data synchronization, see CA APM and CA SAM Data Synchronization (see page 376).

Note: When you implement multi-tenancy with CA SAM, public data is not synchronized.

To implement multi-tenancy with CA SAM, perform the following steps :

- Identify the tenants that require integration with CA SAM.
- For each tenant you identify, determine the computer on which you plan to install CA SAM. For information on CA SAM system requirements, see CA SAM documentation (https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=fd1d7034-8f4f-4f28-9de8-3a9f503e9b2a&productID=8572).
- Map the tenant in CA APM to the instance of CA SAM. See Configure CA SAM Settings for a Tenant (see page 391).

Configure CA SAM Settings for a Tenant

After you install CA SAM on the computers that you identified, map each tenant in CA APM to the respective instance of CA SAM. You can perform the mapping by specifying the CA SAM settings for each tenant in the System Configuration page.

Follow these steps:

1. Log in to CA APM on the web server as the administrator.
2. Navigate to Administration, System Configuration, Software Asset Management.
3. In the APM Tenant drop-down list, select the tenant for which you want to specify the CA SAM settings.
4. Specify the requested information and click Save.

For information on the CA SAM configuration settings, see Enable Software Asset Management Capabilities (see page 386).

Data Management Recommendations

Contents

The recommendations in this section help you manage your data when CA APM is implemented with CA SAM.

Manual Data Synchronization

Data must be synchronized between CA APM and CA SAM to maintain the integrity of the data and of the asset management process. Data synchronization ensures that objects that are the same in both CA APM and CA SAM contain the same data values.

When you create or update the Country and Region objects in CA APM or CA SAM, synchronize the objects manually. For example, if you create a Country object in CA SAM, manually create the same object in CA APM. If you update a Region object in CA APM, manually update that object in CA SAM.

Manual Data Synchronization Rules

To ensure that data is synchronized correctly, use the following rules when you create or update the Country and Region objects:

- Country - The CA APM abbreviation for a country must match the CA SAM record import ID for the same country.
- Region - The CA APM name for a region must match the CA SAM record import ID for the same region.

Cost Center Data Management

The data synchronization between CA APM and CA SAM ensures the integrity of the data and of the asset management process. This synchronization occurs automatically for the following objects:

- Company
- Location
- Cost Center
- Division
- Contact

Note: These objects use the same labels in CA APM and CA SAM, except Contact. In CA SAM, the Contact object is labeled "User".

When you create, update, or delete the Contact, Company, Location, and Division objects in CA APM, the objects are automatically synchronized in CA SAM. The CA SAM Administrator must designate Contact, Company, Location, and Division as read-only in CA SAM. This action prevents CA SAM users from changing these objects, which will be overwritten when the next data synchronization occurs. However, the Administrator cannot designate the Cost Center object as read-only in CA SAM because the Cost Center reporting hierarchy must be administered in CA SAM.

Recommended Guidelines for Cost Center Data Management

To facilitate Cost Center data management, we recommend that you use the following guidelines:

- Add permissions to manage the Cost Center object to an Administrator role in CA SAM. Other user roles are not able to access the Cost Center object.
- Use CA APM when you perform the following actions:
  - Insert or delete Cost Centers.
  - Update Cost Center name or description.

  Important! If you change the Cost Center name or description in CA SAM, the changes are overwritten after the next data synchronization.
- Use CA SAM when you perform the following actions:
  - Administer Cost Center reporting hierarchy.
  - Assign a Cost Center to a country.

Inventory Units of Measurement

CA SAM sends hardware discovery data to CA APM to help with hardware asset management. CA APM requires specific units of measurement for the following hardware inventory items that are sent from CA SAM:

- Total Disk Space: Gigabytes (GB)
- Total Memory: Megabytes (MB)
- Processor (CPU) Speed: Megahertz (MHz)

When you load and manage hardware inventory data for these items in CA SAM, verify that the CA SAM data uses these units of measurement.

Field Requirements for Automatic Data Synchronization

Automatic data synchronization copies the CA APM data for the Company, Location, Cost Center, Division, and Contact objects to the corresponding objects in CA SAM. To ensure a successful synchronization, follow the field requirement guidelines for the objects in the following subsections.

Contact

Some of the fields for the Contact object are optional in CA APM but required in CA SAM. These fields are summarized in the following table. Verify that all fields that are required in CA SAM contain data in CA APM.

CA APM Field	Required in CA APM?	Required in CA SAM?
User ID/User Name	No	Yes
Cost Center	No	Yes
Last Name	Yes	Yes

First Name	No	Yes

Company

CA SAM allows you to report compliance for hierarchical groupings (Division, Company, and Cost Center). To report on Divisions, CA SAM requires Division details for the Company object. Verify that the CA APM Company object has Division details to ensure a successful data synchronization.

Note: To enter Division details for a company in CA APM, you first create divisions in Directory, List Management, Company Lists, Division. Then when you create or update a company on the Company Details page, select a Company Type of Internal. The Division text box appears and you can select a division for the company.

Cost Center

CA SAM allows you to report compliance for hierarchical groups (Division, Company, and Cost Center). To report on Companies, CA SAM requires Company information for the Cost Center object. Verify that the CA APM Cost Center object has Company details to ensure a successful data synchronization.

Assets with Undefined Operating Systems

Discovery data that CA APM receives can contain operating system names that are not defined in CA APM. When this situation occurs, CA APM assigns an operating system value of Undefined to the corresponding asset. CA APM displays the Undefined value in the Operating System field on the Asset Details page.

You can view the original discovered names of the Undefined operating systems, and you can add those names to the CA APM operating system names. You can also update the assets that have Undefined operating systems to include the new names.

Note: CA APM can receive data with undefined operating systems from any discovery source (including CA SAM).

Follow these steps to view the original names of Undefined operating systems:

1. Log in to CA APM as the administrator.
2. Navigate to Administration, Reconciliation Management, Reconciliation Message Search. A list of Reconciliation messages displays.
3. Locate the messages that identify the missing operating systems.

Note: You can search on this page for "Missing Operating System" in the message text.

The messages include the original discovered names.

Follow these steps to update assets with Undefined operating systems:

1. Navigate to Directory, List Management, Operating System and add the missing operating system names to the CA APM names.
2. Update an individual asset with an Undefined operating system by using the following steps:
    a. Navigate to the Asset Details page for an asset with an Undefined operating system.
    b. Click the Select New icon in the Operating System field and select the new name.
3. Update multiple assets with Undefined operating systems by using the following steps:
    a. Navigate to Administration, Reconciliation Management.
    b. Click the reconciliation rule name.
    The Reconciliation Rule Details page appears for the selected rule.
    c. Verify that Monitor Asset Updates is selected.
    d. In the Update Options area, select Operating System and Last Run Date.
    e. Click Save.
    When CA APM receives new discovery data for assets with Undefined operating systems, CA APM updates the operating systems with the new names that you entered.

How to Uninstall CA Software Compliance Manager

To enable SAM capabilities when CA APM is integrated with CA Software Compliance Manager (CA SCM), uninstall CA SCM.

Note: Verify that all users have logged out from CA SCM. Any user who does not log out from the product before the uninstallation begins receives an error when attempting to complete a task.

Follow these steps to uninstall CA SCM 12.0:

1. Log in to the computer on which you installed CA SCM 12.0.
2. Uninstall the CA SCM Release 12.0 cumulative patches, if any, through the Control Panel, Add /Remove Programs.

3. Log in to the CA APM application server where you installed CA APM Release 14.1.
4. Navigate to the folder where you installed CA APM Release 14.1.
5. Copy the SWCM12.0Uninstall folder and all of its contents to a temporary location on each computer (except the database server) where you installed CA SCM 12.0.
   Example of temporary location:

   ```
   C:\Windows\Temp
   ```
6. Navigate to the Uninstall folder in the temporary location on the CA SCM 12.0 computer.
7. Start the uninstallation by double-clicking the SWCM_Uninstall.bat file.
8. Follow the on-screen instructions in the uninstallation process.
   The uninstallation runs and successfully removes all installed CA SCM 12.0 components, except CA Business Intelligence, CA EEM, CA MDB, and the Content Import Client.

Follow these steps to uninstall CA SCM 12.6:

Note: Complete these steps on each computer (except the database server) on which you installed CA SCM 12.6.

1. Log in to the computer on which you installed CA SCM 12.6.
2. Uninstall the CA SCM Release 12.6 cumulative patches, if any, through the Control Panel, Add /Remove Programs.
3. Navigate to the Uninstall folder where CA SCM 12.6 is installed.
   Example:

   ```
   C:\Program Files\CA\SWCM\Uninstall
   ```
4. Start the uninstallation by double-clicking the SWCM_Uninstall.bat file.
5. Follow the on-screen instructions in the uninstallation process.
   The uninstallation runs and successfully removes all installed CA SCM 12.6 components, except CA Business Intelligence [assign the value for boe in your book], CA EEM, CA MDB, and the Content Import Client.

Step 1 - Plan Your CA Asset Portfolio Management Installation

This article contains the following topics:

Before you begin with the installation, ensure that you have completed the following:

- Reviewed the CA Service Management Release Notes (see page 69).

- Reviewed the supportability matrix (see page 119) for a list of third-party software products that are certified for use with CA Asset Portfolio Management.
- Considered and planned for the network availability, usage bandwidth, and responsiveness.
- Reviewed the CA APM product components (see page 319).

Step 1c - Complete the Planning Checklist

Ensure to review and complete the following CA IT Asset Manager Installation Planning Checklist:

Select	Task	Comments
	Ensured that the servers meet the hardware and software requirements (see page 397).	
	Installed Internet Information Services (IIS) 7.0 or above on all the application and web servers..For more information, see Verify that Internet Information Services (IIS) 7.0 or above. (see page 397)	
	Installed Microsoft .NET Framework 4.0 or above.	
	Installed Microsoft Web Services Enhancements (WSE) 3.0 Runtime.	
	Common Components: Installed CA EEM, CA Business Intelligence, and CA Process Automation. ▪ **CA EEM**: Installed CA EEM 12.51 CR02 using the CA Service Management Installation Media or upgraded an earlier installed version of CA EEM to CA EEM 12.51 CR02. For more information, see Install CA EEM (see page 283). Installed CA iTechnology iGateway with CA EEM. It is a shared component that various CA Technologies products use. CA iTechnology iGateway web server sends and receives requests using the http protocol. CA iTechnology iGateway can be installed with other CA products also. ⚠ **Note:** If CA iTechnology iGateway exists on the computer where you are installing CA EEM, determine if it is 32-bit or 64-bit. If CA iTechnology iGateway and your CA EEM 12.51 CR02 server are both 32-bit or both 64-bit, no action is necessary. However, if the two products do not match (for example, one is 32-bit and the other is 64-bit), remove CA iTechnology iGateway (see page 397) and start the CA EEM installation. The correct version of CA iTechnology iGateway is installed when you complete the CA EEM installation ▪ **CA Process Automation:** Installed CA Process Automation for event notification processing. For more information, see Install the CA Process Automation. (see page 292)	

Select	Task	Comments
	▪ **CA Business Intelligence**: Reviewed the CA Business Intelligence Integration (see page 547) content. Installed CA Business Intelligence and recorded the login credentials and connection information. For more information, see Install CA Business Intelligence (see page 285). **Note:** CA EEM is mandatory for CA Asset Portfolio Management while CA Process Automation and CA Business Intelligence are optional.	
	Installed CA SCM (and any cumulative releases) before installing CA Asset Portfolio Management to integrate CA SCM Release 12.6 with CA Asset Portfolio Management.	

Implementing CA Service Desk Manager

As an administrator, install or upgrade CA SDM to avail the service desk capabilities which is an integral part of the CA Service Management solution. This topic describes the planning process, the procedure to install or upgrade, and to configure the product after the installation.

For a successful CA SDM implementation in your enterprise, plan and perform the following steps:

- Plan and prepare for a new installation or an upgrade.
- Install or upgrade all of the necessary product components.
- Configure the product components.
- Integrate with the required CA Technologies products.

Note: This section does not detail integration with all CA Technologies products. For more information about CA SDM Integrations, see the CA Service Desk Manager Integration Best Practices Green Book at http://ca.com/support.

Audience

- System administrators, administrators, and implementation consultants: Install and configure CA SDM for the first time or to upgrade from an earlier version to the latest version.
- Integrators: Integrate CA SDM with the other CA Service Management products.

To implement CA SDM, the following prerequisites apply:

- A working knowledge of the Windows and/or UNIX operating systems, depending on your current production environment.

- The ability to perform basic administrative tasks for your operating system.
- Depending on your working environment, knowledge of mainframe, mobile devices, and server installations.

More Information:

- How to Upgrade CA SDM (see page 399)
- How to Install CA SDM (see page 446)
- How to Install CA SDM Connector (see page 525)
- Uninstall the CA SDM Connector (see page 542)

How to Upgrade CA SDM

You can upgrade CA SDM to the latest version using the migration console. Ensure that you read the planning process before you start the upgrade.

More Information:

- Step1: Plan the CA SDM Upgrades (see page 399)
- Step 2: Use the CA SDM Migration Console (see page 409)
- Step 3: Perform Post Upgrade Configuration (see page 419)
- Support Automation Data Migration (see page 442)

Step1: Plan the CA SDM Upgrades

This article contains the following topics:

General Considerations

- CA SDM supports upgrade from r11.2, r12.0, r12.1, r12.5, r12.6, r12.7, and r12.9 for all supported platforms. For Windows, you can upgrade directly from r11.2, r12.0, r12.1, r12.5, r12.6, r12.7, and r12.9.
- If you installed CA SDM on Linux or UNIX, the upgrade from versions prior to r12.5 requires multiple steps. If your installation is running on an older version of the product, such as r11.2, r12.0 and r12.1 on Linux/UNIX, you must run the automated upgrade script for CA SDM r12.5 and move CA SDM to a supported platform and database before running the automated upgrade script for the new release. If you have modifications, you only have to apply them once - after running the final automated upgrade script to the new release.
- If you have an earlier version of the product, such as CA Service Desk Manager r6.0 or r11.1, you *must* upgrade to CA SDM r11.2 before upgrading.

- You manually added a variable in the NX.env file or updated a variable value and want to retain these variables after the migration. Ensure that you add these variables to the NX.env template file before the configuration and migration.

- CA SDM only supports ITIL. If you are upgrading from a non-ITIL system, the installation updates you to an ITIL environment.

- If you have a combined CA SDM r11.2 and CA CMDB r11.1 installation, you cannot upgrade directly. You *must* first upgrade CA CMDB to r11.2, and then run the upgrade. This process upgrades CA SDM r11.2 to r12.5, and also upgrades CA CMDB r11.2 to r12.5. CA CMDB r12.0 and r12.1 can also be upgraded directly.

  Note: For more information about upgrading from an earlier version, see the *CA SDM Implementation Guide r11.2.* For upgrade patches and assistance, contact Technical Support at http://ca.com/support (http://www.ca.com/support).

- If you are planning to migrate from an earlier version of CA SDM to the current version, before migrating validate that the servlet path URL(in each Repository Server) is in the correct format. To validate, complete the following steps:

  1. Login to CA SDM.
  2. Navigate to **Administration**, **Attachment Library**, **Repository**.
  3. Edit each repository servlet path URL. Remove the Fully Qualified Domain Name (FQDN) from the servlet path and replace it with the hostname in the servlet URL.
     For example, change (http://myhostname.ca.com:8080/CAisd/UploadServlet) to (http://myhostname:8080/CAisd/UploadServlet)
     Ensure that the repository server functionality is intact and working.

- UTF-8 locale must be installed on Linux/UNIX platforms.

- On Linux/UNIX, CA SDM no longer uses the smtp_mail script to process outgoing mail notifications. If you are an existing customer using smtp_mail, and you upgrade to the current release, your administrator must configure the appropriate mail options using the Default Mailbox Detail page to enable the mail notification feature of CA SDM.

  Important! Migration from an advanced availability environment is not possible using rolling maintenance. You must shutdown the CA SDM services in all the application and standby servers before starting the migration activity. You need to first migrate the background server and then verify whether the background server processes are running. Migrate the other servers only after ensuring that the background server processes are running.

- Fresh CA SDM Release 14.1 installation does not install the copy_inactive web option in Options Manager. So the links to inactive objects are not copied. If you are upgrading from CA SDM r12.5 or r12.6, links to inactive objects are copied because migration installs the option.

- If a previous version uses *domsrvr:01*, rename the server ID before starting the upgrade. Execute the *pdm_edit.pl* command and update the domsrvr ID from 01 to another ID value.

  Note: The CA Service Desk Manager 14.1 enhances the *pdm_edit* command to provide an easier interface to configure the servers. As part of this enhancement, the *domsrvr:01* name for object manager is reserved and cannot be used by the custom configuration.

Database Considerations

- Before you migrate from CA SDM Release 12.7 SP2, ensure that you run the following command:

```
update mdb_schema_information set FileTimestamp='2012-04-23T09:19:09+0000'
  where FileName like 'doc_rep.xml'
```

- Back up your existing database using your typical database backup procedures.
- (Applicable for all non-windows machines) If the previous releases of CA SDM is configured with oracle 10gr2 database, install Oracle 11gr2 client before you upgrade.

  Important! Before upgrading, change the Oracle home path to oracle11g r2 client path in the $NXROOT/NX.env file.

- Archive the installation directory ($NX_ROOT) using your typical archive procedures. This action lowers the amount of data movement and saves disk space.
- Run the appropriate script from a command prompt to identify any duplicate records on your database:

  Note: Run this script on the secondary servers. If you want to run this script using SQL Query Analyzer, edit the **SQLCheckr12UniqueIndexes.sql** script and remove the EXIT argument before you run the command.

  - (Oracle) Run OracleCheckr12UniqueIndexes.sql, located in the \Migrate directory on the installation media.
- - (SQL Server)

    Note: The database is named as "use mdb" by default. Before you run the script, update the database name manually to **use <other_database_name>** using the **SQLCheckr12UniqueIndexes.sql** file.

    1. Open a Command Prompt window and run **SQLCheckr12UniqueIndexes.sql** as follows:

```
cd $NX_ROOT\samples\views\SQLServer
```

2. Enter the command:

```
Sqlcmd  - E  - e < SQLCheckr12UniqueIndexes.sql
```

Note: After you upgrade, you can find these files at *$NX_ROOT/samples/views/SQLServer* or *$NX_ROOT/samples/views/Oracle* on the server.

Important! These scripts identify your duplicate records. Delete identified duplicate records before you proceed with the migration.

- For Windows, you can upgrade directly from r11.2, r12.0, r12.1, r12.5, r12.6, r12.7, and r12.9.
- If you installed CA SDM on UNIX or Linux, you can upgrade from r12.5, r12.6, r12.7, and r12,9.
- If your installation contains an earlier version of the product, such as CA SDM r11.2, r12.0, or r12.1 on a non-supported UNIX/Linux operating system and database, you must upgrade to CA SDM r12.5. Then, move CA SDM to a supported operating environment and database before you upgrade.
- Upgrade your CA SDM r11.2 system to a supported database (SQL Server and Oracle).

  Note: For more information about supported database, see the Supportability Matrix (see page 119).

- Upgrade from CA Service Desk Manager r11.0 to CA SDM r11.2 before migrating your data to a supported database.
- Special Windows characters, such as a long hyphen, in CA SDM or Knowledge Management on a non-Windows system, are not properly stored in the database.
- **Ingres** -- If you are using an Ingres database, convert your data to Oracle or SQL Server before upgrading.

  Note: For information about the conversion process, see your database documentation.

- **Oracle** -- Oracle does not support case insensitive indexes for Configuration Item registration. Before you start the migration on Oracle, verify SQLPlus and Oracle DB are able to communicate using hostname. If communication fails, verify that Oracle is configured with loopback adaptor.

> **Note:** When you migrate in a double-byte character environment with an Oracle database, increase the maximum open cursor limit to at least 500. For more information, view Oracle documents about ORA-01000 (maximum open cursor exceeded).

- **SQL Server** -- For an SQL Server upgrade to the current release of CA SDM, the default database for the configured Database Userid must be CA MDB. If the default database is not CA MDB, the migration console fails and displays the following message:
  "The acctyp_v2 table does not exist on the MDB"

- **Tomcat** -- (for CA Service Desk Manager r11.0, r11.1 or CA SDM r11.2) If you configured Tomcat for external authentication, manually reconfigure Tomcat for external authentication after upgrading to the current product release.

- **Table Updates** -- Consider the following table updates that occur during migration:

  - **Status Tables** -- These tables are also updated with the appropriate status records when the same code values do not exist in your database. For example, *Cr_Status* is updated with the code *AEUR* (Awaiting End User Response).

  - **Functional Areas** -- For each role, migration automatically adds a row for each *usp_functional_access* record. Migration sets the access level to the same level for each CA SDM r12.0 and r12.1 functional area that the *usp_role* table includes. New functional areas are mapped using a reference field.

- **Foreign Keys** -- Consider the following information:

  - Foreign keys (SRELs) that reference tables, in which the primary key is a UUID, change from integer type to UUID type (or BYTE 16).

  - If you dropped foreign key constraints in your previous CA SDM system to mass load data, recreate the foreign key constraints before you run the upgrade. The scripts that drop the constraints are found in the following locations:

    - Oracle
      $NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql

    - SQL Server
      $NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql

    > **Note:** Reapply the dropped constraints by running the appropriate script *OracleAddConstraints.sql* or *SQLServer/SQLAddConstraints.sql*. These scripts are found in the same directory as the drop constraints and contain instructions within the files mentioned.

- **MDB** -- The MDB provides a consistent database schema for various IT management data. During the development of the MDB, data elements from your previous CA SDM environment were incorporated into this schema. The size of the data elements can increase and, consequently, increase the overall database size.

Note: When standard data elements extend beyond the column width defined for the MDB, the update process can truncate data in these elements. Messages alert you to any truncation that occurs during the upgrade.

- **Distributed Setup** -- We recommend you upgrade your servers in the following order, depending on your CA SDM configuration:

  1. **Conventional**
     - Primary server
     - (Optional) One or more secondary servers
  2. **Advanced Availability**
     - Background server
     - One or more standby servers
     - One or more application servers

- **Remote Database** -- If you are using a SQL Server MDB database, sqlcmd must be on the client computer before connecting to the remote MDB.

Knowledge Management Considerations

For customers upgrading from a previous release of CA SDM that used the FAST ESP search engine, you *must* change to the EBR search engine. The FAST ESP license expires in May 2013. To change to the EBR search engine, click Options Manager, Search Engine and edit ebr_version to specify KT Search Engine.

LREL Migration Considerations

A *List Relationship* (LREL) represents an association between two objects. An LREL has a left-hand side (lhs) and right-hand side (rhs) relationship. Each side of the relationship is an attribute of the majic object that contains the data relationship.

In previous releases of the product, .maj LREL statements and objects described many-to-many DBMS data relationships. Many-to-many relationships no longer use the LREL majic statement. Instead, individual tables store both sides of the relationship. Objects access the relationship with a standard BREL statement. For example, you can see the relationship between change orders and CIs by reviewing the new usp_lrel_asset_chgnr table and in the corresponding lrel_asset_chgnr object.

The LREL changes eliminate the need to store attribute names in the database. The two sides of the relationship are foreign key single relationships (SREL) that are easy to join and index. If necessary, the relationship can contain additional relational attributes.

During the upgrade, the following activities occur as LREL table data migrates to current release of CA SDM:

- The system automatically migrates tables and objects with LREL relationships.
- The system names new tables using the *usp_lrel_lhsName_rhsName* format.
  For example, the *usp_lrel_asset_chgnr* table has a left-hand relationship to assets and a right-hand relationship to change orders.
- The system names the corresponding objects using the *lrel_lhsName_rhsName*.
  For example, the *lrel_asset_chgnr* object corresponds to the *usp_lrel_asset_chgnr* table.
- Because of a database limitation, some names are abbreviated.
- Your data is migrated from the old tables and all CA SDM code is modified to use the tables of the updated release.
- The system no longer uses the old LREL database tables, such as *bmlrel*. However, for reference purposes, the old tables retain the data.
- A backward relation (BREL) attribute to the new object replaces the original LREL attribute in each related majic object definition.
- If you are using a supported API, such as the *CreateLrelRelationship()* web service method, the code works as expected.
- If you added any custom LREL style relationships, CA SDM migrates them to the tables of the updated release.
- Any site-defined code or reports that directly access the old LREL tables operate on old data because the system no longer uses those tables. We recommend that you update the code to use the tables of the updated release for the code and reports to run properly.

Important! If your code directly accesses legacy LREL objects or tables, the code fails after migration. We recommend that you upgrade the code before migration. For example, if your code uses majic statements to establish LREL relationships, use the *createLrelRelationships()* method instead of directly populating a table.

Note: We recommend that you verify site-defined code or reports that directly access the database or address the legacy LREL majic objects such as the lrel1 object to verify that they operate properly. You can update your code to use a supported interface, such as Web Services. You also update the necessary table names. For reports, you can also update the queries with the new DBMS table references.

Status Transition Considerations

Consider the following information if you plan to use Status Transitions after upgrading from CA SDM r11.2, r12.1, and r12.1:

- Status transitions are inactive when you upgrade.

  Note: All modified status code descriptions that appear on ticket forms are retained during the upgrade process.

- The *Status_Policy_Violations* option is installed and set to Warn by default after you upgrade. This setting allows undefined transitions to occur, but logs a warning.

- If you set the option to Allow, undefined transactions are not logged.

How to Upgrade CA EEM

The current version of CA SDM uses EEM 12.51 SDK which is not compatible with the EEM 8.4 server. To support the existing customers who are using EEM 8.4 server, EEM 8.4 SDK patch has to be applied on the CA SDM server. Find the patch details from the CA Support Online.

You install CA EEM separately.

When migrating, upgrade to at least CA EEM r8.4 SP4.

Note: You can upgrade from CA EEM r8.1 directly to r8.4 SP4.

To upgrade CA EEM, perform the following tasks:

1. Verify that you upgraded to the current version of CA SDM
2. Insert the installation media into your drive.
3. Install CA EEM.

After you install CA EEM, manually set the appropriate options in the Options Manager. Review the upgraded options carefully. The default Process Manager URL is no longer pmService.

Note: The *cawf_pm_url* option has changed to a default of: *http://<wf_hostname>:<wf_tomcat_port>/pm/service/pmService2*, so you *must* manually change "pmService" to "pmService2" for CAWF communication to remain functional.

Important! After you upgrade CA EEM, set the *eiam_hostname*, *use_eiam_artifact*, and *use_eiam_authentication* options in Options Manager, Security if you previously used eIAM CA SDM user authentication.

CA Process Automation Integration

To ensure that CA SDM and CA Process Automation integration works properly, add the ServiceDesk user in CA EEM (if not already added) during the upgrade.

Retain Your Modifications

Before you upgrade, consider the following information to retain the modifications that you have made:

- Any “modifications” or “adaptions” or “configurations” that are done administratively through the interface (web browser, command-line, Web Screen Painter) are “supported”, meaning CA Support can assist with the basic suggestions and troubleshooting. CA Support do NOT perform any changes for the customer. The customer is responsible for the changes made. For example, adding a field to a table and putting the field on a form through Web Screen Painter is a fully supported “modification”. Similarly, installing or uninstalling a feature through the Options Manager administration is a fully supported “configuration”. Anything to do with SPEL code, Java scripting (or any language scripting), or a customer-specific change to the underlying base code-line (done by CA Services or a Partner), is NOT supported by CA Support. The customer can perform these actions, but is responsible for the support, maintenance, and troubleshooting when an issue occurs. If such “customization” affect expected out-of-the-box behavior, CA Support will ask the customer to remove the customization and see if the behavior persists.

- **Modified Reports** -- When you modify the reports that access database tables from previous versions and that have been moved to renamed tables, the column names have been changed in Release 14.1.

- **Modified Forms** -- Upgrade retains the modification of the forms from the previous release of CA SDM. However, you cannot view the CA SDM Release 14.1 functionality on the modified forms after you upgrade.

- **Modified Admin Tree** -- When you modify the Admin tree in CA Service Desk Manager r11.0, these changes are not upgraded due to modifications in the architecture to support the role-based user interface. These Admin tree modifications include the addition of new nodes, renaming of existing nodes, modifying access types, or other data alterations. To use the modifications, perform the following actions:

  1. Before you upgrade, review your CA Service Desk Manager r11.0 Admin tree and note any modifications that you want to use after the upgrade.

  2. After the upgrade completes, identify which roles have Admin tree modifications.

  3. Apply the modifications to the appropriate CA SDM Release 14.1 role-based Admin trees.

  4. Review and test to verify that the desired functionality has been retained.

- **Modified Form Buttons** -- After the upgrade completes, buttons on modified forms in */site/mods /htmpl* that did not have quotes around the msgtxt(n) part of the code result in an error message, instead of the button name.
  For example, in the detail_cr.htmpl form, modify msgtxt(441) with quotes as follows to display the correct button name:

```
ImgBtnCreate("btnchg", "msgtext(441)", "detailSave('NEW_CHANGE')",
```

```
true, 0, msgtext(440)); // Save and Create Change Order
```

- **Retaining Modifications**-- When you need the CA SDM Release 14.1 functionality and would like to preserve your modifications from a previous release then redo the modification on a base CA SDM Release 14.1 form, which has the Release 14.1 functions. When any form is modified, the customer changes are overwritten and has to be recreated. There is a process in the upgrade that attempts to detect and identify the differences in the forms, and reports it to the customer for their investigation. However, it is highly recommended to document your customization BEFORE you perform any upgrade. In some cases, a new feature may be similar to the user customization, so the user changes must be removed. The custom JavaScript file must be customized again according to the base release 14.1 JavaScript file. For more information, see JavaScript Modification (see page 1805).

  Note: When you modify the *acctypedtl.rpt* and *acctypesum.rpt* reports, then the return data in CA SDM Release 14.1 is obsolete.

- **Notification Rules** -- When you remove the default activity notifications Contact, Object Contacts, and Contact Types from the previous installation of CA SDM and want to retain this functionality, then note the default contacts removed before migration. After you upgrade to the new version, remove the default Notification contacts again.

- **Role-based Functionality** -- Upgrading can cause issues with the role-based functionality. If you modified any of the following forms, they are considered as read-only by the Web Screen Painter in CA SDM Release 14.1 and they include an xxx_site.htmpl version where you can use custom code:

  - ahdtop.htmpl
  - menu_frames.htmpl
  - reports.htmpl
  - std_body.htmpl
  - std_footer.htmpl
  - std_head.htmpl
  - styles.htmpl
  - msg_cat.js
  - menu_frames_role.htmpl

- **Modified HTMPL Files** -- Consider the following information:

  - All modified HTMPL files retain their default menu bar settings after you upgrade. A pop-up window inherits its menu bar from the main page tab, as a result of the role-based user interface. Modified HTMPL files are not available on the modified forms from the previous release after the upgrade.

- CA SDM Release 14.1 does not use some modified HTMPL files from previous releases. The migration script executes the perl script $NX_ROOT/bin/*migrate_to_r12_9_web_check.pl* that appends the files with the *incompatible_for_r2_9* extension. After migration completes, open $NX_ROOT/site/web_check_files.txt with a text editor to see the list of incompatible forms for Release 14.1.

- If you modifiedthe list_dblocks.htmpl file in a previous release of CA SDM, this form does not work in CA SDM Release 14.1. If you modifiedthe Admin Tree to display the list_dblocks.htmpl in other parts of the tree, the modification does not work after you migrate. Modify the form manually to use the new URL and form. To complete this modification, click Security and Role Management, Menu Tree Resources and open Current Locks. Update the resources with the following CA SDM Release 14.1 string:

```
OP=SEARCH+FACTORY=record_lock+QBE.NN.lock_time=NULL
```

- **Foreign Keys** -- When the upgrade process detects referential integrity issues while attempting to reset foreign keys then the errors appear in the migration.log file. The associated foreign key sets to a predefined valid reference.

- **Servers and Web Director Configuration** -- When your previous installation was configured to use additional servers or web directors, then you must first create the configuration for the specific servers and run the CA SDM server configuration utility (pdm_configure). **CA Support Automation Divisions** -- When you migrate the divisions to tenants, then convert this data before enabling and configuring Support Automation in CA SDM Release 12.9.

- **Rename Modified HTMPL Forms** – If you modified HTMPL forms in a previous release of CA SDM, you run a script to rename them before you upgrade. You run this script on all CA SDM servers. The migrate_to_r12_9_web_check.pl script renames all modified web forms, style sheets, Java scripts, images, and macros in the site/mods directory. Renaming these files helps you identify your modified forms.
  Follow these steps:

  1. From a command prompt, executepdm_perl $NX_ROOT/bin/migrate_to_r12_9_web_check.pl.
     The script appends the modified forms with an *incompatible_for_r12_9* extension.

  2. Open $NX_ROOT/bin/migrate_to_r12_9_web_check.pl with a text editor.
     A list of incompatible forms for Release 14.1 appears.

  Note: The script does not restore files from backup folders to the legacy or site/mods directories as in previous releases of CA SDM.

Step 2: Use the CA SDM Migration Console

The migration console guides you through the migration and upgrade processes for CA SDM. The console automatically detects an existing installation, such as CA SDM r11.2. The console performs the following tasks:

1. Verifies that your product is CA SDM r11.2, r12.0, r12.1, r12.5, r12.6, r12.7 or r12.9.

2. Converts passwords to a FIPS 140-2 compliant format.

3. Applies MDB updates.

> **Important!** The remote MDB version must be at least CA MDB r1.5, or the migration fails.

4. Migrates LREL data.
5. Converts modified files to UTF-8.
6. Converts access type records to the CA SDM Release 14.1 role and access type records.
7. Migrates and upgrades user scoreboard queries for role-based operations.
8. Migrates and upgrades existing notifications to use notification rules and notification message templates.

> **Note:** After you select Perform Upgrade and click Install, you cannot roll back the migration and upgrade. If you close the Migration Console before the process finishes, it continues to run in the background.

Follow these steps:

1. Consider the following points before you start using the migration console:
   - If your configured web forms are not compatible with CA SDM Release 14.1, the migration console displays a message indicating that these forms moved to the site/mods/wwww /htmpl directory. For more information about these forms, view the Web_Forms_Changed.txt file in the site/mods/ directory.
   - The CA SDM Migration Console does not convert divisions to tenants. If you want to configure Support Automation in a multi-tenancy environment, you *must* separately migrate (see page) CA Support Automation r6.0 SR1 eFix5 divisions to CA SDM Release 14.1 tenants before enabling Support Automation in CA SDM.
   - Uninstall Visualizer before you start using the migration console.
   - Reviewed the following migration scenarios:
     - Upgrade CA SDM Using the SWING Box Method (see page 413)
     - Upgrade CA SDM on Similar Hardware Setup (see page 417)
     - Migrate Data to CA Service Desk Manager 14.1 (see page 418)
2. Start the upgrade from the installation media or start it manually using the following command:
   - **Windows:** $NX_ROOT\bin\migrate_to_r14_1.vbs

- **Linux/UNIX:** $NX_ROOT\bin\migrate_to_r14_1.sh

> **Note:** If migration fails with a "Schema Validation" error, use the previously mentioned command to run the upgrade again.

The installer detects your version of CMDB, such as CMDB 11.2. You can upgrade CMDB from a previous release of CA SDM, such as 11.2, 12.0, and 12.1. If you cancel migration, you *must* execute the script to relaunch the migration console. The script is located in the */bin* directory of the product, such as *C:/CMDB/bin*. For example, if you cancel migration on Linux or Unix, execute the *migration_to_r14.1.sh* script.

> **Note:** If you are upgrading from a standalone CMDB release, you can continue to use standalone CMDB functionality in the updated CA SDM release. If you are upgrading from an environment with CMDB and CA SDM, or if you are upgrading from a CA SDM environment without CMDB, the full CA SDM Release installs during the upgrade. If you are upgrading from a combined CA SDM and CMDB installation, the installer displays the detected environment as a CMDB release, not CA SDM.

3. Click Next.
   The installation warns you not to use CA SDM and Knowledge Management until migration completes.

4. Click Next.
   If the installation detects Visualizer, you are prompted to uninstall it manually.

> **Important!** After you uninstall Visualizer, you *must* reboot and relaunch the CA SDM installer.

5. Accept the terms of the License Agreement and click Install.
   The installation backs up your data and shuts down services.

> **Note:** The CMDB upgrade does *not* back up your database.

After the installation completes, the migration console appears with a warning to review your migration documentation.

6. Click Migrate.
   The migration console loads system data, updates your MDB, and recycles services.

Note: If you encounter problems during the migration and upgrade, the migration log provides a record of the entire process. You can access this log at $NX_ROOT/log /pdm_migrationr14_1.log.

7. The console verifies tables, processes data, backs up, and upgrades CA SDM.
   The CA SDM configuration appears.

8. (Optional) Configure CMDB Only.
   If you are upgrading from a standalone CMDB environment, a *Configure CMDB Only* check box displays on the General Settings form.

   Important! During configuration, when you migrate from CA CMDB stand alone version to CA SDM, a Configure CMDB Only check box displays. When you clear the Configure CMDB Only check box and you click Next, you cannot configure CA CMDB again. Even if you click Back, the Configure CMDB Only check box is no longer available. A message warns you of this behavior in the configuration dialog. If you cancel the configuration before it completes and rerun it, the Configure CMDB Only check box is available.
   The Configure CMDB Only check box controls the value of the CA SDM environment variable NX_CMDB. The environment variable controls whether the Support Automation feature is configured. If the check box is cleared, Support Automation is configureable, otherwise it is not. The environment variable affects the behavior of some Web forms.

   If you are upgrading from a standalone CMDB environment, and want to use standalone CMDB functionality in updated CA SDM Release, you cannot configure Support Automation.

9. Complete the configuration, as appropriate to your environment.

10. (Optional) Reviewed the Migrate from a Nonsupported Windows Environment (see page 412) and Migrate from a Nonsupported Non Windows Environment (see page 413) examples.

Example Migrate from a Nonsupported Windows Environment

In this example, you have CA SDM r11.2 installed on Windows 2003 (32-bit) with SQL Server 2005. You want to migrate your data and upgrade to CA SDM Release 14.1 on a Windows 2008 64-bit system with SQL Server 2008 successfully.

Follow these steps:

1. Migrate to CA SDM Release 14.1 on the same computer.

2. Upgrade SQL Server 2005 to 2008.

3. Back up the MDB database.

4. Install CA SDM Release 14.1 on Windows 2008 (64-bit).

5. Load the MDB backup that you completed in Step 3.
6. Move the $NX_ROOT\site\mod folder from the older computer to the new computer.
7. Update the NX.env file with the modified variables.
8. Copy the Attachment folder from the older computer to the new computer.
9. Run configuration again on the new computer.
10. Update the computer details in the required places in Options Manager.

Example Migrate from a Nonsupported Non Windows Environment

In this example, you have CA SDM r11.2 installed on Redhat Enterprise Linux 4 with Oracle 10g. You want to migrate your data and upgrade to CA SDM Release 14.1 on a Redhat Enterprise Linux 6 system with Oracle 11g R2 successfully.

Follow these steps:

1. Migrate to CA SDM r12.5 on the same computer.
2. Back up the MDB database.
3. Install CA SDM r12.5 on Redhat Enterprise Linux 6 with Oracle 11g R2.
4. Load the MDB backup that you completed in Step 2.
5. Move the $NX_ROOT\site\mod folder from the older computer to the new computer.
6. Update the NX.env file with the modified variables.
7. Copy the Attachment folder from the older computer to the new computer.
8. Run configuration again on the new computer.
9. Update the computer details in the required places in Options Manager.
10. Migrate from CA SDM r12.5 to Release 14.1.

Upgrade CA SDM Using the SWING Box Method

The SWING Box method is performed by using a separate server, typically, referred to as a SWING system.

In this method, the following are the main steps:

- Replicate your current production system on the SWING system.
- Migrate to CA Service Desk Manager (SDM) 14.1.
- Move the migrated CA SDM 14.1 data and customizations to a clean (never migrated) server.

- Install on new hardware.

This method has the following advantages:

- The current production system retains its integrity even during a DR issue or failed migration.
- At the end of the process, you install CA SDM 14.1 on a never migrated, system, with an updated version of the operating system and database.
- If you are using a VMware environment as the SWING system, you can use the snapshot functionality to test the migration process multiple times, gather data on timings and steps, ensure an easy migration.

Ensure that you consider the following prerequisites before performing this method:

- After initiating migration testing, *do not* perform any changes to the form, or schema (tables and columns) customizations on any system. For example, *do not* make any modification on 12.7/12.x production or 14.1 development, test, SWING, and so on. If you plan to add or modify additional tables or columns, it should be done either on 12.7/12.x and should put into production before testing migration. You can also modify during another outage that is planned after your production migration is complete and you are running CA SDM 14.1 on the new production system.
- You have completed the following tasks:
  - A test migration of the replicated production system
  - Customized again the custom forms from 12.7/12.x that are incompatible with CA SDM 14.1.
  - Ensured that the you have the latest customized and complete *site**mods* directory from a 14.1 environment where all testing was completed.
- Replicate the most recent migrated CA SDM 14.1 test environment installation to the latest production hardware, including your customized forms built for CA SDM 14.1.

Follow these steps:

- Step 1: Gather Files or Data from Current Production System (see page 414)
- Step 2: Prepare the SWING Environment and Replicate Production to SWING (see page 415)
- Step 3: Upgrade and Migrate to CA SDM 14.1 on the SWING System (see page 416)
- Step 4: Move Migrated SWING Box Install to New Production Hardware (see page 417)

Step 1: Gather Files or Data from Current Production System

Follow these steps:

1. Create an SQL backup of the MDB as a .bak file (usually a normal SQL backup).
2. Copy the *C:**Program Files**CA**Service Desk**site**mods* directory and create a zip file, if possible.
3. Copy the *C:**Program Files**CA**Service Desk**site**attachments* (or the directory where your repositories are configured to store your attachments in) and create a zip file, if required.

4. Copy the files in steps 1 - 3 to a stand-by directory on that system. Do not paste them yet on the SWING environment.

Step 2: Prepare the SWING Environment and Replicate Production to SWING

Note: If your SWING environment has both Database and Application running on the same system, then you might start at step 3. In this section, the database server is referred to as SWING-DB and the application server as SWING-APP.

Follow these steps:

1. On SWING DB (assuming SQL is already installed), run the MDB installer wizard from the CA SDM 12.7/12.x install media.

2. On SWING-APP, install the SQL client and native client (workstation tools also).

3. Install CA SDM 12.7/12.x on SWING-APP and run configuration so that you have a vanilla 12.7 /12.x Service Desk Manager installation running.

4. As the database administrator, execute the SQL Restore and restore the MDB from your current production that you backed up, to the SWING-DB server. Set option to *OVERWRITE entire database* when restoring.

5. Execute the stored procedure in SQL to fix the orphaned users which are created when restoring a database from one SQL instance to another. Example: sp_change_users_login 'AUTO_FIX','ServiceDesk'.

6. Copy the *site**mods* directory that you backed up from current production and put in place on SWING-APP system.

7. Copy the *site**attachments* directory (or whichever attachments directory) you backed up from current production and place it on SWING-APP system.

8. Execute *pdm_configure*:

    a. Skip selecting **TO LOAD DEFAULT DATA**.

    b. In the configuration wizard, click **next** at the database section. A message displays, stating that database was previously configured.
    This message indicates that you restored the MDB from a different environment.

    c. Click **Yes**.

9. After the configuration is complete, perform the following tasks:

    a. Start CA SDM services (if not started).

    b. Test the system functionality to ensure 12.7/12.x is running with your data, and customizations, as a full replica of your production environment.

Step 3: Upgrade and Migrate to CA SDM 14.1 on the SWING System

Test the migration and become familiar with the process and issues you might run into while migrating your production system. If your SWING system is on a VMware environment, then take a snapshot. You can roll back to that snapshot, then take your production system down, do another SQL backup on production, restore it to the SWING environment and then complete the steps mentioned in this section. In case migration fails, you can bring your 12.7/12.x production system back up and start the services. You can then retest migration on the SWING environment again, and schedule it for another time.

Follow these steps:

1. Mount CA SDM 14.1 install media from a local folder, or run the setup.exe from the local folder where the install media is being stored.

   Important! If you are extracting an ISO of the install media, it should be stored in a path and folder that has no spaces in the name, for example, SD127Setup. Also, run locally from the same drive volume where you plan to install CA SDM 14.1. Do not run the installer from a network drive or mounted share as this has been known to cause install and even post install problems to occur.

2. Launch the CA Service Management 14.1 installer.

3. Select a language and click **Next**.
   For example, select English and then click **Next**.

4. Select CA Service Management.

5. Follow the prompts to perform this upgrade.

6. Copy the CA Service Management 14.1 *site**mods* folder from previous test or development environment to this SWING system and run a *pdm_configure* to ensure that all customizations are properly implemented.

7. Test the migrated, and customized 14.1 SWING system for integrity and functionality.

   Note: If this is your test run on the SWING environment, the re-build your form customizations using the 14.1 forms that are delivered with the product as your previously customized 12.7/12.x versions are incompatible in 14.1. Once you have completed the rebuilding of your customizations, take a backup of your *site**mods* directory on the SWING box and store it somewhere outside of this environment for use later (as described in step 6).

8. If all tests are successfully completed, you might now start the process of moving your migrated data, and customizations to the new production hardware.

Step 4: Move Migrated SWING Box Install to New Production Hardware

Follow these steps:

1. Create an SQL backup on the SWING system, and let your database administrator perform an SQL Restore onto the SQL instance that your new production system is using.
   For more information, see Step 2 procedure and execute the steps 4-7.

2. If you are using the Advance Availability configuration, complete the following steps or skip to step 4:

   a. Ensure that you have installed the following components:

      - (Oracle) client is installed and net service name is configured to connect with the new database server.

      - (MS SQL) MS SQL client is installed.

   b. From the DBCleanupUtility folder of the installer DVD, run the following script:

   - (Windows) ResetSDMuspServers.bat

   - (UNIX) ResetSDMuspServers.sh

   a. Follow the steps that are provided in the script (it might need database credentials). This utility deactivates all the servers present in usp_servers table.

3. If you are using the conventional configuration, add NX_SWING_BOX_MIGRATE=Yes variable to NX.env file and run pdm_configure:

   a. Skip selecting **TO LOAD DEFAULT DATA**.

   b. In the configuration wizard, click **next** at the database section. A message displays, stating that database was previously configured.
      This message indicates that you restored the MDB from a different environment.

   c. Click **Yes**.

4. After the configuration is complete, perform the following tasks:

   a. Start CA SDM services (if not started).

   b. Test the system functionality to ensure 12.7/12.x is running with your data, and customizations, as a full replica of your production environment.

Upgrade CA SDM on Similar Hardware Setup

Follow these steps to upgrade CA SDM advanced availability configuration with the similar hardware setup:

1. Shutdown all the services on the application and standby servers.

2. Upgrade CA SDM on the background server. Ensure that the background server is up and running.

3. Upgrade CA SDM on the standby and application servers.

Migrate Data to CA Service Desk Manager 14.1

This topic contains the following information:

How to Migrate Data to CA SDM Release 14.1 on a 64-Bit Linux/UNIX

Follow these steps:

1. Install the Oracle 32-Bit client.

2. Establish the connection with Oracle_Server_SID.

3. Create a Local Net Service Name and test the connection.

4. Export TWO_TASK variable.

5. Edit the ORACLE_HOME and PATH variables to have oracle_client home and remove server home, as shown in the following example:

   ```
   ORACLE_HOME= /opt/app/product/11.2.0/client_1
   PATH= /opt/app/product/11.2.0/client_1/bin
   ```

   Note: Update the ORACLE_HOME variable in the NX.env as shown in the previous example.

6. Set LD_LIBRARY_PATH and LIBPATH to the client-lib which are 32 -bit binaries, as shown in the following example:

   ```
   LD_LIBRARY_PATH=/opt/app/product/11.2.0/client_1/lib
   ```

7. Execute pdm_configure with ORACLE_HOME set to client_home, as shown in the following example:
   C:\app\Administrator\product\11.2.0\client_1\

8. Install CA SDM Release 14.1.

How to Migrate Data to CA SDM Release 14.1 on a 64-Bit Windows

Follow these steps:

1. Install the Oracle 32-bit client.

2. Establish the connection with Oracle_Server_SID.
3. Create a Local Net Service Name and test the connection.
4. Edit the PATH variable to have oracle_client home and remove server home from PATH, as shown in the following example:
   C:\app\Administrator\product\11.2.0\client_1\bin
5. Execute pdm_configure with ORACLE_HOME set to client_home, as shown in the following example:
   C:\app\Administrator\product\11.2.0\client_1\
6. Install CA SDM Release 14.1.

Step 3: Perform Post Upgrade Configuration

Configure the product after the upgrade. Use the configuration wizard to verify your existing modifications.

Note: If the Configuration dialog closes without completing post-upgrade configuration, run *pdm_configure -s* from the command line.

Consider the following post-upgrade configuration:

- User Interface Migration (see page 419)
- KPI Data (see page 420)
- Configure Support Automation Role Access (see page 420)
- Configure the Servers After Upgrade (see page 420)
- Configure Ticket Management After Upgrade (see page 423)
- Modify HTMPL Forms (see page 426)
- Set Ticket Values for Self-Service Users (see page 427)
- Upgrade Knowledge Management from Older Releases (see page 429)
- LREL Post-Migration (see page 434)
- Modify Functional Access Areas (see page 437)
- Email Upgrading (see page 440)

User Interface Migration

- Migration backs up forms automatically. If you used modified HTMPL forms in CA SDM r11.2, r12.0, r12.1, or r12.5, you *must* modify them again after upgrading.
- After you upgrade, modify all the changed HTMPL forms that contained notebook controls to include the new web macros and provide the appropriate tab group names. You modify <PDM_NOTEBOOK> statements to <PDM_MACRO name=startNotebook> and <PDM_TAB> statements to <PDM_MACRO name=TAB> in WSP.

KPI Data

After you upgrade, all versions (active and inactive) of webLicenseCt KPIs are no longer available and all the related KPI data becomes invalid. These data still remain in the usp_kpi_data table, but this data is not fetched while reporting. Customers can choose to execute the OOTB KPI Rule, KPI Data (System) (inactive by default), to remove this data.

Important! We recommend you to check the data available in the usp_kpi_data table, as executing this KPI rule will also archive and/or purge other system KPI collected data.

Note: A new KPI, webConcurrentTotalLicenseCt is used in current release of CA SDM to calculate the number of unique users logged in to CA SDM during that interval. For more information, see User Authentication (see page 1007).

Configure Support Automation Role Access

If you configure Support Automation before migration, the role access configures properly. If you configure Support Automation after migration, set the Support Automation access field for each role to the appropriate value. If the role access is not properly set up, you cannot access the Support Automation Analyst Interface or the End User interface.

The following process outlines how you configure the Support Automation role access after migration:

1. Install the *supportautomation_url* option.
2. Set the Support Automation access field for each role you want to access Support Automation.

Configure the Servers After Upgrade

This article contains the following topics:

Inactive Servers Other Than Primary or Secondary

After you upgrade, all the servers that are not entered as primary server in the usp_servers table are converted to secondary server. Before upgrading, if you have added any server in the usp_servers table, which are not secondary or primary server, inactive them after you upgrade. You can inactive servers from the primary server Web UI.The local host name is stored in the usp_servers table in local_host column.

Clear the Webengine and Browser Cache

After you upgrade CA SDM, run the pdm_webcache utility to clear the cache for the webengine and browser.

```
pdm_webcache -b -H
```

- **-b**
  Warns the user to clear their browser cache.

- **-H**
  Clears the webengine cache.

Configure the Web Director and Servers

After you upgrade, we recommend that you configure the servers and Web Director.

To configure the Web Director and servers

If the previous version was configured to use additional servers, or web directors, you can configure the servers and web director and apply the configuration after upgrade.

For more information, see Managing Servers.

Adjust Data Partition Settings

You can adjust partition constraints after you configure the roles in your system. You adjust the partition constraints to verify that the appropriate permissions function properly after you upgrade to the current release of the product.

To adjust data partition constraints

1. On the Administration tab, browse to Security and Role Management, Data Partitions, Data Partition Constraints.

2. Verify the Majic code constraint settings for the following tables:

   - **SKELETONS**
     Specifies the table used for Knowledge Documents.

   - **O_INDEXES**
     Specifies the table used for Knowledge Categories.

   The table constraint settings are verified.

3. Click Show Filter and enter the Data Partitions you previously used.

Note: You can also use the Table Name field in the Search area to limit your list. For example, enter *SKELETONS* or *O_INDEXES* in the Table Name field and click Search.

Default Constraint Settings

The typical default settings for Constraints are listed as follows:

- **Constraint Settings for the Customer (like) and Employee (like) Data Partitions**

Constraint Settings for Customer (like) and Employee (like) Data Partitions should be the following:

SKELETONS Table

View constraint as:

'SKELETONS READ_PGROUP in @root.pgroups or READ_PGROUP.[pgroup] contained_roles.role in @root.role) and ACTIVE_STATE = 0'Pre-update and Delete constraint:

'id = 0' (id=0 indicates no access)

- **O_INDEXES Table**
  View constraint as:
  READ_PGROUP in @root.pgroups or READ_PGROUP.[pgroup] contained_roles.role in @root.role
  Pre-update and delete constraint:WRITE_PGROUP in @root.pgroups OR WRITE_PGROUP.
  [pgroup] contained_roles.role IN @root.role

Constraint Settings for CA SDM Analyst (like), Knowledge Managers (like) and Knowledge Engineers (like)

Constraint Settings for CA SDM Analyst (like), Knowledge Managers (like) and Knowledge Engineers (like) should be the following:

SKELETONS Table

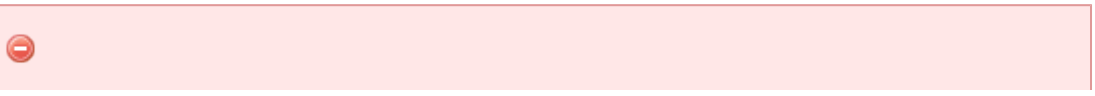
View constraint as:(ACTIVE_STATE >=0)and (READ_PGROUP in @root.pgroups or READ_PGROUP.
[pgroup] contained_roles.role in @root.role) OR (ACTIVE_STATE > 0 AND ASSIGNEE_ID = @root.id)
OR (ACTIVE_STATE = 0 AND OWNER_ID = @root.id)) Active

Pre-update and delete constraint:(ACTIVE_STATE >= 0) AND (WRITE_PGROUP in @root.pgroups OR
WRITE_PGROUP.[pgroup] contained_roles.role IN @root.role) OR (ACTIVE_STATE > 0 AND
ASSIGNEE_ID = @root.id) OR (ACTIVE_STATE = 0 AND OWNER_ID= @root.id)) Active

- **O_INDEXES Table**
  View constraint as:READ_PGROUP in @root.pgroups or READ_PGROUP.[pgroup] contained_roles.
  role in @root.role
  Pre-update and delete constraint:WRITE_PGROUP in @root.pgroups OR WRITE_PGROUP.
  [pgroup] contained_roles.role IN @root.role

Start the IIS Web Interface (CAisd)

After you upgrade a CA SDM r11.2 Windows installation that had an IIS integration, the CA SDM IIS web interface (CAisd) stops. If you want to continue using the IIS integration, manually start CAisd after you upgrade.



Important! If you want to use IIS 7.0, you *must* install the CGI and Metabase Compatability components.

Configure Ticket Management After Upgrade

This article contains the following topics:

How to Add the Incident Priority Field to Incidents

The *incident priority* is the sum of the Urgency and Impact values. The incident priority is only for the incident ticket type. The Incident Priority value appears on the incidents after you install the use_incident_priority option and add it to the incident Detail page form with Web Screen Painter.

To add the Incident Priority field to incident, do the following:

1. Install the use_incident_priority option from the Options Manager, Request Mgr.
2. Use Web Screen Painter to add the Incident Priority field to the Incident Detail pages. The Incident Priority value appears on saved Incident Detail page when the use_incident_priority option is installed. When the use_incident_priority option is not installed, the Incident Priority value is zero.

Note: The use_incident_priority option only manages the Incident Priority value. This option is not related to priority calculation.

Add the Urgency Field to Employee Tickets

By default the Urgency field does not appear on Employee incidents or requests. However, you can add the Urgency field by using the urgency_on_employee option.

Note: When you uninstall the urgency_on_employee option and disable priority calculation, the Priority field appears on the Request and Incident Detail pages for self-service Users.

To add the Urgency field to Employee tickets, install the urgency_on_employee option from the Options Manager, Request Mgr. The Urgency field appears on Employee incidents or requests. Self-service users can override the value on the incident.

Activate Status Transitions

After the upgrade, all predefined status transitions are inactive, so status transitions are not in effect. You can activate and modify these status transitions to accommodate the ticket status transition flow you want.

Note: All modified status code descriptions that appear on ticket forms are retained during the upgrade process.

To activate a status transition

1. On the Administration tab, expand the Service Desk node, and select one of the following ticket types:
   - Change Orders
     - Change Order Transitions
   - Issues
     - Issue Transitions
   - Requests/Incidents/Problems:
     - Incident Transitions
     - Problem Transitions
     - Request Transitions

   The Transitions List appears.
2. Select Show Filter on the Transitions List page.
   The top portion of the page reveals additional search fields.
3. Select Inactive in the Record Status field and click Search.
   The Transitions List at the bottom of the page displays all inactive transitions.
4. Open the transition for editing.
5. Select Active in the Record Status drop-down list.
6. Click Save, Close Window.
7. Click Search.
   The Transition List displays the active transition.

Enable Priority Calculation

Priority calculation is a set of values that automatically set Priority, Urgency, and Impact values on problems and incidents. For new CA SDM installations, the default priority calculation is enabled for problem and incident ticket types by default. However, if you are upgrading from a previous release, the default priority calculation is inactive.

If you create and activate a different priority calculation, the ticket values reflect the settings in the active priority calculation that is associated with an incident or a problem. When no priority calculation is active, users can manually set the Priority and other values on tickets.

Note: The modified forms on the Employee and Customer interface operate in the same manner as the previous versions. The Self-Service users can directly change the Priority regardless of the settings in Priority calculation.

To enable priority calculation after the migration, do the following:

1. On the Administration tab, navigate to Service Desk, Request/Incidents/Problems, Priority Calculation.

2. Right-click the default priority calculation or another priority calculation and select Edit from the short-cut menu.
   The Update Priority Calculation page appears.

3. Set the Status to Active.

4. Select one or more of the following ticket types:

   - **Incidents**
     Enables this priority calculation to manage incident tickets. Only one active priority calculation can manage incidents.

   - **Problems**
     Enables this priority calculation to manage problem tickets. Only one active priority calculation can manage problems.

5. Click Save.
   The values on the default priority calculation apply to new tickets unless you activated another priority calculation. On new tickets that use a priority calculation, the Priority field is read-only.

Activate Transition Types

By default, all predefined transition types delivered with the product are inactive, so status transition buttons are not in effect. You can activate and modify these transition types to accommodate the status transition flow you want.

To activate a transition type

1. Select Show Filter on the Transition Type List page.
   The top portion of the page reveals additional search fields.

2. Select Inactive in the Record Status field and click Search.
   The Transition Type List displays all inactive transition types.

3. Right-click the title of the transition type and select Edit from the menu.

4. Select Active in the Record Status drop-down list.

5. Click Save, Close Window.

6. Click Search.
   The Transition Type List displays the active transition type.

Modify HTMPL Forms

This article contains the following topics:

After you upgrade CA SDM, you modify all the HTMPL forms that contained notebook controls to include web macros and provide the appropriate tab group names.

For each modified form, use WSP to modify <PDM_NOTEBOOK> statements to <PDM_MACRO name=startNotebook> and <PDM_TAB> statements to <PDM_MACRO name=TAB>.

SITEMODS.JS File

Lines of code added to the sitemods.js file of the previous version, called from an HTMPL page, must be merged into the current sitemods.js file before the code works.

Modify Help Sets after Migrating Roles

After you upgrade, CA SDM provides all migrated roles with the complete *Online Help*. You can modify help sets for any role, as appropriate to the needs of your online help system.

To modify help sets for a role

1. On the Administration tab, browse to Security and Role Management, Role List.

2. Open the Role for modification, such as *customer*.

3. Click Edit.

4. Select the Web Interface Tab.
   Click Help View.
   The list of available Help Sets appears for the selected role.

5. Select a Help Set, such as customer.

6. Save the Role.
   The help View for the role changes to the selected online help set.

You can also view the topics available under an online help set by selecting the help set detail and clicking the View Help button.

DocType Validation

Previous releases of CA SDM used the following DocType for HTML generated from HTMPL forms in the HtmplDoctype property of web.cfg:

```
HtmplDoctype <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
```

The HtmplDoctype property of web.cfg appears as follows:

```
HtmplDoctype <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN" "http://www.
w3.org/TR/html4/frameset.dtd">
```

This line begins on the first list of a page, typically. After you upgrade, verify that the HtmplDoctype property value changed in your modified forms. You can open an HTML file from the $NX_ROOT /bopcfg/www/wwwroot/html directory with text editor and can verify the DocType value.

Set Ticket Values for Self-Service Users

This article contains the following topics:

You can control the Urgency and Priority values that appear to Self-Service users. The properties you set properties in the *web.cfg* file manage choices that appear to users while they create or edit tickets.

To set ticket values for Self-Service users, consider the following:

1. For each override value in the *web.cfg* parameter, specify one or more values.
2. For Urgency values (see page 428), specify one or more numbers from 0 through 4.
3. For Priority values (see page 429), specify one or more numbers from 1 through 5 or the word None.
4. Separate each value with a space.
5. Specify the first value that appears in the list as the default value that appears on tickets. If necessary, you can repeat the default value in the list to improve legibility.

Set the Urgency Range for Self-Service Users

For self-service incidents and requests, you can set default Urgency values in the *web.cfg* file. When you set a range of Urgency values, self-service users such as employees, VIP employees, or guests can set Urgency values on tickets. The choices that appear to self-service users are based on the range of values that you set in the *web.cfg*.

To set the default Urgency range for self-service users

1. Open the w*eb.cfg* file from the appropriate directory:
   - (Windows) %NX_ROOT%\bopcfg\www\

- (UNIX) $NX_ROOT/bopcfg/www/

2. For each parameter, specify one or more urgency property values (see page 428). Separate each value with a space:

   - **ESCEmpUrg**
     Specifies how VIP employees can override Urgency on tickets.

   - **EmpUrg**
     Specifies how employees can override Urgency on tickets.

   - **AnonymousUrg**
     Specifies valid priorities for tickets created by guest users.

3. Save the *web.cfg*.
   On new tickets, employees, VIP employees, or guests can set Urgency values based on the range of values in the *web.cfg*.

Example: Show Guests Only Two Urgency Values on a Request

1. Open the *web.cfg.*

2. Set the *AnonymousUrg* parameter as 0 4. For example, AnonymousUrg 0 4.

3. Save the *web.cfg*.
   The Urgency values that appear to the self-service user are 1-When Possible and 5-Immediate. The default Urgency is 1-When Possible.

Urgency Property Values

The *web.cfg* contains settings to control how self-service users override Urgency on tickets. The following Urgency property values are available:

- **0** -- Lets the user set the Urgency to 1-When Possible
- **1** -- Lets the user set the Urgency to 2-Soon
- **2** -- Lets the user set the Urgency to 3-Quickly
- **3** -- Lets the user set the Urgency to 4-Very Quickly
- **4** -- Lets the user set the Urgency to 5-Immediate

Set the Priority Range for Self-Service Users

You can set a range of valid priorities to allow self-service users to override Priority values on tickets. When you set the priority range, customers, employees, or guests can set Priority values based on the range of values in the *web.cfg*.

To set the priority range for self-service users

1. On the w*eb.cfg* file from the appropriate directory:

- (Windows) %NX_ROOT%\bopcfg\wwww\
- (UNIX) $NX_ROOT/bopcfg/wwww/

2. For each of the parameters, specify one or more Priority property values (see page 429).
   - **CstPrio**
     Specifies how customers can override Priority on tickets.
   - **EmpPrio**
     Specifies how employees can override Priority on tickets.
   - **AnonymousPrio**
     Specifies how employees can override Priority on tickets.
3. Save the *web.cfg*.
   On new tickets, customers, employees, or guests can set Priority values based on the range of values in the *web.cfg*.

Example: Show Guests Only Two Priority Values

1. Open the *web.cfg*.
2. Set the *AnonymousPrio* parameter to None 4. For example: AnonymousPrio None 4.
3. Save the *web.cfg*.
   When a guest works with tickets, the values for Urgency are None or 4. The default value is None.

Priority Property Values

The *web.cfg* contains settings to control how self-service users override ticket Priority. The following Priority property values are available:

- **None** -- Lets the user set the Priority to None
- **1** -- Lets the user set the Priority to 1 (highest priority)
- **2** -- Lets the user set the Priority to 2
- **3** -- Lets the user set the Priority to 3
- **4** -- Lets the user set the Priority to 4
- **5** -- Lets the user set the Priority to 5 (lowest priority)

Upgrade Knowledge Management from Older Releases

This article contains the following topics:

Upgrade Knowledge Management From CA SDM r12.x

Upgrading from CA SDM r12 or r12.1 automatically upgrades your Knowledge Management environment. When the upgrade finishes, complete the following steps:

1. Map links created in a resolution of a document to the database to locate broken links.

   Note: You use the default *Flag broken links* policy to locate broken links.

2. On the Administration tab, browse to Knowledge, Automated Policies, Policies, Scheduling. The Scheduling page appears.

3. Select the Run Calculation check box in the Last Updated field.

4. Enter a date in the Schedule text box or click the Calendar icon to select a date.

5. Select the time interval to perform the calculation and run the policies.

6. Click Save.
   The policies are processed at the specified date and time.

7. On the **Administration** tab, browse to **Knowledge**, **Systems**, **General Settings**.
   The General Settings page opens.

8. Complete the following information:

   Path for EBR Index Files

   Defines the location for storing EBR index files. CA SDM creates EBR index files when you save and publish any knowledge document. Depending on your configuration type, consider the following points while defining the EBR index file path:

   - Conventional: If you are upgrading from the CA SDM Release 12.9 from r11.2 or r12.X, you may choose not to use UNC shared path. If you have not created a UNC path, CA SDM uses the default path to store EBR index files. If you are using a UNC shared drive, manually copy the ebr/ebr_ADM folders from the default location ($NX_ROOT/site/) to the UNC shared path.

   - Advanced availability: If you are upgrading to the advanced availability configuration from CA SDM r11.2 or r12.X, you must create the UNC shared path and use it to store EBR index files. The UNC credentials are not required for the default path. After you create the UNC path, manually copy the ebr/ebr_ADM folders from the default location ($NX_ROOT/site/) to the UNC shared path.

     Important!EBR Index Files path & **KEIT Files path** must refer to the same UNC credentials and the path must reside on a same server to support this.

   Default: $NX_ROOT/site/ebr

- **Path For Knowledge Import/Export Files**

Defines the location for storing KEIT import/export packages during an import/export operation. Depending on your configuration type, consider the following points while defining KEIT file path:

- Conventional: If you are upgrading to CA SDM Release 12.9 from r11.2 or r12.X, you may chose not to use UNC shared path. If you have not created a UNC path, CA SDM uses the default path to store the KEIT files. If you are using a UNC shared drive, manually copy the Import/Export package folders from the default location ($NX_ROOT/site/keit) to the UNC shared path.

- Advanced availability: If you are upgrading to the advanced availability configuration from CA SDM r11.2 or r12.X, you must create the UNC shared path and use it to store the KEIT files. The UNC credentials are not required for the default path. After you create the UNC path, manually copy the Import/Export package folders from the default location ($NX_ROOT/site/keit) to the UNC shared path.

  Important!EBR Index Files path & **KEIT Files path** must refer to the same UNC credentials and the path must reside on a same server to support this.

Default: $NX_ROOT/site/keit

- **UNC Credentials**

You can use this option to create UNC credentials to access the network shared drive to access EBR indexing files and import/export packages. Use the **UNC Credentials** link to create the UNC credentials.

Note: UNC paths and UNC credentials are required in case of the advanced availability configuration. Restart the CA SDM service when you change any of the UNC details (UNC paths or UNC credentials).

9. (For Keyword Search implementations) Enter the following command at the command prompt:

```
pdm_k_reindex factory:all
```

Important! The *all* variable is case sensitive. If you use factory:ALL, errors appear in the log files.

The Knowledge Management environment is upgraded.

Note: After the upgrade, printing Knowledge Documents can result in a large space inserted after the Resolution section of the document. This space is inserted due to an issue with upgrading document templates from a previous release. For more information about resolving this printing issue, see the CA Service Desk Manager Known Knowledge Management Issues (see page 152).

Important! After you upgrade, Knowledge Management notification data from previous releases of CA SDM uses the Release 14.1 notification engine. For example, there are default activity notifications and notification rules for object types, such as the Knowledge Report Card.

Upgrade Knowledge Management From r11.2

Upgrading CA SDM r11.2 automatically upgrades your Knowledge Management environment. When the upgrade finishes, complete the following steps:

1. Map links created in a resolution of a document to the database to locate broken links.

   Note: You use the default *Flag broken links* policy to locate broken links.

2. Select **Knowledge**, **Automated Policies**, **Scheduling** on the **Administration** tab.
   The Automated Policies page opens.

3. Select the **Run the Automated Policies calculation** check box.

4. Select the time interval to perform the calculation and click **Save**.
   The policies will start processing at the specified date and time.

5. Select **Knowledge**, **Systems**, **General Settings** on the **Administration** tab.
   The **System** page opens.

6. Complete the following information:

   Path for EBR Index Files

   Defines the location for storing EBR index files. CA SDM creates EBR index files when you save and publish any knowledge document. Depending on your configuration type, consider the following points while defining the EBR index file path:

   - Conventional: If you are upgrading from the CA SDM Release 12.9 from r11.2 or r12.X, you may choose not to use UNC shared path. If you have not created a UNC path, CA SDM uses the default path to store EBR index files. If you are using a UNC shared drive, manually copy the ebr/ebr_ADM folders from the default location ($NX_ROOT/site/) to the UNC shared path.

- Advanced availability: If you are upgrading to the advanced availability configuration from CA SDM r11.2 or r12.X, you must create the UNC shared path and use it to store EBR index files. The UNC credentials are not required for the default path. After you create the UNC path, manually copy the ebr/ebr_ADM folders from the default location ($NX_ROOT/site/) to the UNC shared path.

  Important!EBR Index Files path & **KEIT Files path** must refer to the same UNC credentials and the path must reside on a same server to support this.

Default: $NX_ROOT/site/ebr

- **Path For Knowledge Import/Export Files**

Defines the location for storing KEIT import/export packages during an import/export operation. Depending on your configuration type, consider the following points while defining KEIT file path:

- Conventional: If you are upgrading to CA SDM Release 12.9 from r11.2 or r12.X, you may chose not to use UNC shared path. If you have not created a UNC path, CA SDM uses the default path to store the KEIT files. If you are using a UNC shared drive, manually copy the Import/Export package folders from the default location ($NX_ROOT/site/keit) to the UNC shared path.

- Advanced availability: If you are upgrading to the advanced availability configuration from CA SDM r11.2 or r12.X, you must create the UNC shared path and use it to store the KEIT files. The UNC credentials are not required for the default path. After you create the UNC path, manually copy the Import/Export package folders from the default location ($NX_ROOT/site/keit) to the UNC shared path.

  Important!EBR Index Files path & **KEIT Files path** must refer to the same UNC credentials and the path must reside on a same server to support this.

Default: $NX_ROOT/site/keit

- **UNC Credentials**

You can use this option to create UNC credentials to access the network shared drive to access EBR indexing files and import/export packages. Use the **UNC Credentials** link to create the UNC credentials.

Note: UNC paths and UNC credentials are required in case of the advanced availability configuration. Restart the CA SDM service when you change any of the UNC details (UNC paths or UNC credentials).

7. Run pdm_k_reindex as follows:

- **pdm_k_reindex -pm**
  Fixes the document links and embedded images inside the resolution field.

  Important! After you upgrade, you can get a critical error when running *pdm_k_reindex -pm*. If you get this error, browse to Knowledge, Approval Process Manager, Approval Process Settings, and change the *Permissions for Document Edit after Publish* option to *User with full permissions may edit documents,* and then run pdm_k_reindex -pm.

- **pdm_k_reindex -ml**
  Fixes the document links inside the resolution field and maps them to the database.

- **pdm_k_reindex**
  Indexes the documents so they are searchable in your knowledge environment.

The Knowledge Management environment is upgraded.

Note: After the upgrade, printing Knowledge Documents can result in a large space inserted after the Resolution section of the document. This space is inserted due to an issue with upgrading document templates from a previous release. For more information about resolving this printing issue, see the CA Service Desk Manager Known Knowledge Management Issues (see page 152).

Important! After you upgrade, Knowledge Management notification data from previous releases of CA SDM uses the Release 14.1 notification engine. For example, there are default activity notifications and notification rules for object types, such as the Knowledge Report Card.

LREL Post-Migration

This article contains the following topics:

After migration, complete the following verification steps:

1. Query the contents of the new tables to verify that the tables contain the correct data.

2. Update each site-defined report to verify that report data originates from the new LREL tables.

3. Test site-defined reports.

Deprecated Object and Tables

The following objects and tables are deprecated for this release of CA SDM. During migration, the system copies the data to Release 12.9 LREL tables. The system uses the LREL tables and objects, but for reference purposes, the old tables retain the data that was present at the time of the upgrade.

DBMS Name	Object Name
Attachment_Lrel	attmnt_lrel
Business_Management_Repository_ Lrel	bmlrel
Chgcat_Group	chgcat_grp
Chgcat_Loc	chgcat_loc
Chgcat_Workshift	chgcat_workshift
Group_Loc	grp_loc
Isscat_Group	isscat_grp
Isscat_Loc	isscat_loc
Isscat_Workshift	isscat _workshift
Knowledge_Lrel_Table	kmlrel
Lrel_Table	lrel1
Pcat_Group	pcat_grp
Pcat_Loc	pcat_loc
Pcat_Workshift	pcat_workshift
Wftpl_Group	wftpl_grp

LREL Tables and Objects

These tables and objects information help users to understand how CA SDM/CMDB schema work and troubleshoot problems. The migration process automatically creates the following tables and objects to manage many-to-many data relationships:

DBMS Name	Object Name
usp_lrel_asset_chgnr	lrel_asset_chgnr
usp_lrel_asset_issnr	lrel_asset_issnr
usp_lrel_att_cntlist_macro_ntf	lrel_att_cntlist_macro_ntf
usp_lrel_att_ctplist_macro_ntf	lrel_att_ctplist_macro_ntf
usp_lrel_att_ntflist_macro_ntf	lrel_att_ntflist_macro_ntf
usp_lrel_attachments_changes	lrel_attachments_changes

usp_lrel_attachments_issues	lrel_attachments_issues
usp_lrel_attachments_requests	lrel_attachments_requests
usp_lrel_aty_events	lrel_aty_events
usp_lrel_bm_reps_assets	lrel_bm_reps_assets
usp_lrel_bm_reps_bmhiers	lrel_bm_reps_bmhiers
usp_lrel_cenv_cntref	lrel_cenv_cntref
usp_lrel_dist_cntlist_mgs_ntf	lrel_dist_cntlist_mgs_ntf
usp_lrel_dist_ctplist_mgs_ntf	lrel_dist_ctplist_mgs_ntf
usp_lrel_dist_ntflist_mgs_ntf	lrel_dist_ntflist_mgs_ntf
usp_lrel_false_action_act_f	lrel_false_action_act_f
usp_lrel_false_bhv_false	lrel_false_bhv_false
usp_lrel_kwrds_crsolref	lrel_kwrds_crsolref
usp_lrel_notify_list_cntchgntf	lrel_notify_list_cntchgntf
usp_lrel_notify_list_cntissntf	lrel_notify_list_cntissntf
usp_lrel_notify_list_cntntf	lrel_notify_list_cntntf
usp_lrel_ntfr_cntlist_att_ntfrlist	lrel_ntfr_cntlist_att_ntfrlist
usp_lrel_ntfr_ctplist_att_ntfrlist	lrel_ntfr_ctplist_att_ntfrlist
usp_lrel_ntfr_macrolist_att_ntfrlist	lrel_ntfr_macrolist_att_ntfrlist
usp_lrel_ntfr_ntflist_att_ntfrlist	lrel_ntfr_ntflist_att_ntfrlist
usp_lrel_oenv_orgref	lrel_oenv_orgref
usp_lrel_status_codes_tsktypes	lrel_status_codes_tsktypes
usp_lrel_svc_grps_svc_chgcat	lrel_svc_grps_svc_chgcat
usp_lrel_svc_grps_svc_isscat	lrel_svc_grps_svc_isscat
usp_lrel_svc_grps_svc_pcat	lrel_svc_grps_svc_pcat
usp_lrel_svc_grps_svc_wftpl	lrel_svc_grps_svc_wftpl
usp_lrel_svc_locs_svc_chgcat	lrel_svc_locs_svc_chgcat
usp_lrel_svc_locs_svc_groups	lrel_svc_locs_svc_groups
usp_lrel_svc_locs_svc_isscat	lrel_svc_locs_svc_isscat
usp_lrel_svc_locs_svc_pcat	lrel_svc_locs_svc_pcat
usp_lrel_svc_schedules_chgcat_svc	lrel_svc_schedules_chgcat_svc
usp_lrel_svc_schedules_isscat_svc	lrel_svc_schedules_isscat_svc
usp_lrel_svc_schedules_pcat_svc	lrel_svc_schedules_pcat_svc
usp_lrel_true_action_act_t	lrel_true_action_act_t
usp_lrel_true_bhv_true	lrel_true_bhv_true

Verify Data in New LREL Tables

During data migration, the system adds to manage many-to-many relationships. You can verify the contents of the new tables and updated site-defined code and reports.

Follow these steps:

1. Query the contents of the tables to verify that they contain the correct data.
2. Update each site-defined report to verify that report data originates from the new LREL tables.
3. Update the queries with the new DBMS table references.
4. Test site-defined reports and code. Update your code to use the new LREL tables and a supported interface, such as Web Services. If necessary, update the table names in your code.

Verify Database Modifications

You can verify that your database modifications are migrated correctly to the current release of the product.

Follow these steps:

1. Review each modified table using either your database management product or WSP.
2. Verify that your modified files appear in the following directory:

   ```
   $NX_ROOT/site/mods/
   ```

Verify Web Form Modifications

You can verify that your web form modifications work correctly in the current release of the product.

Follow these steps:

1. Verify that your modified forms appear in the *$NX_ROOT/site/mods/www/htmpl* directory.
2. Verify that your web form opens correctly within a browser.
3. Verify that your web form opens correctly in Web Screen Painter.

Modify Functional Access Areas

This article contains the following topics:

A *functional access area* is a group of objects that let you restrict user access. Previous versions of CA SDM included eight fixed functional access groups to restrict access to code components.

During migration, the functional access groups migrate to new functional access areas for each role. Migration automatically handles the Majic changes, the default reference data, and role mapping to the new functional access areas.

After migration, consider the following actions:

- Review how the objects map to existing and new functional access areas and role permissions to each area. Use Web Screen Painter to verify the functional access areas.
- Use CA SDM to remap or change permissions. Verify that users have the proper access to features and objects.

Note: For details about default permissions and how objects map to the new functional access areas, see the Product Support website. For information about how to change or add functional access areas, see How Functional Access Areas Works.

The following table maps Functional access areas to code components:

Functional access area	Code Component	New
Administration	admin	No
Incident/Problem/Request	call_mgr	No
Change Order	change_mgr	No
Inventory	inventory	No
Issue	issue_mgr	No
Knowledge Document	kd	No
Notification	notify	No
Reference	reference	No
Security	security	No
Announcement	announcement	Yes
Incident/Problem/Request Reference	call_mgr_reference	Yes
Incident/Problem/Request Template	call_mgr_template	Yes
Change Order Template	change_mgr_template	Yes
Change Order Reference	change_reference	Yes
Configuration Item	ci	Yes
Configuration Item Common	ci_common_ro	Yes
Configuration Item Reference	ci_reference	Yes
Contact	contact	Yes
Group	group	Yes
Issue Template	issue_mgr_template	Yes
Issue Reference	issue_reference	Yes
Location	location	Yes
Notification Reference	notification_reference	Yes

Organization	organization	Yes
Prioritization	prioritization	Yes
Service Level	service_level	Yes
Site	site	Yes
Stored Query	stored_queries	Yes
Survey	survey	Yes
Tenant Admin	tenant_admin	Yes
Timezone	timezone	Yes
Workflow Reference	workflow_reference	Yes
Workshift	workshifts	Yes

Post-Migration Access Level Changes

After migration, you can verify functional access levels for every role. Because the objects moved to another functional access areas, the user could have access to some screens in some situations that they were denied previously. They can also be denied access to forms to which they had access previously. Both situations can occur when a new functional access area manages permissions for two of the original functional access areas.

Note: For details about default permissions and how objects map to the new functional access areas, see the Product Support web site.

Edit Access Types

When you upgrade from CA SDM r11.2, the upgrade process automatically creates roles for all access types and correctly assigns access and permissions to the roles. If you want to take advantage of the new roles in Release 12.9, you can create roles for access types.

To create roles for access types

1. Log in to the web interface as a user with the ability to access the Administration tab.
2. Click the Administration tab.
3. In the tree on the left, select Security and Role Management, Access Types.
   All available access types display.
4. Click an available access type.
5. Click the Roles tab.
6. Select a new role for the access type and click Update Roles.
   The new role is associated with the access type.

Note: You can also create a custom role and assign it to the access type.

Adjust Access Types

If you modified access types and data partitions in the previous release of CA SDM, you may have a problem with the Knowledge Management data partitions settings after upgrading. These customizations can cause a problem with the permission groups settings on categories and documents. For example, a user has access to restricted information.

Note: Even if you recreated a data partition or an access type after deleting it, verify your access type and data partition settings after the upgrade.

To adjust access types

1. Click the Administration tab.
2. Click Security and Role Management, Role Management, Role List.
3. Complete the following steps for each role:
    a. Right-click the role and select Edit.
    b. Review the Data Partition Name field under the Authorization tab.
    If this field is empty, there is no data partition associated with the selected access type, so the user has no restrictions and can access any document or category in the product, even if you set up permission groups.
    This action can be appropriate for administrators, but not for all roles. If there is no data partition associated with the role, you can create or modify one.

Email Upgrading

This article contains the following topic:

- Maileater.cfg Considerations (see page 441)

CA SDM replaces the Options Manager, Email inbound email options with a Mailbox (*usp_mailbox* table) that supplies corresponding options. The Email outbound email options are still present under the Options Manager. When you upgrade, CA SDM uses your existing email settings to configure a mailbox, instead of the default Mailbox settings that are supplied with the release. Each email option, except EMAIL_ATTACHMENT_DIR (which is no longer needed), is mapped to an option in the *usp_mailbox* table. Any option that is not set, is set as null in the table.

The following table lists options that are removed from the Email options, provided in the *usp_mailbox* table, and indicates their labels in the Mailbox Detail page:

Email Option	usp_mailbox Option	Default Mailbox Detail Label
EMAIL_ALLOW_ANONYMOUS	allow_anonymous	Allow Anonymous
EMAIL_ATTACHMENT_DIR	N/A	

Email Option	usp_mailbox Option	Default Mailbox Detail Label
		N/A **Note:** Because EMAIL_ATTACHMENT_DIR is deprecated, you must manually select an Attachment Repository if this option was set and EMAIL_ATTACHMENT_REPOSITORY was not.
EMAIL_ATTACHMENT_REPOSITORY	attmnt_repository	Attachment Repository
EMAIL_FORCE_ATTACHMENT_SPLITOUT	split_out_attachment	Force Attachment Splitout
EMAIL_IS_ATTACHMENT	attach_email	Attach Entire Email
EMAIL_SAVE_UNKNOWN_EMAILS	save_unknown_emails	Save Unknown Emails
MAIL_EATER_IMAP_HOST_PORT	host_port	Port Override
MAILEATER_CHECK_MAIL_INTERVAL	check_interval	Check Interval
MAILEATER_HOST	host_name	Hostname
MAILEATER_LOGIN_PASSWORD	password	Password
MAILEATER_LOGIN_USERID	userid	Userid
MAILEATER_POP3_HOST_PORT	host_port	Port Override
MAILEATER_SECURITY_LEVEL	security_lvl	Security Level
MAILEATER_SERVER_TYPE	email_type	Email Type

Important! The Attachment Directory setting is deprecated after you upgrade, so you *must* specify an Attachment Repository before you continue polling the mailboxes.

Maileater.cfg Considerations

Information that was previously included in the *maileater.cfg* file maps to the *usp_mailbox_rule* table after you upgrade. Consider the following information about the mapping from *maileater.cfg* to *usp_mailbox_rule*:

- The '-i' at the beginning of the line denotes case insensitivity and maps to the filter_ignore_case field.
- The search filter "Subject: *..." previously denoted a regular expression on which to filter. The "Subject:" is removed, is replaced with a "^" symbol, and the remaining value maps to the *filter_string* field. The Filter_type is set to "Subject Contains" type.
- The "TEXT_API xxx" denotes the object that is processed for the rule. The string "TEXT_API " is removed, and the remainder maps to the *action_object* field. The *action_operation* field is set to Create/Update Object.
- The reply to the user typically contains "PDM_MAIL ...". If you have "PDM_MAIL" set, set reply_method to 1800 or else leave it set to null.
- If the - s parameter is set, remove the subject field from the text and set the *reply_subject* with this value.
- The functionality maintains the order of entries. A sequence number starting at 100 and incremented by 100 is set for each valid row.

The other fields in the *usp_mailbox_rule* are set as follows:

Field	Value
mailbox	Default
action_write_to_log	0
action_log_prefix	null
delete_flag	0
description	Migrated from pdm_maileater.cfg file
reply_failure_html	<leave blank to inherit default action>
reply_failure_text	<leave blank to inherit default action>
reply_success_html	<leave blank to inherit default action>
reply_success_text	<leave blank to inherit default action>
text_api_defaults	null
text_api_ignore_incoming	null
action_subject_handling	null
last_mod_dt	null
last_mod_by	null
inclusion_list	"*"
email_address_per_hour	-1
exclusion_list	null
log_policy_violation	1

Support Automation Data Migration

This topic contains the following information:

You can migrate CA Support Automation r6.0 SR1 eFix5 data to CA SDM Release 14.1 from the following environments:

- CA Service Desk Manager r11.2
- CA SDM r12.0
- CA SDM r12.1
- CA Support Automation r6.0 SR1 eFix5 without CA SDM.

Note: You can only migration data from CA Support Automation r6.0 SR1 eFix5. We recommend that you run a full backup of the CA Support Automation r6.0 SR1 eFix5 database before migrating.

Important! Branding modifications from CA Support Automation r6.0 SR1 eFix5 do not migrate automatically. We recommend that you review the modified branding to verify that it corresponds to the CA SDM branding. If necessary, copy and paste the Header, Footer, and CSS URL data of each division to the corresponding tenant (or public) in CA SDM to migrate the branding data.

Migrate a Support Automation Database

You can configure the migration tool to migrate data from the Support Automation database to the CA SDM database, including Support Automation names transformation into the CA SDM database conventions. Migrate the data from the Support Automation database to the CA SDM database before the first usage of Support Automation.

If you do not want to migrate all the historical data from the CA Support Automation r6.0 SR1 eFix5 database, you can purge some of the historical data. You can configure the number of days to leave in the database in the purge script setup. You can download the purge script from ftp://ftp.ca.com/pub/supportbridge/6.0/patch-01/purge_history_6.0_sp1.zip.

Follow these steps:

1. Export (see page) the CA Support Automation data using the script on the installation media.
   The export tool converts the data into *.DAT* format. The tool performs the following major steps when you migrate the data:

- Import the Support Automation database schema into the CA SDM database.
  This schema creates the necessary tables that Support Automation uses.

- Migrate the data from the Support Automation database migration XML into the CA SDM database.
  The CA SDM migration tool generates necessary UUIDs and creates necessary records which represent relationships between Support Automation ID and CA SDM UUID.

2. Copy the CA Support Automation data export folder to the NX_ROOT/site/sbmigration/SA60 directory.
   The data export completes.

3. Import (see page) the data into CA SDM using the CA Support Automation Migration tool.
   The data loads into the database and migration completes.

Convert Divisions to Tenants

You can only migrate divisions from CA Support Automation r6.0 SR1 eFix5. You convert these divisions to tenants to use multi-tenancy in a Support Automation environment. You can migrate each division separately as its own tenant. During the initial data import, all rows in tenant-optional tables are made tenanted.

Important! You migrate this data before enabling Support Automation in CA SDM.

Follow these steps:

1. Export (see page) the division data using the script on the installation media.
   You can export a single division or all divisions.

2. The export tool converts the data into *.DAT* format.
   The tool displays the status of the division export.

3. Copy the CA Support Automation data export folder to the NX_ROOT/site/sbmigration/SA60 directory.
   The data export completes.

4. Import (see page) the data into CA SDM using the CA Support Automation Migration tool.
   The data loads into the database and migration completes.

Export CA Support Automation Data

You export CA Support Automation r6.0 SR1 eFix5 data by converting it to the *.DAT* format that CA SDM uses. You can export divisions into separate tenants, and import the data to a public environment. The export tool logs the process and displays the output directory of the log file after the export completes. The export process records the successful output of each table and indicates any unexpected conditions or errors it encounters.

Important! You can only migrate divisions from CA Support Automation r6.0 SR1 eFix5.

Follow these steps:

1. Execute the *SA60Export* script from the installation media in the /casd.nt/SAMigration directory:

   Note: The file extension depends on your operating system. For example, Windows uses “bat,” UNIX uses “sh” for the bourne shell script, “csh” for the C shell, or “ksh” for the korn shell, and so on.

   The CA Support Automation Migration tool appears.

2. Perform the following actions:

   a. Enter the CA Support Automation r6.0 SR1 eFix5 "WEB-INF" installation parent directory.

   b. Enter a directory to export your CA Support Automation data.
   Note: After the export completes, move this folder to the *NX_ROOT/site/sbmigration /SA60* directory on the CA SDM server.

   c. (Optional) Specify whether passwords can be exported. If you select this option, passwords are exported for users, default credentials, and automated task credentials.

   d. (Optional) Export a single division or all the divisions. If you select this option, a drop-down list displays all active divisions.

3. Click Run.
   The Process Status displays information about the export, such as the database table being migrated, and a count of the records in the table.
   A message appears if the tool detects unrecoverable errors.

   Note: You can stop the export by selecting Stop from the toolbar or file menu.

   The data export completes.

4. Configure and implement Support Automation, as appropriate to your environment.

Import Support Automation Data

You import Support Automation data after converting it to *.DAT* format. You can import the data into CA SDM using the Support Automation migration script. You invoke the utility after installing and configuring CA SDM. You can also execute *sa_migrate.pl* using the *pdm_perl* command.

You can access the script in the *NX_ROOT**bin*\ directory. The migration script performs tasks such as processing tables to maintain database constraints, creates corresponding CA SDM objects, maps tenant column values, and so on.

The default location for migration-related files in the CA SDM installation is in the *NX_ROOT/site /sbmigration* directory. For example, you can find the import configuration file in the *NX_ROOT/site /sbmigration/config* folder. The *sa_migration_config.dat* file stores the id, prop_name, value, and prop_description columns in the CA SDM data format.

The directory stores CA Support Automation r6.0 SR1 eFix5 export data, migration utility code, and Perl scripts, and so on.

Follow these steps:

1. Start the CA SDM Service.
   The service starts and you can verify that it is running.

2. Enter the following on the command line:

   ```
   pdm_perl <NX_ROOT>\bin\sa_migrate.pl
   ```

   The Support Automation data loads into the database from the export package.

How to Install CA SDM

This topic contains the following information:

For a successful CA SDM implementation, you need to understand the CA SDM deployment model and the different configurations that are available.

Deployment Model

You can deploy CA SDM using one of the following deployment models that best suits your requirement:

- **Centralized** – Installs and configures all product components on one server. This is the default installation. You can implement multiple Object Managers and web engines for load balancing and failover, however your business may outgrow this implementation.

- **Distributed** – Installs and configures product components on servers that are closer to the clients receiving the service. For example, a business with many subnets can have analysts that are using the Web Client. In this type of deployment you place an additional server at the branch location. This server performs caching and reduces the network traffic and response time between the branch location and the main server location. This type of implementation supports the implementation of multiple Object Managers and web engines for load balancing and failover.

- **Global** – Having two or more centralized or distributed implementations that are known as regions. The main server of a region replicates minimal information to and from a master region. Hence, a single region can have all necessary information about all other regions. An analyst is aware of tickets from all regions and can connect to a region when required. This type of implementation is useful when network bandwidth is too limited for a distributed implementation. For example, business locations in different countries with a slow link between them.

CA SDM Configuration

Conventional (see page 447) or the advanced availability (see page 448) are two types of configurations that are deployed using the centralized and distributed models. You can install CA SDM using one of the configurations.

CA SDM Architecture for Conventional Configuration

The conventional configuration includes a primary server, a database, and one or more secondary servers. The secondary servers are optional; configure them to support a large number of concurrent users. Only the primary server can access the database directly. The secondary servers access the database through a central process that is available on the primary server. A secondary server can be removed from the configuration without disrupting other servers. Only the users connected to the specific secondary server are affected.

When to Opt for Conventional Configuration

Conventional is the default configuration and is suitable for smaller deployments. Choose the conventional configuration if you do not require any high availability. Be aware that with conventional configuration, the application is not available during maintenance or when a server crashes.

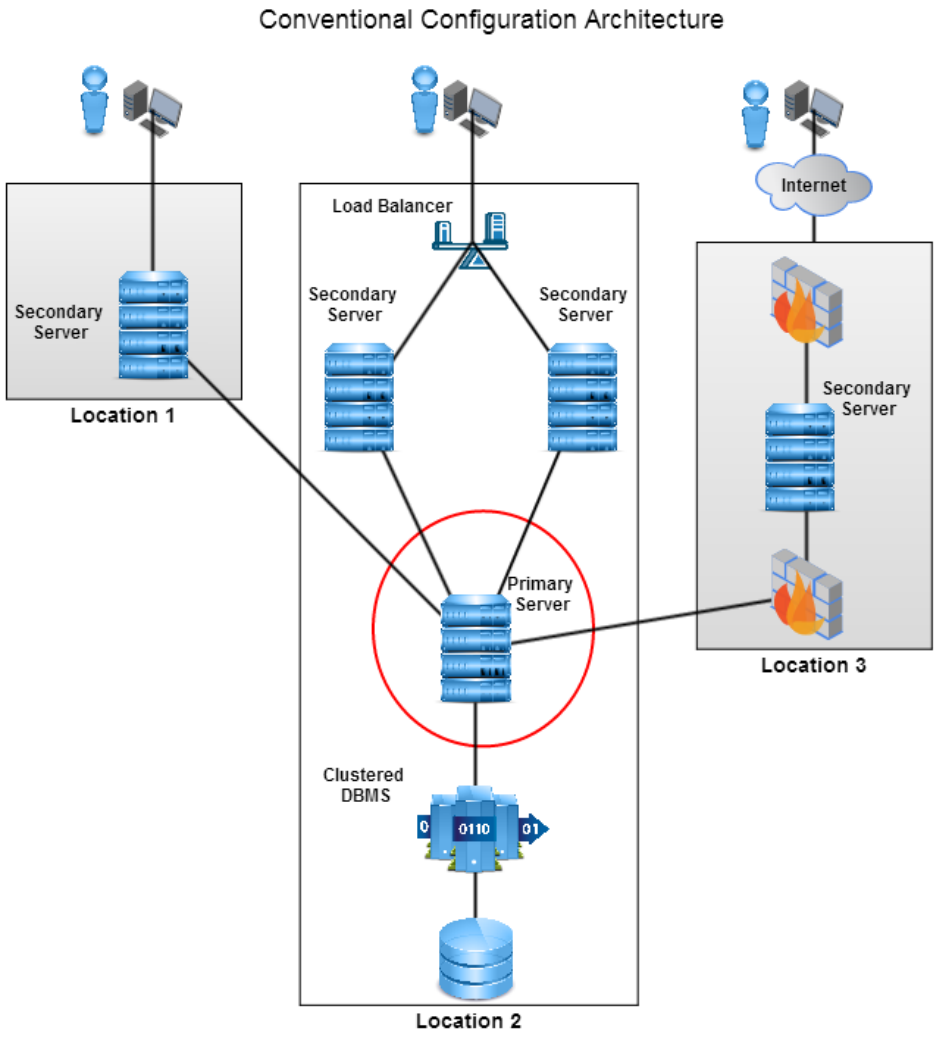
Primary Server

The Primary Server is the main server in a conventional configuration. In a single server CA SDM configuration, the server is the Primary Server. When CA SDM is distributed across two or more servers, one server is designated as the Primary Server. This server performs roles in the configuration such as accessing the database. There is always only one Primary Server.

Secondary Server

A Secondary Server is configured when there are more than one CA SDM server in a configuration. In this scenario, all servers other than the Primary Server are configured as Secondary Servers. Secondary servers perform only a subset of the roles of the Primary Server. Secondary Servers are added to a configuration to scale CA SDM to handle more users.

The following diagram provides an example of the conventional configuration architecture:



CA SDM Architecture for Advanced Availability

The advanced availability configuration includes a background server, one or more standby servers, and one or more application servers. To reduce the single point of failure, each of these servers has a direct connection with the database. All the components of the architecture communicate using an internal CA protocol.

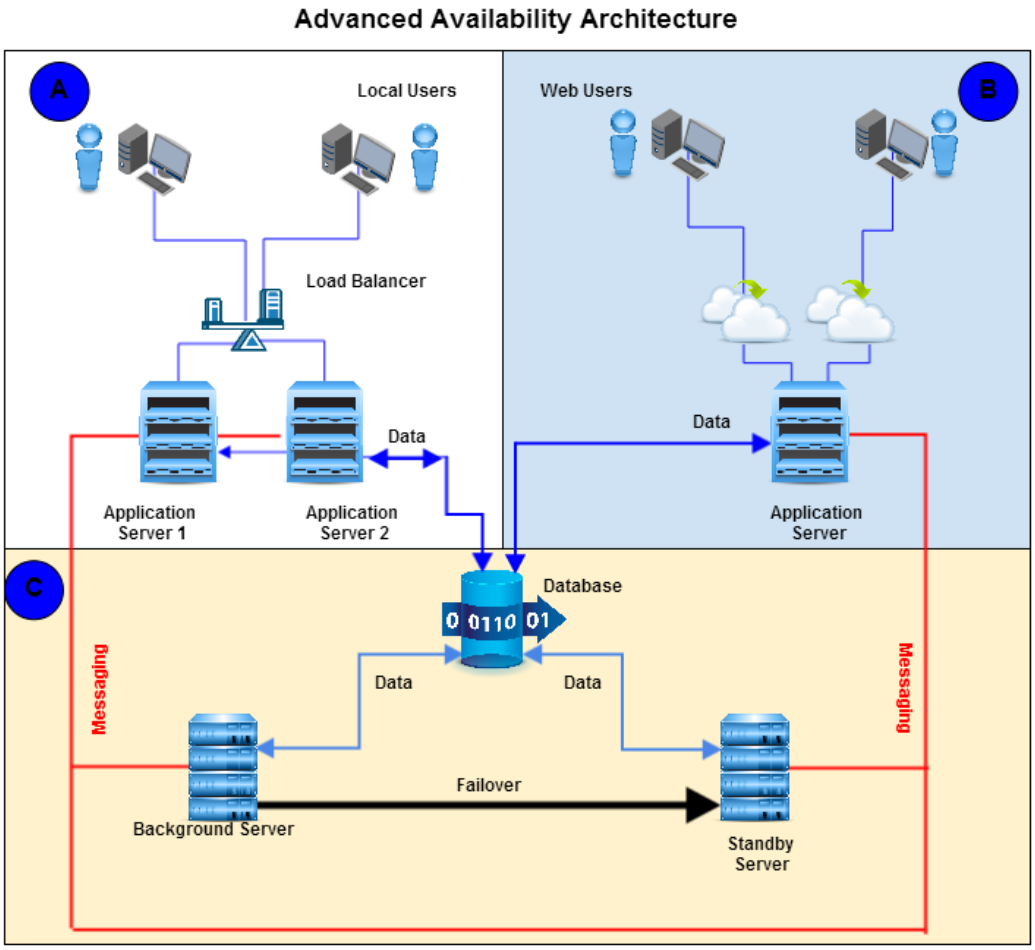
When to Opt for Advanced Availability Configuration

The advanced availability configuration provides higher availability, reduces down times, and supports rolling maintenance. Consider the advanced availability configuration when any of the following factors is true:

- You require a high degree of CA SDM availability.
- You require the CA SDM servers to be more independent and more resilient to failures.

- You require an ability to remove and return the CA SDM servers to service, without bringing down the entire CA SDM installation.
- You require near zero downtime during rolling maintenance.

The following diagram provides an example of advanced availability architecture:



The architecture is spread across three different locations A, B, and C. Location A has two application servers, serving users through a load balancer. The location B has an application server directly serving the users and the location C has the background server, the standby server, and the database. Each of the servers has direct connection to the database. The blue lines mark the flow to and from the database. The red lines identify the internal communication between the components.

Background Server

The background server is the core of the advanced availability architecture. This server provides ancillary services to other servers and runs all singleton processes of CA SDM. A process can be is designated as singleton when only single copy of it can be active in any SDM installation. Only the users with the Administrator Access Type have access to the background server. To increase the availability, the standby server shadows the background server. You can switch the standby server as the background server in case of any failure or when performing rolling maintenance.

Standby Server

The primary function of the standby server is to act as a warm standby for the background server. The standby server has the same hardware and OS platform as the background server. The standby server can run all processes that run on the background server. The standby server stays idle during normal working of the system. However, it listens to the internal CA SDM system messages for database changes and updates the critical caches continuously. If the background server fails or requires rolling maintenance, you can promote the standby server to background server. When you promote the server, the application servers as well as the end users have minimal disruption. You can invoke a utility to perform this switchover.

The standby server is only running a small subset of the processes that normally run on the background server. You cannot log on to the web interface on the standby server.

Application Server

The application server has all the CA SDM components necessary to serve the end users through various interfaces like web, SOAP, and RESTful web services. The application servers are independent of each other and resilient to the background server outages for short periods of time. Users access the application servers. You can individually remove the application servers and return to service by using the new Quiesce facility. The quiesce facility allows current users to complete their work and then sign in to an alternate application server.

More information:

- Step 1- Plan your CA SDM Installation (see page 450)
- Step 2- Install CA SDM (see page 479)
- Step 3- Install Other Components (see page 498)
- Step 4- Post-Installation Requirements (see page 504)
- Step 5- Configure the Servers (see page 505)
- Step 6- Verify the Installation (see page 519)
- Troubleshooting the Installation (see page 523)
- Secure CA SDM from Cross-Site Scripting Vulnerabilities (see page 524)
- Install and Configure JRE 1.8.0_45 (see page 525)

Step 1- Plan your CA SDM Installation

Before you start installing CA SDM, ensure that you have reviewed the following considerations:

- Hardware and Software Requirements for the Install (see page 452)
- Installation Considerations (see page 467)

(Recommended) After you review the considerations, keep the following checklist in place while you are installing CA SDM, to ensure that you do not miss any critical step.

Select	Task	Comments
	Installed the database of your choice (SQL Server or Oracle).	
	Decided the type of configuration (advanced availability or conventional) that you would want to implement.	
	Decided the number of servers required for the CA SDM installation.	
	Ensured that the hardware and software requirements are met.	
	To help ensure that you can configure the product and components on the **Micros oft SQL Server**, you completed the following steps: 1. a. Enabled TCP/IP on the computer on which you want to perform the installation and configuration. b. Obtained the following information: ▪ ▪ ▪ ▪ The named instance of the server that is running Microsoft SQL Server. ▪ The Microsoft SQL Server database user name and password. ▪ The Microsoft SQL Server database port number.	
	To help ensure that you can configure the product and components on **Oracle**, you obtained the following information: 1. a. Whether the Oracle database is local or remote. b. Whether you need to create tablespaces. c. The Net service name. d. The DBA user name and password. e. The data and index tablespace name. f. The complete path for the tablespace. g. JDBC connection information, including the system identifier (SID) and listener port.	
	(For configuring to a 64-bit Oracle database on a 64-bit computer) Pointed the system library path to the 32-bit Oracle libraries. The 32-bit Oracle libraries are found in $ORACLE_HOME/lib32.	
	(For configuring a 64-bit Oracle 11g database on a 64-bit computer) Installed the Oracle 32-Bit Client on the server and while configuring the database pointed the system library path to the 32-bit Oracle libraries. This step is required for both configuration and runtime. Also, created a net service name on the Oracle client to point to the Oracle database server instance.	
	(If you are using an Oracle database and you want to use existing tablespaces) Created a Data tablespace that is at least 400 MB, and an Index tablespace that is at least 100 MB before configuring CA SDM.	
	Increased the hardware configuration of the DBMS server. Each of the servers is directly connected to the database, leading to an increased resource contention at the DBMS level.	

Select	Task	Comments
	If you are installing CA SDM in the pure IPV6 environment, the installation may fail. Ensure that the NX_PROTOCOL_ONLY variable is set to IPV6 and click on Retry Install.	
	(If you plan to install Unified Self-Service with CA SDM) Before you install Unified Self-Service, download Liferay CE 6.1.2 GA3 edition zip file (https://www.liferay.com/downloads/liferay-portal/available-releases). **Note:** Do not Install Liferay Manually as the installer unzips the downloaded file and installs Liferay.	
	(If you would like to identify performance problems in CA SDM) For a Windows installation, install the pslist.exe tool and add its directory path variable to the system path variable. For more information, see the How to Identify Performance Problems in CA SDM (see page 3329) topic.	
	(If you have CA Business Intelligence 3.3 and if you want reporting capability) Install CA Business Intelligence Release 4.1 SP3 (see page 285) and then install CA SDM	
	For CA Business Intelligence ODBC services to start properly, export the library path, as follows: ▪ (For AIX) Export LIBPATH=$LIBPATH:<CA_SharedComponent>/lib:<NX_ROOT>/lib **Example:** Export LIBPATH=$LIBPATH:/opt/CA/SC/lib:/opt/CAisd/lib ▪ (For Solaris/Linux) Export LD_LIBRARARY_PATH=$ LD_LIBRARARY_PATH:/opt/CA/SC/lib:<NX_ROOT>/lib **Example:** Export LD_LIBRARARY_PATH=$ LD_LIBRARARY_PATH:/opt/CA/SC/lib:/opt/CAisd/lib	

Hardware and Software Requirements for the Install

Review the following requirements before you proceed with the installation:

- Operating Systems (see page 452)
- Database Management Systems (see page 454)
- Hardware Requirements (see page 455)
- Server Components (see page 458)

Operating Systems

Find more information about version numbers of each operating system in the Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix). Depending on the operating system that you use, ensure that you read the following considerations.

IBM AIX Operating Systems

- Before installing CA SDM (or migrating from a previous release), the IBM XL C/C++ Runtime Environment version 9.0.0.9 (or later) must be installed and running on IBM AIX servers.

- You can integrate CA SDM with CA Business Intelligence, which uses Business Objects Enterprise XI, although we do not support installing CA Business Intelligence on IBM AIX.
- On IBM AIX, install CA EEM by following the instructions provided when CA EEM is selected during installation.

Important! CA SDM does *not* provide tools.jar and javac for AIX. Configuring REST Web Services and Support Automation requires the tools.jar file. To use the REST sample files, you must install javac on AIX. You can download the Java SDK for AIX from the IBM website in the IBM Developer kits section for Linux. Download the 32-bit binaries of Java SE and install JDK 1.7 SR4 on the AIX computer at any location. Copy tools.jar from the installed JDK location to <Shared Component>\JRE\1.7.0_04\lib and copy javac to \JRE\1.7.0 _04\bin. You can also find the JRE location in the NX_JRE_INSTALL_DIR variable. You *must* copy the tools.jar file across all AIX installation, before you run the product configuration.

Redhat Enterprise Linux Operating Systems

- You can integrate CA SDM with CA Business Intelligence, which uses Business Objects Enterprise XI, although we do not support installing CA Business Intelligence on Redhat Linux.
- Verify that you have the following Java libraries on Redhat Linux to launch the product installer:
  - java-1.4.2-gcj-compat-1.4.2.0-40jpp.115
  - java-1.4.2-gcj-compat-devel-1.4.2.0-40jpp.115
  - java-1.4.2-gcj-compat-devel-1.4.2.0-40jpp.115
  - java-1.4.2-gcj-compat-src-1.4.2.0-40jpp.115
- To install CA SDM on RedHat Enterprise Linux 6.0 successfully, verify that you have the following RPM packages and their dependencies:

Required RPM	Dependencies
libXp-1.0.0-15.1.el6.i686.rpm	▪ libXau-1.0.5-1.el6.i686.rpm ▪ libxcb-1.5.1-1.el6.i686.rpm ▪ libXext-1.1.3-1.el6.i686.rpm ▪ libX11-1.3.2-1.el6.i686.rpm
libXtst-1.0.99.2-3.el6.i686.rpm	libXi-1.3.3-3.el6.i686.rpm
openssl-1.0.0-4.el6.i686.rpm	▪ zlib-1.2.3-25.el6.i686.rpm ▪ libselinux-20.94-2.el6.i686.rpm ▪ keyutils-libs-1.4-1.el6.i686.rpm ▪ krb5-libs-1.8.2-3.el6.i686.rpm
openldap-2.4.19-15.el6.i686.rpm	▪ db4-4.7.25-16.el6.i686.rpm

Required RPM	Dependencies
	▪ cyrus-sasl-lib-2.1.23-8.el6.i686.rpm
pam-1.1.1-4.el6.i686.rpm	▪ ▪ cracklib-2.8.16-2.el6.i686.rpm ▪ audit-libs-2.0.4-1.el6.i686.rpm ⚠ **Note**: These 32-bit packages (pam-1, cracklib-2, and audit-libs-2) are required on both 32-bit and 64-bit systems.

- ▪ Verify that you have the following pcre and libuuid packages:
  - pcre-7.8-3.1.el6.i686.rpm
  - libuuid-2.17.2-6.el6.i686.rpm

⚠ **Note**: These 32-bit packages (pcre-7 and libuuid-2) are required on both 32-bit and 64-bit systems.

Oracle Solaris Operating Systems

- You can integrate CA SDM with CA Business Intelligence, which uses Business Objects Enterprise XI, although we do not support installing CA Business Intelligence on Oracle Solaris.
- You can install CA EEM on Oracle Solaris, however CA SDM on Oracle Solaris cannot use external authentication for CA EEM on any platform. The CA EEM authentication feature requires the site to move the boplgin daemon to a Windows, Linux, or AIX operating system. The boplgin daemon on Oracle Solaris cannot integrate with the CA EEM Server on any platform.

Novell SUSE Linux (SLES) Operating Systems - You can integrate CA SDM with CA Business Intelligence, which uses Business Objects Enterprise XI, although we do not support installing CA Business Intelligence on SUSE Linux.

VMware Operating Systems - If you want to configure CA SDM on Windows in a network address translation (NAT) environment, modify the local HOSTS file with the hostname and IP address of your server. You can find the hosts file in the *system32**drivers**etc**hosts*\ directory.

Database Management Systems

Consider the following information:

- For UNIX/Linux Oracle implementations, set the Oracle environment variables before you install or migrate CA SDM.
- To resolve some known issues with Oracle 11g, you *must* force case sensitivity by setting the NX.env variable as NX_ORACLE_CASE_INSENSITIVE=0. We recommend that you also set NX_DSSORT to BINARY to make the domsrvr sort case sensitive. After upgrading to the latest release of Oracle 11gR2 (which *must* include Oracle patch 10248523), you can reset NX_ORACLE_CASE_INSENSITIVE=1 for case insensitivity support.

- If you want to use a remote MDB, the database client (Oracle or SQL Server) *must* be installed on the same computer where you install CA SDM.
- (For Oracle database only) 32-bit ORACLE client must be installed on all CA SDM servers.
- We support remote MDB on HP UNIX with Oracle 11g R2.

Hardware Requirements

We recommend that at least 512 MB of temporary disk space is available for the CA SDM installation and 256 MB of temporary disk space is available for CA MDB installation. If the temporary disk space on your system is less than the recommended minimum value, use the IATEMPDIR variable to redirect this temporary space of the installer to another folder.

Note: If you plan to install Unified Self-Service with CA Service Desk Manager, 2 GB RAM is required in addition to the listed hardware requirements.

(Advanced availability configuration) The following requirements must be met or exceeded for a CA SDM server to install and run properly:

Server Type	CPU Requirements	RAM Requirements	Disk Space Requirements
Standby or Background server	Minimum Dual Processor 2 GHz Preferred Quad Core Processor 2 GHz	Minimum 4 GB Recommended 8 GB	4 GB (for product installation and for minimal application log growth.)
Application server (minimum recommended configuration for each of the application servers must be the same)	Minimum Dual Processor 2 GHz Preferred Quad Core Processor 2 GHz	Minimum 4 GB Recommended 8 GB (Can be increased based upon the number of *domsrvr or webengine pairs)	4 GB
Remote MDB	Minimum Dual Processor 2 GHz	Minimum 4 GB Recommended 8 GB	20 GB (recommended minimum disk space) You should also allow for

Server Type	CPU Requirements	RAM Requirements	Disk Space Requirements
	Preferred Quad Core Processor 2 GHz		incremental growth to accommodate both new MDB table entries and to provide enough space for additional Service Desk-related documents.
Attachments It is not recommended to have the attachment repository location as part of the standby or background or application server to avoid any link breakup during failover. It is recommended to keep it on an independent file server, preferably on a shared storage location, For advanced availability configuration, you may use SAN with RAID 5 configured. Best performance is achieved by using multiple repositories on multiple application servers.			Based on your organization requirements.

(Conventional configuration) The following requirements must be met or exceeded for a CA SDM server to install and run properly:

Server Type	CPU Requirements	RAM Requirements	Disk Space Requirements
Primary server	Minimum Dual Processor 2 GHz	Minimum 4 GB Recommended 6 GB (Can be increased based upon the number of domsrvr or webengine pairs)	4 GB
Secondary server	Minimum Dual Processor 2 GHz	Minimum 4 GB Recommended 6 GB (Can be increased based upon the number of *domsrvr or webengine pairs)	4 GB
Remote MDB		Minimum 4 GB Recommended 8 GB	20 GB (recommended minimum disk space)

Server Type	CPU Requirements	RAM Requirements	Disk Space Requirements
	Minimum Dual Processor 2 GHz Recommended: Quad Core Processor 2 GHz		You should also allow for incremental growth to accommodate both new MDB table entries and to provide enough space for additional Service Desk-related documents

Note: Use only one *DOM server or Web engine pair for each CPU and allocate 1GB RAM per pair.

The following requirements must be met or exceeded for a CA SDM Web Client computer to access CA SDM with better performance:

Hardware	Requirements
CPU	Dual Processor 2.0 GHz preferred
RAM	Minimum 2 GB available free memory
Disk Space	4 GB

Based on the size of your CA SDM environment, the following requirements must be met or exceeded for the product install and run properly:

Database Size	Hardware	Requirements
Small—Used for installing CA SDM in a test environment.	CPU	Minimum Dual Processor 2.0 GHz
	RAM	Minimum 2 GB
	Disk Space	4 GB minimum. This will increase over time to accommodate database growth.
Medium—The CA SDM default. The recommended setting for most CA SDM installations.	CPU	Dual Processor 2.0 GHz
	RAM	Minimum 4 GB Recommended 6 GB
	Disk Space	4 GB minimum. This will increase over time to accommodate database growth.
Large—Used for large CA SDM installations.	CPU	Quad Processor 2.0 GHz

Database Size	Hardware	Requirements
	RAM	Minimum 4 GB Recommended 8 GB
	Disk Space	4 GB minimum. This will increase over time to accommodate database growth.

* The domsrvr or DOM server is the internal daemon which manages the objects in the memory. The webengine is the internal daemon which generates the HTML pages and sends it to the client. A single webengine and domsrvr are deployed in pairs. Each pair requires one dedicated processor core and at least 1 GB of RAM. Each webengine or domsrvr pair can serve 200-250 users. If you need to add more than one pair for scaling up the system, ensure that you have the necessary processor and the RAM are available.

Note: The data files directory of the database server for the MDB requires at least 2 GB of space.

Important! When CA SDM is up and running, it is recommended to check the process memory. For optimal performance, we recommend the following method:

1. Set a notification when the process memory exceeds 1.25 GB and begin a check on the processes that are running.
2. Set a warning notification when the process memory exceeds 1.5 GB and take corrective actions to check the memory usage.

Server Components

CA SDM includes components that work together and run on different servers, depending on the CA SDM configuration. Before, you begin your implementation, ensure that you have a basic understanding of the following components:

Daemon Manager (pdm_d_mgr)

Starts process sets as defined in the startup file, pdm_startup. By default, the daemon manager tries to start a failed component up to 10 times. To check the status of all CA SDM components, use the pdm_status utility. The pdm_d_refresh utility instructs the daemon manager to start a new cycle of 10 attempts to start any process marked as previously failed.

The daemon manager runs on all CA SDM servers.

Message Dispatcher (sslump_nxd)

Acts as a common bus or message passing system. Components that need to communicate with each other first register with the Message Dispatcher. When a component sends a message, the Message Dispatcher delivers it to those components that have registered to receive that type of message. If two components communicate so much that it would be inefficient to pass the messages through the Message Dispatcher, they create a fast channel between them. You can view a list of registered components using the slstat utility.

The message dispatcher runs on the following servers, depending on your CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: All servers

Database Agent (platform_agent)

Performs SQL queries on the database. Database agents adhere to the logical schema of CA SDM and translate the SQL at this level to the physical database platform SQL.

Note: The database agent detects momentary disconnection and failed queries, and attempts to reconnect and communicate with the database. This is only meant for short outages, such as for a brief network outage and momentary disconnection. It is not meant for long outages such as shutting down a database service for maintenance, and so forth. The agent will only retry the connection for a defined number of times (the default is 3 times), and only for a short time period of a few minutes. If the outage is longer than a few minutes, the agent will stop trying to connect, and CA SDM must be recycled after the database has been made available again.

The database agent runs on the following servers, depending on your CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: All servers

Agent Provider (platform_prov_nxd)

Starts or stops database agents. By default, a number of agents are running. If more are required to handle the number of database queries, the Agent Provider starts them. If the system no longer requires so many database agents, the Agent Provider terminates the unnecessary ones.

The agent provider runs on the following servers, depending on the CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: All servers

Virtual Database (bpvirtdb_srvr)

Enables the operation of multiple Object Managers. All Object Managers running on primary or secondary servers connect to the Virtual Database, which arbitrates their access to database agents. For example, when retrieving a new range of ticket reference numbers, the Virtual Database helps ensure that only one Object Manager at a time accesses the table containing the reference numbers. The Virtual Database also performs caching of database information for Object Managers.

The Virtual Database runs on the following servers, depending on CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: All servers

Continuous Archive and Purge (arcpur_srvr)

Runs your archive and purge rules as configured by the CA SDM administrator.

The Continuous Archive and Purge runs on the following servers depending on CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: Background server

Database Monitor (dbmonitor_nxd)

Monitors changes to common tables in the CA MDB, for example, ca_contact.

The Database Monitor runs on the following servers depending on CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: Background server

Mail Daemon (pdm_mail_nxd)

Sends outbound email notifications.

The Mail Daemon runs on the following servers, depending on the CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: All servers

Mail Eater (pdm_maileater_nxd)

Accepts inbound email for ticket creation and updates.

The Mail Eater daemon runs on the following servers, depending on the CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: Background server

Notification Manager (bpnotify_nxd)

Manages notifications in a Windows environment.

The Notification Manager runs on the following servers, depending on the CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: Application, background, and standby servers

Spell Checker (lexagent_nxd)

Performs spell checking as requested by clients.

The Spell Checker runs on all CA SDM servers.

Text API Daemon (pdm_text_nxd)

Creates and updates tickets by external interfaces, such as the command line and email.

The Text API daemon runs on all CA SDM servers.

Timed Event (animator_nxd)

Runs the delay times of events. In an implementation that has many service types or contracts, there may be many active events that the Timed Event engine has to track. In this situation, you must dedicate the primary server Object Manager entirely to the Timed Event engine. You can configure other Object Managers on the primary or secondary servers for product access as appropriate.

The Timed Event daemon runs on the following servers, depending on CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: Background server

Time-To-Violation (ttv_nxd)

Calculates projected violation times for service types.

The Time-To-Violation daemon runs on the following servers, depending on the CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: Background server

Proctor Daemon (pdm_proctor_nxd)

(Windows only) Starts and restarts the CA SDM components, as instructed by the Daemon Manager, on primary and secondary servers. When you install a secondary server, the pdm_proctor_nxd process is installed as the CA SDM Remote Daemon Proctor service. When the primary server starts,

the Daemon Manager instructs the Remote Daemon Proctor to connect to the Message Dispatcher. The Daemon Manager then instructs the Remote Daemon Proctor to start components on the secondary server. The process for starting the components is defined by the Process Sets in the startup file pdm_startup.

The Proctor daemon runs on all the CA SDM servers in advanced availability configuration.

Object Manager (domsrvr)

Acts as the server process of CA SDM. When you install a primary server, by default, two Object Managers are installed: one for connections to the product, and one dedicated to the Web Screen Painter. Having multiple Object Managers helps you test your modifications without affecting the production environment. When you install a secondary server, you can configure more Object Managers.

There must always be a default Object Manager running on the primary server to which clients such as the Timed Event engine can connect.

The Object Manager also caches various records and tables for clients. If you use pdm_userload to manipulate these records, you can also use the pdm_cache_refresh utility to make the Object Manager retrieve the new data.

The Object Manager runs on all the CA SDM servers in advanced availability configuration.

Method Engine (spel_srvr)

Runs SPEL code, event, macros, and so forth, for an Object Manager. We recommend that you run every Object Manager with its own method engine.

The Method Engine runs on all CA SDM servers.

Login Server (boplgin)

Manages authenticated user sessions.

The Login Server runs on the following servers, depending on the CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: All servers

LDAP Virtual Database (ldap_virtdb)

Interfaces with an LDAP directory.

The Method Engine runs on the following servers depending on the CA SDM configuration:

- Conventional: Primary or secondary server
- Advanced Availability: Background or application server

Knowledge Management Search Daemon (bpebr_nxd)

Performs knowledge base searches. Upon CA SDM startup, the bpebr_nxd daemon caches Knowledge Document data in its memory from the database. With a large document base, you might have memory resource issues. The bpebr_nxd daemon has the following size requirements:

Knowledge Management Search

- 100,000 documents
- Memory size = 332,000 KB

The Knowledge Management daemon runs on the following servers depending on the CA SDM configuration:

- Conventional: Primary or secondary server
- Advanced Availability: Background server

Knowledge Management/Keyword Indexing Daemon (bpeid_nxd)

Indexes the knowledge base.

The Keyword Index daemon runs on the following servers depending on the CA SDM configuration:

- Conventional: Primary or secondary server
- Advanced Availability: Background server

Knowledge Management FAQ Ratings Daemon (bu_daemon)

The bu_daemon runs on the following servers depending on the CA SDM configuration:

- - Conventional: Primary or secondary server
  - Advanced Availability: Background server

Knowledge Report Card Daemon (krc_daemon)

Performs the calculations for the Knowledge Management Knowledge Report Card (KRC) feature. This feature enables analysts and managers to display different matrix views of their knowledge contributions and provide feedback about which documents are most effective. The information that is provided can be used to improve the processes of creating knowledge documents and providing the best support to customers.

The Knowledge Report Card daemon runs on the following servers depending on the CA SDM configuration:

- Conventional: Primary or secondary server
- Advanced Availability: Background server

Knowledge Management Daemon (kt_daemon)

Manages knowledge base administration and knowledge management logic. It also manages notifications and the document approval process.

The Knowledge Management daemon runs on all CA SDM servers.

Repository Daemon (rep_daemon)

Manages the attachment repositories for CA SDM and the Knowledge Management/Keyword Search Daemon.

The Repository Daemon runs on the following servers depending on the CA SDM configuration:

- Conventional: Primary or secondary servers
- Advanced Availability: All servers

Version Control Daemon (pdm_ver_nxd)

Synchronizes the schema files between a primary and secondary server to ensure that they are using the same schema.

The Version Control Daemon runs on the following servers depending on the CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: Background server

Apache Tomcat Web Server (javaw)

Enables certain features to be implemented, regardless of whether Microsoft Internet Information Server (IIS) is used as the web server for access to CA SDM. These features include Graph Items, Attachments, and Web Services.

The Apache Tomcat web server can be administered with the apache Tomcat controller (*pdm_tomcat_nxd*).

The Apache Tomcat Web Server runs on all CA SDM servers.

Web Engine (webengine)

Connects to web browsers through a pdmweb cgi running on a Microsoft IIS or Apache Tomcat web server. There must be at least one web engine for WSP on the following servers, depending on your CA SDM configuration.

- Conventional: Primary server
- Advanced availability: Application, standby, and background servers

This process ensures that WSP Schema Designer can write schema files. Web engines are the true client of an Object Manager, which the web browser uses to access the product.

Web engines cache .htmpl web forms for connected users. You can manipulate the cache using the pdm_webcache utility and can see connection statistics using the pdm_webstat utility.

The Web Engine runs on all CA SDM servers.

RF Broker (pdm_rfbroker_nxd)

(Applicable for advanced availability configuration only). Manage the roles of the servers and controls them across the configuration. This daemon runs on all servers in advanced availability configuration and performs the following tasks:

- Acquire information about background and standby servers.
- Update information (such as slump ID, node name, server type) in the ServerStatusMonitor class.
- Receive broadcast messages of server status changes.
- Quiesce the requests. Register for SLUMP_NODE_GONE messages that are forwarded to ServerStatusMonitor objects when the failing node is the background server.

Login User Authentication (bopauth_nxd)

This daemon performs the operating system user account validation. To match a user with an access type, the contact record lookups using the System Login field.

If your business provides CA SDM for other client businesses, place the Login server on a secondary server at a single client location. The external authentication is then enabled in access types. Based on the CA SDM configuration, the daemon runs on the following servers:

- Conventional: Primary or secondary (if configured) server
- Advanced Availability: Background or application (if configured) server

Interval Logger (pdm_intrvlog_nxd)

The interval logger daemon gathers the debugging information for debugging the system. Runs on all CA SDM servers.

QRY KPI Daemon (kpi_qry_daemon)

Executes the SQL queries for updating the Key Performance Indicators (KPIs) in the database. The QRY KPI daemon runs on the following servers, depending on the CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: Background server

SYS KPI Daemon (kpi_sys_daemon)

Daemon to collect system type key performance indicators and write to the database. The SYS KPI daemon runs on the following servers, depending on your CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: All servers

Confirm Database (confirm_db)

A utility to verify database access that runs on all CA SDM servers.

Data Dictionary (ddictbuild)

A utility to build the data dictionary and runs on all CA SDM servers.

Set LogFile (pdm_logfile)

A utility to display or set the log file size limits. The pdm_logfile daemon runs on all CA SDM servers.

Report Manager (pcrpt_nxd)

A utility for PC reporting that runs on all CA SDM servers.

RPC Server (rpc_srvr)

Used for making outbound SOAP web service calls and runs on all CA SDM servers.

CA SA Tomcat (sa_tomcat)

CA SA Tomcat to run support automation and can be configured on any CA SDM server.

Visualizer Tomcat (viz_tomcat)

The Tomcat instance to run visualizer and can be configured on the following servers:

- Conventional: All servers
- Advanced Availability: Application server

Event Manager (ehm_nxd)

The Event Manager manages events coming from CA NSM. The Event Manager runs on the following servers, depending on the CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: Background server

Knowledge Management Indexing Daemon (bpeid_nxd)

Responsible for indexing the knowledge documents and runs on the following servers:

- Conventional: Primary server
- Advanced Availability: Background server

Registration Server (mdb_registration_nxd)

An agent for handling MDB registration requests. The Registration Server runs on the following servers, depending on your CA SDM configuration:

- Conventional: Primary server
- Advanced Availability: All servers

Installation Considerations

This article includes the following topics:

This topic provides the general information that you must be aware of, before you install CA SDM. Read the considerations for the specific operating systems and components that are described in the respective sections.

General Considerations for CA SDM

Installation Home Directory

When installing CA SDM, do not install the CA Shared Components in the same directory as the CA SDM installation directory (NX_ROOT).

Note: References to NX_ROOT pertain to the environmental variable containing the installation path of CA SDM. The NX_ROOT variable is set in the NX.env configuration file that is used to set environmental variables for CA SDM.
Example: NX_ROOT Definition
@NX_ROOT=C:\Program Files\CA\Service Desk Manager

(Applicable for Windows only) Filesystem

Complete the following steps to ensure that the filesystem where you are installing CA SDM is 8.3 enabled:

1. Run the following command on the drive where you plan to install CA SDM:
   <installation drive>:\Users\Administrator>FSUTIL.EXE 8dot3name query *<installation drive>:*
   For example, if you are using the D drive to install CA SDM, then the following command must be used:

   ```
   D:\Users\Administrator>FSUTIL.EXE 8dot3name query d:
   ```

2. If 8dot3 name creation is **disabled** on D drive, the following result is displayed:

```
The volume state is: 1 (8dot3 name creation is disabled).

The registry state is: 2 (Per volume setting - the default).
```

3. To enable, run the following command:
   <installation drive>: \Users\Administrator> FSUTIL.EXE 8dot3name set *<installation drive>*: 0
   For example,

```
D:

\Users\Administrator>

FSUTIL.EXE 8dot3name set d: 0
```

Database

- If CA SDM has been configured with one database, and then the configuration is run a second time with a different database type, the configuration does not work. For example, you initially configure for SQL Server and you configure again for an Oracle database. The workaround is to restart the computer before the second configuration is run.
- Database connection information, if different, is not accepted in subsequent configurations. If an additional configuration is needed as a result of a change in the database connection information, delete the $NX_ROOT\NX.env file before proceeding.
- **Oracle**
- - When configuring to a 64-bit Oracle database on a 64-bit computer, the system library path must point to the 32-bit Oracle libraries. The 32-bit Oracle libraries are found in $ORACLE_HOME/lib32.
- - For configuring a 64-bit Oracle 11g database on a 64-bit computer, you must also install the Oracle 32-Bit Client on the server. When configuring the database, the system library path must point to the 32-bit Oracle libraries. This step is required for both configuration and runtime. Also, create a net service name on the Oracle client to point to the Oracle database server instance.
- - Suppose that you are using an Oracle database and you want to use existing tablespaces. Create a Data tablespace that is at least 400 MB, and an Index tablespace that is at least 100 MB before configuring CA SDM.
- - Set the Oracle environment variables before you install or migrate CA SDM, as follows:
- - Verify that the ORACLE_HOME variable is set correctly.

Important! Export TWO_TASK variable when Oracle 32-bit client variables are exported on non-Windows operating systems.

-

- Include the 32-bit Oracle libraries (typically $ORACLE_HOME/lib32 for 64-bit Oracle) in the library path variable LD_LIBRARY_PATH (LIBPATH on AIX).

Internationalization

- You cannot use multi-byte characters for either the user you are logged in as or for the CA SDM privileged username. This applies when you install on multi-byte operating systems such as Simplified Chinese and Japanese. Doing so causes the installation to fail.
- Do not specify multi-byte characters in the file path names during installation and configuration. Doing so causes one or both to fail.
- CA SDM must run on UTF-8 locale on Linux and UNIX platforms.
- The Timespan Symbol names that are provided with the default CA SDM installation (Administration tab, Service Desk, Application Data, Codes, Timespans) are in English. For example, TODAY, YESTERDAY, THIS MONTH. For localized versions of the product, administrators may want to define new localized Timespans as required. Do not delete or modify the default Timespans.
- Date formats in CA SDM do not support international specifiers such as, localized date-picture specifiers. For example, "jj/MM/AAAA" for French. The syntax is limited to generic specifiers such as "DD/MM/YYYY". However, many international short date-time patterns can be constructed from these generic specifiers (for example, "YYYY.MM.DD" would supply a common Japanese short date format).
- For outbound plain-text email notifications, the NX_SMTP_HEADER_CHARSET and NX_SMTP_BODY_CHARSET options may have to be adjusted in the NX.env file. Adjusting the options helps tag the email message with the character encoding used by the international operating environment correctly. The default values for these options are set to UTF-8 on all platforms.
- International users may want to adjust the DateFormat property in web.cfg to use the date and date-time formats.
- International users may want to change from the default spell check lexicon to a lexicon matching their regional language. Use the LEX_LANG option in the Options Manager.
- Short File Names -- If you have disabled short file names on your Windows operating system, enable them before attempting to install CA SDM. In addition to enabling short files names, you set both the TEMP and TMP environment variables to a short file name. For example, c:\temp, after enabling short file names before starting the installation process. For more information, see the Microsoft Knowledge Base Article 121007 on the Microsoft Help and Support web site.
- Web Interface and Internet Information Services (IIS)--To configure the web interface with IIS 7.0 on Windows 2008, install the CGI and Metabase Compatibility components of IIS 7.0. Add these components using the Roles section of the Server Manager, after installing the IIS Management Compatibility modules.
- Localized releases of CA SDM are supported only on the matching localized Windows server operating environment. In all cases, configure the "Language for non-Unicode programs" for your computer accurately to support the target certified language. This setting is available in the

Regional and Language Options window in the Control Panel. For more information about the localized releases of Windows Server operating systems, see the Microsoft Global Development and Computing Portal.

- Knowledge searches containing multi-byte Japanese characters works properly with SQL Server only when SQL Server is installed with Windows collation. Make sure to specify the Collation option for your data during the SQL Server installation.

Special Characters and Spaces (Directory, Media Path, and Folder Name)

- (UNIX, Linux, and Windows) Do not specify spaces in the installation media path and folder name. If you do, the installation does not work.

Tomcat

- Tomcat is set as the default CA SDM web server during the product installation. If you want to use IIS as the default web server, run the configuration and select IIS. Or, re-run the configuration and select IIS.
- If Tomcat is configured with the external authentication on the primary server, set up a secondary server with a webengine and repository daemon. This setup allows users that are not authenticated to use attachments. The Tomcat installation on the secondary server cannot use external authentication.
- The CA SDM installation sets the Tomcat port to 8080. Other CA products, such as CA Asset Portfolio Management or the Service Delivery Suite of products, also default the Tomcat port to 8080. If you are installing multiple CA products on the same server, select a port number other than 8080 for subsequent CA product installations. Selecting a different port number helps the products function properly together. To change the Tomcat port number to something other than 8080 for CA SDM, install the product. If the product is already installed, re-run the product configuration and specify an available port number for Tomcat when prompted.
- After a restart, the CA SDM Tomcat process may not start properly. To start Tomcat properly, stop and restart Tomcat using the following commands:
- - pdm_tomcat_nxd - c STOP
- - pdm_tomcat_nxd - c START

Users and Authentication

- User authentication does not work if the system is using shadow files and there is an x in the password field of the /etc/passwd file.
- On HP-UX, if you have configured security to store the system passwords in /etc/shadow (for example, anx is stored in /etc/passwd in place of passwords), CA SDM user authentication fails. Users cannot log in to CA SDM.
- The password that is specified for the privileged user must conform to the password policy imposed by the network domain. If the password does not meet the policy, CA SDM configuration does not work.

Web Screen Painter
When you install Web Screen Painter as part of the CA SDM installation, you must configure it to work properly.

copy_inactive Web Option

Fresh CA SDM Release 14.1 installation does not install the copy_inactive web option in Options Manager. So the links to inactive objects are not copied. If you are upgrading from CA SDM r12.5 or r12.6, links to inactive objects are copied because migration installs the option.

Consider the following information when you do not install the copy_inactive option:

- CA SDM does not copy SRELs that point to inactive objects, unless SREL is required.
  For example, the Organization org1 has an inactive Location. When you copy org1, the new organization does not have a location. However, if SREL is required, CA SDM ignores this rule and copies the location. For example, CA SDM ignores the rule and you can copy a CI with an inactive class.

- CA SDM does not copy LREL (many-to-many) relationships to inactive objects.
  For example, the CI named CITest1 has a relationship to the inactive Organization org2. When you copy CITest1, org2 does not link to the new CI.

Important! These rules also apply when you copy a ticket, even if you create a ticket from a template. Whether you installed copy_inactive, the exception to the rule is for Inactive Areas and Categories, which are not copied from existing tickets or populated from templates.

Support Automation Planning Considerations

You can use the following information to research and gather information to help you plan for a successful Support Automation configuration.

- **Server and Network** -- Consider the following supported Support Automation server modes:
  - **Main Server** -- Support Automation uses main application server. The server provides socket-based and HTTP-based communications.
  - **Socket Proxy Server** -- Support Automation uses a socket proxy on the same tier as the web server. The web server off-loads encryption/decryption processing from the main server for direct socket connections to support scalability.
  - **Message Routing Server (MRS)** -- Support Automation separates high bandwidth and unpredictable traffic from the main application server. The separation supports server scalability and provides a network routing shortcut for geographical scalability using remote control connections.
- **Server Sizing** -- Consider the following server variables:

- **Network characteristics of end-user and analyst connections** -- The server load is directly proportional to the data of the message routing component. Low bandwidth, high latency, and high packet loss contribute significantly to lowering the load on the server. When network conditions are optimal (high bandwidth, low latency, low packet loss), the speed on the server is much higher. The total number of concurrent analyst users and end-user logins per minute, including self-service user, can place a heavy load on the server.

- **Connection type** -- The number of socket connections as opposed to the number of HTTP connections affects the servers as follows:

  - When you connect predominantly through socket connections, the load on the servers is very light. If we assume powerful hardware, the application is network bound rather than CPU bound. The hardware does not limit the number of concurrent connections but rather the network can limit the connections.

  - When you connect through HTTP, the load on the web and application servers is higher and the application is CPU bound unless scaled significantly.

- **Remote Control usage** -- Remote Control uses significant network bandwidth in a sustained way whenever it is running. All traffic that is routed between end users and analysts flows through the server. The number of concurrent Remote Control connections has a significant role in any sizing assessments.

  Note: Remote Control is the only high-bandwidth tool in the Live Assistance toolset. Chat and Automation are low bandwidth. Screenshot and File Transfer can use high bandwidth for short periods while files are transferred.

Support Automation Network and Bandwidth Considerations

The amount of bandwidth you consume on the end-user computer depends on the tools you use as follows:

- For the Chat and Automation features, the amount of bandwidth that is required is small. A dial-up modem of 56 kbps or less is adequate to support these functions.

- For the Remote Control feature, the amount of bandwidth required increases. However, Live Assistance Remote Control automatically adapts to low-bandwidth environments by reducing the image quality and refresh rate of the remote control session.

The amount of bandwidth also depends on the connection model you employ. Two connection models are available:

- HTTP connectivity -- Use HTTP when the end user is behind a restrictive firewall and the firewall lets only HTTP connections to the server.

- SSL direct socket -- Use SSL direct socket when the end user connects to the server using a connection on the SSL port 443.

The following chart illustrates the necessary bandwidth depending on the tools you use.

Tools/Bandwidth	Chat/Automation	Remote Control
< 3 KBps (28.8 kbps dial-up)	Very fast and responsive	Slow
< 5 KBps (< 56 kbps dial-up)	Very fast and responsive	Adequate with image degradation
< 50 KBps (Cable/ADSL)	Very fast and responsive	Very fast and responsive
< 100 KBps (LAN)	Very fast and responsive	Very fast and responsive

Considerations for Advanced Availability Configuration

We recommend you to consider the following points before you decide to implement the advanced availability configuration:

General

All the planning considerations of the conventional configuration are valid for the advanced availability configuration. For more information, see How to Convert from Advanced Availability to Conventional Configuration (see page 514) and Step 1- Plan your CA SDM Installation (see page 450)

- Additional hardware costs are expected as you require one background, at least one standby, and one or more application servers. The configuration of standby and background server must be identical.
- You require a remote database server and a server to share knowledge Management index files and import/export files, archive purge output files, and attachment repositories. To allow the background and the standby server to access these files, a shared location is required. Linux and Unix installations can use NFS mounts. UNC support has been added for Windows installations.
- The CA SDM performance is expected to remain the same even with the additional servers for background and standby operations. If you deploy more application servers, the performance can possibly improve.
- Each of the servers is directly connected to the database, leading to an increased resource contention at the DBMS level. We recommend increasing the hardware configuration of the DBMS server. For more information, check the system information.
- Converting a conventional configuration to an advanced availability configuration is a manual effort. The larger implementations are usually more complex and you may have to engage CA Services for the assistance.
- To migrate to the advanced availability configuration, upgrade to CA SDM Release 12.9 in the conventional configuration and then convert to the advanced availability configuration.
- Install the background and the standby server on the same network subnet to make ping times and latencies from different application servers similar.
- Consider locating the background and the standby servers in a central location with a good network connectivity to all your users. The application servers can be located either centrally or they can be distributed across the globe.

- An advanced availability configuration must always have one background server and at least one standby server.
  (Recommended) Ensure that both background server and all other standby servers have similar configuration. This process ensures that during a failover when a standby server becomes the new background server, it can function exactly like the old background server.

Any number of standby servers can be configured. To increase the CA SDM availability, consider placing one standby server in your backup data center or the disaster recover site.

- The minimum advanced availability implementation requires one application server. We recommend you to have two application servers to increase the availability and a load balancer to direct web traffic.

- Except for CA SDM administrators, no other users are allowed to log in to the background server. Also, no users are allowed to log in to the standby servers.

We can send email notifications from all CA SDM servers. There is no way to limit or configure this option. Every server in the advanced availability configuration must have a connection to the mail server.

- An email notification resulting from an end-user interaction is sent from the application server to which the user is connected.

- An email notification resulting from a background process is sent by the pdm_mail_nxd utility running on the background server. Animator processing an Attached Event is an example of a background process.

- During a background server failure, the queued emails are sent when the background server comes up as a standby server.

Failover

During a failover of the background server to the standby server, consider the following points:

- The new users cannot log in.

- For the users that are already connected, some actions do not work during the failover. The users must try the actions after the failover. The following actions do not work:

  - Creating the tickets with attachments

  - Downloading the attachments

  - Searching Knowledge documents

  - Indexing the new knowledge documents

  - Inbound email

  - The SLA events that are not triggered until the failover has completed

Important! If you have configured your third-party tool to enable the auto-failover of the CA SDM servers, you must disable it before starting the rolling maintenance.

Database

- A direct connection exists from each of the servers to the other as well as to the database. If the CA SDM server is within DMZ, open the firewall ports or implement a tunneling proxy technology for this connectivity. Also consider licensing arrangements with your DBMS vendor.
- Ensure that you install the database client on all the CA SDM servers.
- In advanced availability configuration, all the servers still connect to a single database. As the database can be a single point of failure, consider taking the advantages of database clustering to increase the availability of DBMS.
- Microsoft SQL Server is only natively supported on the Windows platform. For example, suppose that your implementation consists of servers with heterogeneous operating systems such as Windows and Linux. Select Oracle as the DBMS as Microsoft SQL Server is not supported on Linux.
- The pdm_isql utility works only on the application server.

System Configuration, Administration, and Operation

- SOAP Web Services and RESTful Web Services are only supported on the application servers. Web directors can be configured on all CA SDM servers.
- As the application servers are independent of each other, web directors can only service web engines running on the same application server. Web directors cannot service web engines across application servers.
- Since the servers in the advanced availability configuration have a higher degree of independence, most command-line utilities function only on the local server. For example, pdm_status only shows you the CA SDM processes running on the server on which you are executing the command. The pdm_webcache utility only refreshes the form caches on the server on which it was issued.
- In advanced availability, processes on each server are controlled independently. This is unlike conventional configuration, where you run pdm_d_mgr on the primary server to start and stop CA SDM processes.
- We recommend you to use the new pdm_server_control instead of pdm_halt command to shutdown application servers. Before the shutdown, you can ask the active users to move to another application server. You can notify the users using the quiesce option.
- The pdm_edit utility has been replaced with a new graphical user interface, eliminating many manual configuration file changes required earlier.

- Unlike conventional, in the advanced availability configuration, you can use the bopauth_host option to specify the authentication server details. The option is available in the Options Manager of the background server Web interface. You no longer make this configuration change in pdm_edit for the advanced availability configuration. Users cannot log in when the authentication server is unavailable.

  Note: In the conventional configuration, you can use a secondary server to integrate CA SDM with an authentication system running on a different system or even on a different hardware platform.

- To prevent rogue servers from joining the advanced availability configuration, define all servers from the background server Web interface, before you configure them.

- The role and other information for a server in the advanced availability configuration can be changed from the **Administration** tab. Stop the CA SDM services before attempting to change a server definition. The server reconfiguration is required for the changes to take effect.

- You can change a server between the conventional configuration and the advanced availability configuration by running the configuration utility. Be sure to change all servers in the implementation. Your data remains unaffected, but the manual updates are required to change the settings.

- Use the latest pdm_startup files while migrating to CA SDM Release 12.9. Do not use the files from previous versions of CA SDM. For example, files that are generated by the pdm_edit utility.

- New environment variables have been added to NX.env to support the advanced availability and the system automatically maintains the variable values.

  Important! Do not change NX.env manually unless instructed to do so.

- A new facility generates ticket numbers and numeric record keys. To avoid possible database corruption, never try to load or manually alter the Key_Control table.

- You cannot move the Knowledge Management daemons to another server in the advanced availability configuration. The kt_daemon now runs on all servers. All other Knowledge Management daemons run as singletons on the background server.

- Knowledge Management now support UNC file paths on Windows for the EBR index files and input/output files locations. These files are used by the Knowledge Export Import facility. This feature is available for both the advanced availability and the conventional configurations.

  Important! EBR Index Files path & **KEIT Files path** must refer to the same UNC credentials and the path must reside on a same server to support this.

- Version control distributes the files (for example, htmpl, .maj, .mod, and .sch) that are configured in the server_secondary_custom.ver file from the background server. Upon startup, the standby or the application server runs the version control client to pull updated files from the background server.

- Archive/Purge runs on the background server and supports UNC file paths on Windows for output files. This feature is available in the advanced availability and the conventional configurations.

- Attachments on incoming emails are now stored by pdm_maileater when the repository is on a remote server.

- Ensure that you allow the daemon manager to modify the procsets and do not run the pdm_dmnmode command for this action.

General Web User Interface

- A web server is required on all the servers of the advanced availability configuration.

- When the background server is not available due to failover, a Delayed Server Response form is presented to the web users. Users are allowed to resume their work when the standby server is promoted to the background server.

- The value of the web_cgi_url option must point to:

  - The load balancer if you have more than one application servers.

  - The application server, if you have only one application server.

Attachment

- You can increase the availability of attachments by configuring multiple document repository processes to access a shared file repository.

Web Screen Painter

- You can use the Web Screen Painter (WSP) only on the background server.

- Follow the recommended procedure to publish WSP form changes so that the updated forms are distributed to all the servers in the installation. For more information, see the *How to Modify Schema Using Web Screen Painter* and *How to Modify Web Interface using Web Screen Painter* scenarios.

- The virtual database layer daemons run on all servers. Install the CA SDM database modifications and object definitions on all the servers.

Reporting

- CA Business Intelligence can automatically retrieve data from alternate application servers. You can configure this feature to increase the availability of CA SDM reporting.

- BOXI is not integrated with the background server. For this reason, you cannot view reports from the background server web UI. An error message is displayed if you select the Reports tab from the background server web UI.

- (If you have CA Business Intelligence Release 3.3) Install CA Business Intelligence Release 4.1 SP3 (see page 285) and then install CA SDM.

- For CA Business Intelligence ODBC services to start properly, export the library path, as follows:

  - (For AIX) Export LIBPATH=$LIBPATH:<CA_SharedComponent>/lib:<NX_ROOT>/lib
    Example: Export LIBPATH=$LIBPATH:/opt/CA/SC/lib:/opt/CAisd/lib

  - (For Solaris/Linux) Export LD_LIBRARARY_PATH=$ LD_LIBRARARY_PATH:/opt/CA/SC/lib:<NX_ROOT>/lib
    Example: Export LD_LIBRARARY_PATH=$ LD_LIBRARARY_PATH:/opt/CA/SC/lib:/opt/CAisd/lib

Options Manager

You can install or uninstall options through Options Manager only from the background server web UI. After you install or uninstall the options, restart the CA SDM servers.

Web Services

- You can configure web services only on the application servers.

- The webservices_domsrvr option no longer exists in the Options Manager. You can configure NX_WEBSERVICES_DOMSRVR variable independently on each application server by modifying NX.env.

Integration

- The URL to the CA SDM web user interface must point to a properly configured application server. The ca_application_registration contains a URL to your CA SDM installation that other CA products use. This URL points to the CA SDM server that is configured first, which is most commonly the background server. Only the CA SDM administrators can change the value through the administration facility. If you are using a load balancer, point this URL to the load balancer instead of a single application server. For more information, see the *Online Help*.

- Most end-users interaction and integrations with other software products are done at the application server level. There is no failover for the application servers. If the application server is unavailable, the web services for the application server are also unavailable. To increase the application server availability, you can deploy a load balancer to route requests among different application servers.

- You can integrate NSM only to a single application server as the IP addresses are involved. The NSM integration is unavailable when that server is down.

- CA SDM and Unified Self-Service Integration:

  - Ensure that you install both the products on different machines.

- Before you install Unified Self-Service, download Liferay CE 6.1.2 GA3 edition zip file (https://www.liferay.com/downloads/liferay-portal/available-releases).

Note: Do not Install Liferay Manually as the installer unzips the downloaded file and installs Liferay.

Conversion

- You can convert the background server to a primary server only.
- You can convert the primary server to a background server only.
- You can convert the secondary server to a standby server or application server only.
- You can convert the standby or an application server to the secondary server only.

CA SDM Connector Considerations

For CA SDM connector to function for CA SDM installed in supported locales, you must apply RO72246 (Language Independent) and RO72249 (Language Combo) patches on CA SDM 12.9. Then apply the following patches.

Language	Patch
German	T52Y442
Simplified Chinese	T52Y443
Japanese	T52Y444
English	T52Y445
French	T52Y446
French Canadian	T52Y447
Spanish	T52Y448
Italian	T52Y449
Brazilian Portuguese	T52Y450

Step 2- Install CA SDM

You can use the CA Service Management Installer (see page 293) to install or upgrade CA SDM in conventional (see page 480)or in advanced availability (see page 487) configuration. When you install CA SDM on a server, the following files, components, and features are installed:

- Server functionality, which is based on how you configure the product after installation.
- The ODBC Interface

Important! The ODBC interface is installed solely for use to access the ODBC driver for Business Objects reporting in CA SDM with CA Business Intelligence. Use of the ODBC driver by other applications is not directly supported, certified, or warranted by CA Technologies. You use it at your own risk.

- CA MDB - If CA SDM is installed on the primary server, CA MDB is installed automatically during the installation.
- The Web Interface
- Visualizer
- Support Automation

Note: For optimal performance, consider setting up Unified Self-Service in a clustered environment (see page 619).

Install CA SDM Using Conventional Configuration

You can install CA SDM using the conventional configuration.

For UNIX/ Linuix, mount the installation media on your drive and navigate to the root directory of the installation media and start the installation by running the following command:

```
sh ./setup.sh
```

Also, consider the following points:

- When installing on Linux and UNIX, you may not be able to view some pop-up messages clearly, for color properties white on white.
- Suppose that Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) hosts coexist on the network. Verify that the appropriate transition strategies, tools, and mechanisms to support these technologies are in place before you start the product configuration.
- If you start, and then stop the installation on UNIX or Linux, you may see a directory at the root of the installation named install.dir.#####. This is a feature of InstallAnywhere. These files are not needed and you can safely delete them.
- Create the **CA Service Desk Manager Server Privileged** user before you begin the installation.

Follow these steps:

1. Ensure that you completed the following steps from the CA Service Management Installer (see page 293):
    a. Selected a language and **CA Service Management** from the **Select the required installer** screen

b. Accepted the license agreement.

c. Entered the database information correctly.

> **Note:** For Linux/ UNIX, only information related to Oracle database is required.

d. Select **CA Service Desk Manager** from the **Select the Products and Integrations** screen. If you want to integrate Unified Self-Service with CA SDM, keep the check box for Unified Self-Service selected.

> **Important!** While integrating these products, use the Unified Self-Service User ID and Email Address in CA SDM.

e. Review the Installation Prerequisites report and take corrective measures to proceed with the installation.

2. If you are installing for the first time, you need to enter the common Administrator credentials for CA Service Management in the **CA Service Management Administrator details** screen.

3. Navigate to **CA Service Desk Manager Product Configuration** screen.

   a. Select the **Conventional** radio button.

   b. Select **Primary Server** from the **Select Server Type** drop down.

   c. Select the other components that you want to install on this server. For example, Federated Search.

   d. If you have already created server process configuration, then select the configuration or else keep the **Default** option selected.

   e. Click **Browse** to select the installation directory and click **Next**. The following screenshot corresponds to the installation on Windows.

4. Enter the following information in the **CA Service Desk Manager Server Details** screen:

> **Note:** Enter the primary server host name in the **Primary Server Node** field (defaulted to the localhost name).

Image 9_1.JPG

5. On the **CA Service Desk Manager Server Privileged User Details** screen, select the **Load Default Data** check box to load on the predefined date and enter the privileged user details.

6. On the **CA Service Desk Manager Optional Component Details** screen, enter the port numbers to install the components that you have chosen.

Image 11.JPG

7. If you have selected to integrate CA SDM with Support Automation, enter the following information:

   - **Main Server:** Configures the Support Automation server in main server (standalone) mode. If you select the **Main Server Configuration Type**, the **Host Name** or **IP** field defaults to the local Host Name. All parameters must be provided for the **Main Server** except the **Internal Port** section and the **Bind to IP** in **Socket Server** section, which are optional. Configure the main server on the following CA SDM server according to the CA SDM configuration type:

   -
     - Conventional: Primary server or secondary server.
     - Advanced availability: Background server.

Important! When you set the **supportautomation_url** *option*, this URL must use the URL of the Support Automation main server. It should not reference the proxy server or load balancer server. This is applicable only for conventional model. In the advanced availability configuration the URL can point to load balancer, main server, or proxy server.

Note: If you select the **Main Server** option, and are also planning to configure one or more socket proxy servers, you *must* set the **Socket Server host name** and **external port** to the socket proxy host and external port. For multiple socket proxies, you set the **Socket Server to the host** and **external port** of the load balancer server.

   - **Tomcat Port:** Specifies the Support Automation Tomcat port.
   - **Tomcat Shutdown Port:** Specifies the Support Automation Tomcat Shutdown port.

Note: When you change the main server Tomcat port, also change the port references in the server.properties file with tomcat server.xml.

- **Host Name or IP**: Specifies the address of your server.
- **External Port** : Specifies the external port of your server.
- **Host Name or IP**—Specifies the address of your socket server.
- **External Port** —Specifies the external port of your socket server.
- **Internal Port**—Specifies the internal port of your socket server.
- **Bind to IP**—Specifies the IP where you want to bind the server.
- **Socket Proxy Server:** Configures the Support Automation server in socket proxy mode. Use a Socket Proxy Server to off-load some of the CPU-intensive operations of Support Automation, such as encryption/decryption from the main server.
-
  - Advanced Availability: Application server.
  - Conventional: Secondary server.
- **Main Server Host Name or IP**: Specifies the address of the main server.
- **Main Server Internal Port**: Specifies the internal port of the main server.
- **Main Server HTTP Port**: Specifies the HTTP port of the main server. This field is available only for conventional configuration.
- **External Port**: Specifies the external port of the server.
- **Bind to IP**: Specifies the IP where you want to bind the server.
- **Message Routing Server:** Configures the Support Automation server in message routing server mode. Use Message Routing Servers (MRS) to manage multiple Remote Control sessions that are based on the geographical location of the local server. Using MRS helps improve performance during assistance sessions.
  - Advanced Availability:Application server.
  - Conventional: Secondary server.
- **External Port**—Specifies the external port of the socket.
- **Bind to IP**—Specifies the IP where you want to bind the server.

CA SDM installs and configures the following Support Automation components:

- End-User Client

- Support Automation Analyst Interface
- Server

You install and configure the following components separately:

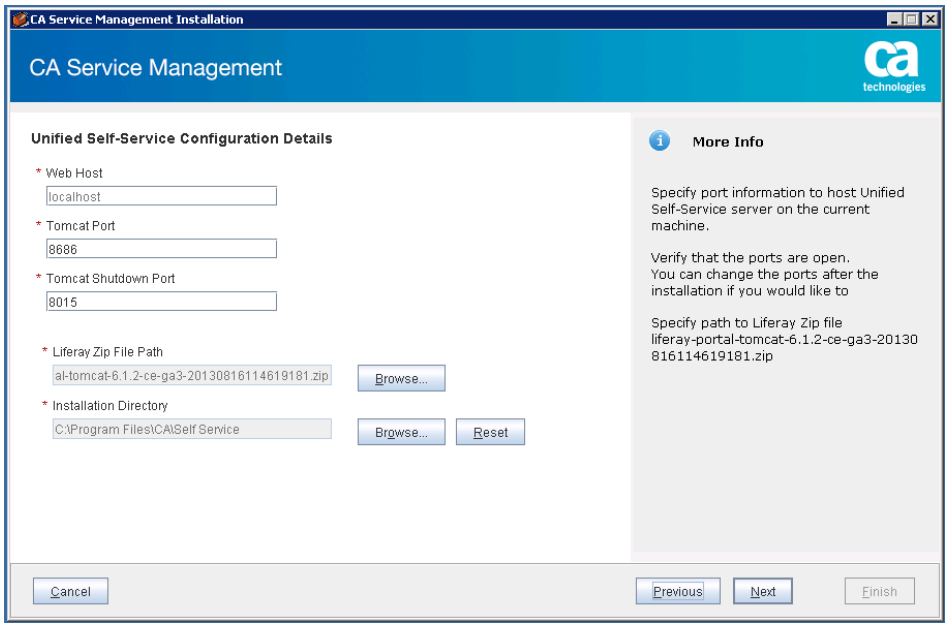
- End-User Agent
- Automated Tasks Editor IDE

8. If you have selected to integrate CA SDM with Unified Self-Service, complete the following steps:

> **Note:** For optimal performance, consider setting up Unified Self-Service in a clustered environment (see page 619).

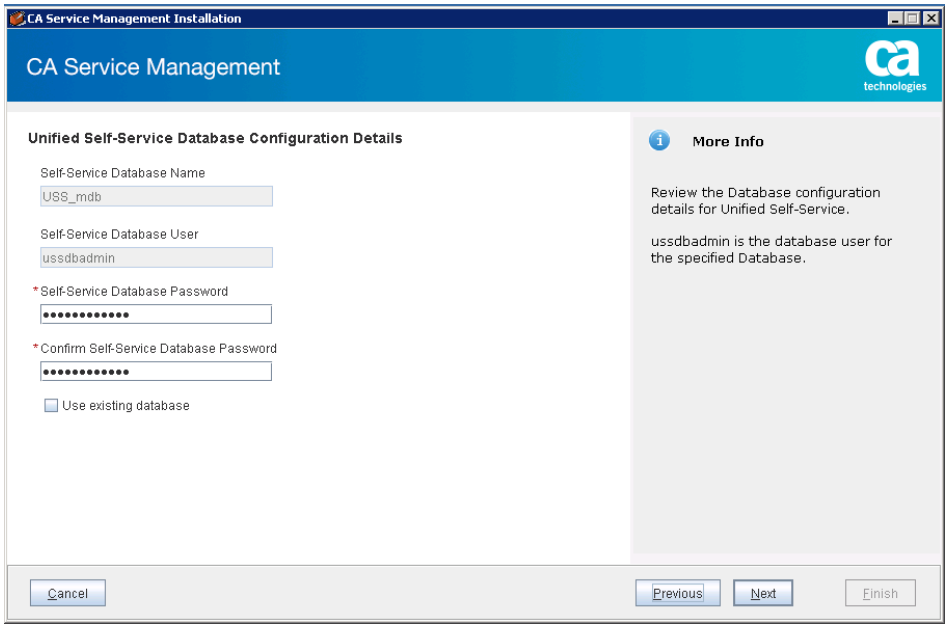
a. Enter the configuration details in the **Unified Self-Service Configuration Details** screen. Enter the Web Host as the host name of the machine where you are installing Unified Self Service.

> **Note:** Before you install Unified Self-Service, download Liferay CE 6.1.2 GA3 edition zip file (https://www.liferay.com/downloads/liferay-portal/available-releases). Do not Install Liferay manually as the installer unzips the downloaded file and installs Liferay.



Unified Self-Service Configuration Details

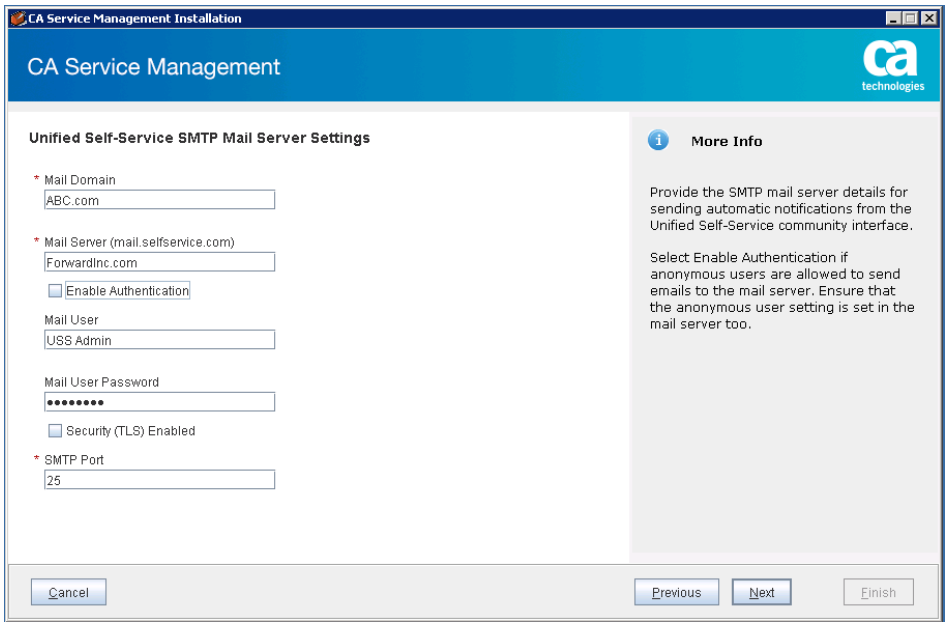
b. Enter the database information in the **Unified Self-Service Database Configuration Details** screen. If you have already set up a database, select the Use existing database check box and select the backup file. The database for Unified Self-Service is created during this installation.



Unified Self-Service Database Configuration Details

c. Enter the SMTP mail server details to send automatic notifications from the Unified Self-Service community interface in the **Unified Self-Service SMTP Mail Server Settings** screen:

- **Mail User**
  Defines the name of the mail user using which you want to send automatic notifications.
- **Mail User Password**
  Defines the password of the mail user.
- **Security (TLS) enabled**
  Specifies whether the TLS security is enabled or not for the mail server.



Unified Self-Service SMTP Mail Server Settings

You have entered all the Unified Self-Service information.

Important! For integration between Unified Self-Service and CA Service Desk Manager to work appropriately, ensure the Unified Self-Service users that are available in CA Service Desk Manager have the same User ID and email address.

9. Review the Pre-Installation Configuration Summary Report.
10. Review the Installation progress information and click **Install** to install the selected product /products.
11. Review the Installation Guidance Report summary to ensure that the installation succeeded.
12. After installing CA SDM on the primary server, create the server process configuration for the secondary server.
13. Log in to the secondary server and start the CA Service Management installation. You can either skip the database configuration to come to the **CA Service Desk Manager Product Configuration** screen directly or enter the database information (if different from the primary server) and proceed with the installation.

Image 7_1.JPG

14. After you install CA SDM (or migrate to CA SDM from a CMDB standalone system), run the *cmdb_update_ambiguity* utility. Use the -h command to view the mandatory options.

Note: If configuration fails during the Validate Extension Tables step, database connectivity can be an issue. Retry the installation and verify that you provided the correct database connectivity information.

Install CA SDM Using Advanced Availability Configuration

You can install CA SDM using the advanced availability configuration.

For UNIX/ Linuix, mount the installation media on your drive and navigate to the root directory of the installation media and start the installation by running the following command:

```
sh ./setup.sh
```

Also, consider the following points:

- When installing on Linux and UNIX, you may not be able to view some pop-up messages clearly, for color properties white on white.
- Suppose that Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) hosts coexist on the network. Verify that the appropriate transition strategies, tools, and mechanisms to support these technologies are in place before you start the product configuration.
- If you start, and then stop the installation on UNIX or Linux, you may see a directory at the root of the installation named install.dir.#####. This is a feature of InstallAnywhere. These files are not needed and you can safely delete them.
- Create the **CA Service Desk Manager Server Privileged** user before you begin the installation.

Follow these steps:

1. Ensure that you completed the following steps from the CA Service Management Installer (see page 296):
    a. Selected a language and **CA Service Management** from the **Select the required installer** screen
    b. Accepted the license agreement.
    c. Entered the database information correctly.

Note: For Linux/ UNIX, only information related to Oracle database is required.

    d. Selected **CA Service Desk Manager** from the **Select the Products and Integrations** screen. If you want to integrate Unified Self-Service with CA SDM, keep the check box for Unified Self-Service selected.

> **Important!** While integrating these products, use the Unified Self-Service User ID and Email Address in CA SDM.

e. Review the Installation Prerequisites report and take corrective measures to proceed with the installation.

2. If you are installing for the first time, you need to enter the common Administrator credentials for CA Service Management in the **CA Service Management Administrator details** screen.

3. Navigate to **CA Service Desk Manager Product Configuration** screen.

   a. Select the **Advanced Availability** radio button. The background server option is selected by default.

   b. Keep the **Default** option selected.

   c. Click **Browse** to select the installation directory and click **Next**. The following screenshot corresponds to the installation on Windows.

4. Enter the following information in the **CA Service Desk Manager Server Details** screen:

Image 9_1_AA.JPG

5. On the **CA Service Desk Manager Server Privileged User Details** screen, select the **Load Default Data** check box to load on the predefined data and enter the privileged user details.

6. On the **CA Service Desk Manager Additional Server Details** screen, enter the following information of the servers that you want to add:

Image 11_AA.JPG

7. If you have selected to integrate CA SDM with Support Automation, enter the following information:

   - **Main Server:** Configures the Support Automation server in main server (standalone) mode. If you select the **Main Server Configuration Type**, the **Host Name** or **IP** field defaults to the local Host Name. All parameters must be provided for the **Main Server** except the **Internal Port** section and the **Bind to IP** in **Socket Server** section, which are optional. Configure the main server on the following CA SDM server according to the CA SDM configuration type:

     - Conventional: Primary server or secondary server.

- Advanced availability: Background server.

Important! When you set the ***supportautomation_url*** *option*, this URL must use the URL of the Support Automation main server. It should not reference the proxy server or load balancer server. This is applicable only for conventional model. In the advanced availability configuration the URL can point to load balancer, main server, or proxy server.

Note: If you select the **Main Server** option, and are also planning to configure one or more socket proxy servers, you *must* set the **Socket Server host name** and **external port** to the socket proxy host and external port. For multiple socket proxies, you set the **Socket Server to the host** and **external port** of the load balancer server.

- **Tomcat Port:** Specifies the Support Automation Tomcat port.
- **Tomcat Shutdown Port:** Specifies the Support Automation Tomcat Shutdown port.

Note: When you change the main server Tomcat port, also change the port references in the server.properties file with tomcat server.xml.

- **Host Name or IP**: Specifies the address of your server.
- **External Port** : Specifies the external port of your server.
- **Host Name or IP**—Specifies the address of your socket server.
- **External Port** —Specifies the external port of your socket server.
- **Internal Port**—Specifies the internal port of your socket server.
- **Bind to IP**—Specifies the IP where you want to bind the server.
- **Socket Proxy Server:** Configures the Support Automation server in socket proxy mode. Use a Socket Proxy Server to off-load some of the CPU-intensive operations of Support Automation, such as encryption/decryption from the main server.
-
  - Advanced Availability: Application server.
  - Conventional: Secondary server.
- **Main Server Host Name or IP**: Specifies the address of the main server.

- **Main Server Internal Port**: Specifies the internal port of the main server.
- **Main Server HTTP Port**: Specifies the HTTP port of the main server. This field is available only for conventional configuration.
- **External Port**: Specifies the external port of the server.
- **Bind to IP**: Specifies the IP where you want to bind the server.
- **Message Routing Server:** Configures the Support Automation server in message routing server mode. Use Message Routing Servers (MRS) to manage multiple Remote Control sessions that are based on the geographical location of the local server. Using MRS helps improve performance during assistance sessions.
  - Advanced Availability:Application server.
  - Conventional: Secondary server.
- **External Port**—Specifies the external port of the socket.
- **Bind to IP**—Specifies the IP where you want to bind the server.

CA SDM installs and configures the following Support Automation components:

- End-User Client
- Support Automation Analyst Interface
- Server

You install and configure the following components separately:

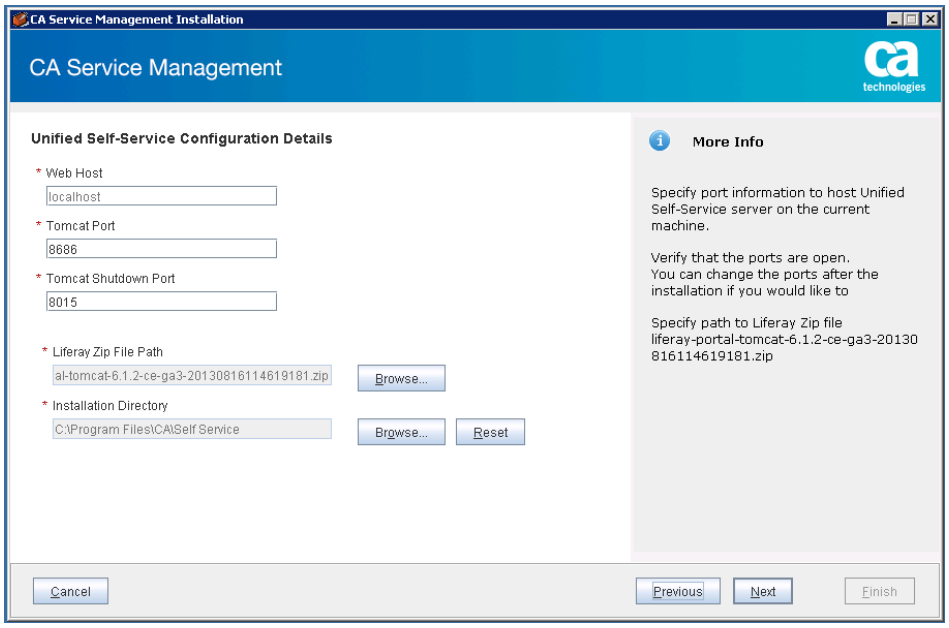
- End-User Agent
- Automated Tasks Editor IDE

8. If you have selected to integrate CA SDM with Unified Self-Service, complete the following steps:

   Note: For optimal performance, consider Setting up Unified Self-Service in a clustered environment (see page 619).

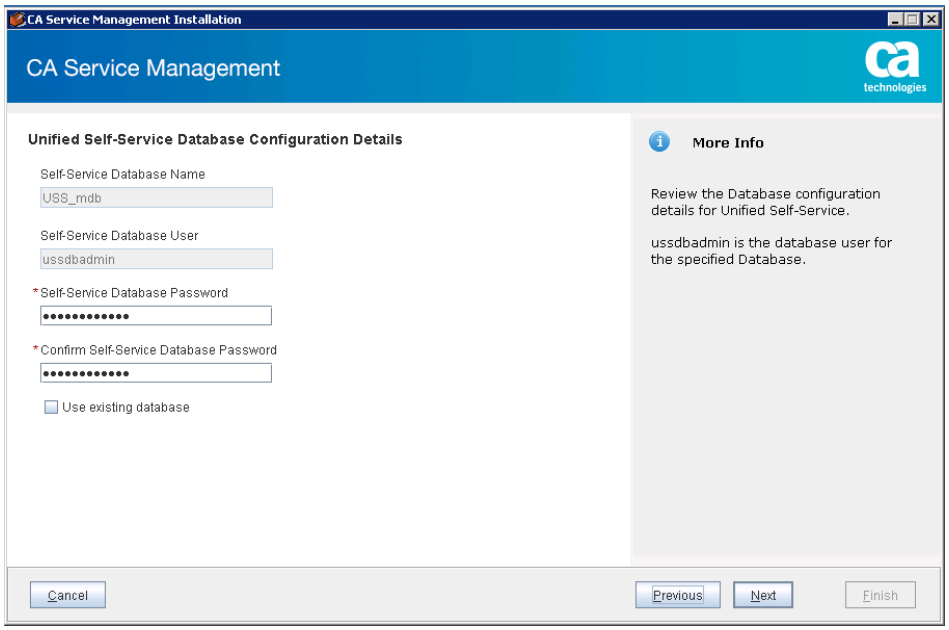
   a. Enter the configuration details in the **Unified Self-Service Configuration Details** screen. Enter the Web Host as the host name of the machine where you are installing Unified Self Service.

Note: Before you install Unified Self-Service, download Liferay CE 6.1.2 GA3 edition zip file (https://www.liferay.com/downloads/liferay-portal/available-releases). Do not Install Liferay manually as the installer unzips the downloaded file and installs Liferay.



Unified Self-Service Configuration Details

b. Enter the database information in the **Unified Self-Service Database Configuration Details** screen. If you have already set up a database, select the Use existing database check box and select the backup file. The database for Unified Self-Service is created during this installation.



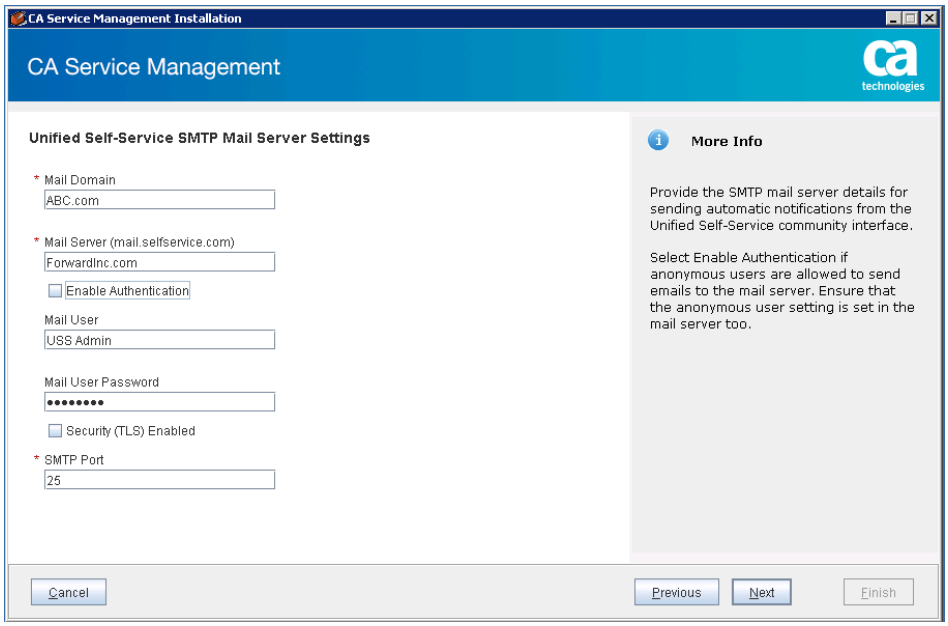
Unified Self-Service Database Configuration Details

c. Enter the SMTP mail server details to send automatic notifications from the Unified Self-Service community interface in the **Unified Self-Service SMTP Mail Server Settings** screen:

- **Mail User**
  Defines the name of the mail user using which you want to send automatic notifications.

- **Mail User Password**
  Defines the password of the mail user.

- **Security (TLS) enabled**
  Specifies whether the TLS security is enabled or not for the mail server.



Unified Self-Service SMTP Mail Server Settings

You have entered all the Unified Self-Service information.

Important! For integration between Unified Self-Service and CA Service Desk Manager to work appropriately, ensure the Unified Self-Service users that are available in CA Service Desk Manager have the same User ID and email address.

9. Review the PreInstallation Configuration Summary Report.
10. Review the Installation progress information and click **Install** to install the selected product /products.
11. Review the Installation Guidance Report summary to ensure that the installation succeeded.
12. After installing CA SDM on the background server, create the server process configuration for the other servers.
13. Install CA SDM on the other servers. For the application server, on the **CA Service Desk Manager Optional Component Details** screen, enter the port numbers to install the components.

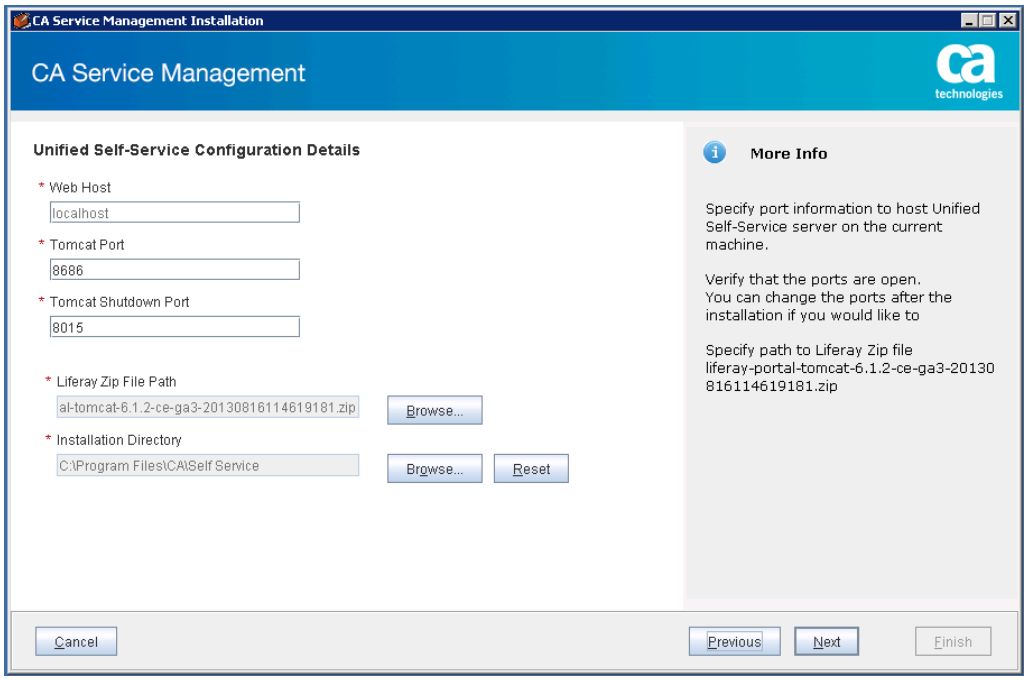
Image 11.JPG

Install Unified Self-Service with CA Service Desk Manager

Note: For optimal performance, consider setting up Unified Self-Service in a clustered environment (see page 619).

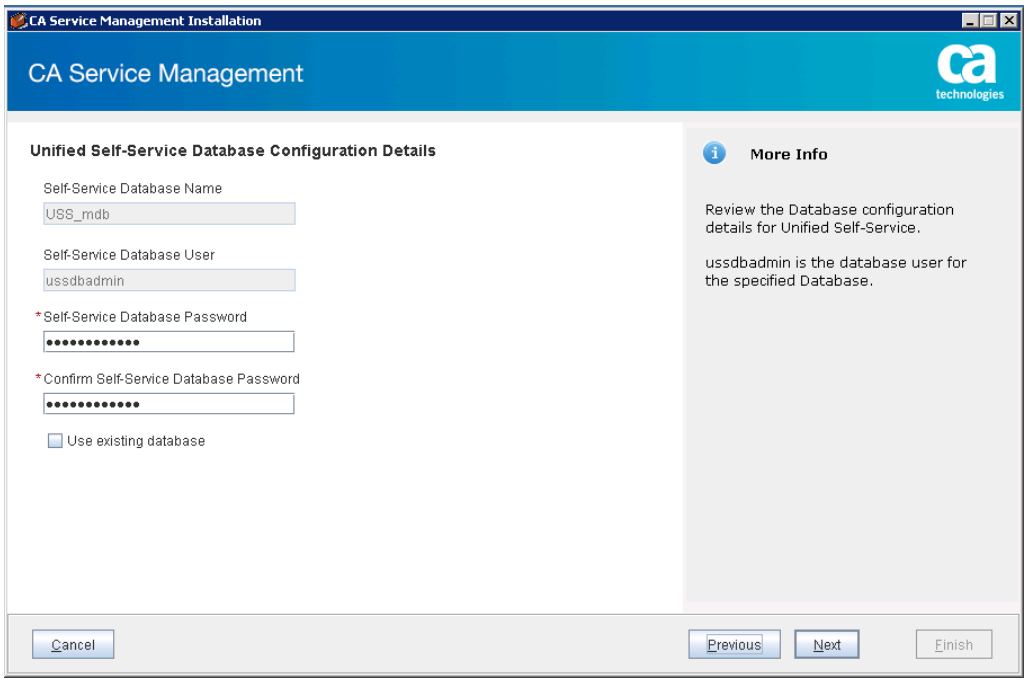
1. Enter the configuration details in the **Unified Self-Service Configuration Details** screen. Enter the Web Host as the host name of the machine where you are installing Unified Self Service.

   Note: Before you install Unified Self-Service, download Liferay CE 6.1.2 GA3 edition zip file (https://www.liferay.com/downloads/liferay-portal/available-releases). Do not Install Liferay manually as the installer unzips the downloaded file and installs Liferay.



Unified Self-Service Configuration Details

2. Enter the database information in the **Unified Self-Service Database Configuration Details** screen. If you have already set up a database, select the Use existing database check box and select the backup file. The database for Unified Self-Service is created during this installation.



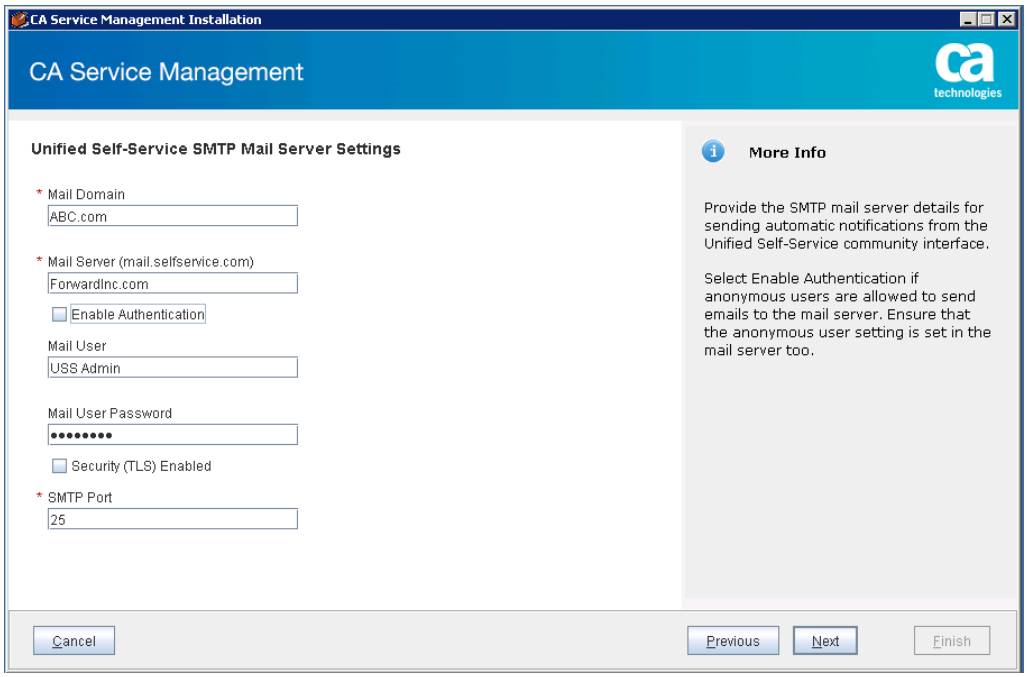
Unified Self-Service Database Configuration Details

3. Enter the SMTP mail server details to send automatic notifications from the Unified Self-Service community interface in the **Unified Self-Service SMTP Mail Server Settings** screen:

   - **Mail User**
     Defines the name of the mail user using which you want to send automatic notifications.

   - **Mail User Password**
     Defines the password of the mail user.

   - **Security (TLS) enabled**
     Specifies whether the TLS security is enabled or not for the mail server.



Unified Self-Service SMTP Mail Server Settings

You have entered all the Unified Self-Service information.

Important! For integration between Unified Self-Service and CA Service Desk Manager to work appropriately, ensure the Unified Self-Service users that are available in CA Service Desk Manager have the same User ID and email address.

Support Automation Configuration Details

Enter the following information:

Main Server: Configures the Support Automation server in main server (standalone) mode.

Tomcat Configuration

Tomcat Port

Specifies the Support Automation Tomcat port. **Default:** 8070

Tomcat Shutdown Port

Specifies the Support Automation Tomcat Shutdown port. **Default:** 8075

Note: When you change the main server Tomcat port, also change the port references in the server.properties file with tomcat server.xml.

HTTP

- **Host Name or IP**—Specifies the address of your server.
- **External Port** —Specifies the external port of your server. **Default:** 8070.

Socket Server

- **Host Name or IP**—Specifies the address of your socket server.
- **External Port** —Specifies the external port of your socket server. **Default:** 10443.
- **Internal Port**—Specifies the internal port of your socket server.
- **Bind to IP**—Specifies the IP where you want to bind the server. **Default:** 7005.

Socket Proxy Server

Configures the Support Automation server in socket proxy mode. Use a Socket Proxy Server to off-load some of the CPU-intensive operations of Support Automation, such as encryption/decryption from the main server.

- - Advanced Availability: This option is available only for the application server.
  - Conventional: This option is available only for the secondary server.

Socket Configuration

Main Server Host Name or IP—Specifies the address of the main server.

Main Server Internal Port—Specifies the internal port of the main server. **Default:** 7005

Main Server HTTP Port—Specifies the HTTP port of the main server. This field is available only for conventional configuration.

External Port—Specifies the external port of the server. **Default:** 10444

Bind to IP—Specifies the IP where you want to bind the server.

Message Routing Server

Configures the Support Automation server in message routing server mode. Use Message Routing Servers (MRS) to manage multiple Remote Control sessions that are based on the geographical location of the local server. Using MRS helps improve performance during assistance sessions.

- - Advanced Availability: This option is available only for the application server.
  - Conventional: This option is available only for the secondary server.

Socket Configuration

External Port—Specifies the external port of the socket. **Default:** 10444

Bind to IP—Specifies the IP where you want to bind the server.

Step 3- Install Other Components

This article includes the following topics:

Install Web Screen Painter

Install Web Screen Painter to modify the schema and web interface.

Follow these steps:

1. Log in to the following server where you want to install Web Screen Painter, depending on your CA SDM configuration:
   - Conventional: Primary or secondary server or any remote computer
   - Advanced availability: Background server

   Important! Web Screen Painter can only run on the background server. The Web Screen Painter installer does not stop you from installing it on any other server. However, it prevents from running standalone, or on the standby server and application server. For example, you installed Web Screen Painter on a server other than background server. The Web Screen Painter shortcuts appear on the Start menu and on clicking the shortcut, an error message is displayed.
2. Launch the installer.
3. Click CA Web Screen Painter for Service Desk Manager in the Select the required installer page.
4. Continue following the on-screen instructions to complete the Web Screen Painter installation.

Web Screen Painter is installed. In a Web Screen Painter preview session in test mode, search filters are ignored on new tables that are not published.

Install and Configure JRE 1.8.0_45

Complete the following steps to install and configure JRE 1.8.0_45 (32-bit) to use with CA SDM release 14.1:

1. Shut down the CA SDM Daemon or CA SDM Proctor Service, or both on the relevant CA SDM server (primary or secondary, or both).
2. Download JRE 1.8.0_45 (jre-8u45-windows-i586 via the Download JRE link) from http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html

3. During the installation, select the Change destination folder option and enter the destination folder as <drive>:\<install_directory>\CA\SC\JRE\1.8.45

4. Take a backup of NX.env, located at <drive>:\<install_directory>\CA\Service Desk\

5. Modify NX.env as follows:

   ```
   @NX_JRE_INSTALL_DIR=C:/Program Files (x86)/Java/jre1.8.0_45
   ```

6. Start Service Desk.

7. Install and configure Apache Tomcat 7.0.59 (see page 498) for Support Automation to work properly.

Install and Configure Apache Tomcat 7.0.59

CA SDM 14.1 provides out-of-the-box Apache Tomcat 7.0.23. Complete the following steps to upgrade to Apache Tomcat 7.0.59:

1. Shut down CA SDM Daemon Service or CA SDM Proctor Service, or both on the relevant CA SDM server (primary or secondary, or both).

2. Download Tomcat 7.0.59 (apache-tomcat-7.0.59.zip) from http://archive.apache.org/dist/tomcat/tomcat-7/v7.0.59/bin/

   Note: CA SDM supports service packs and point releases of Operating Systems, Databases, Web Servers, Web Browsers, Java, Servlets, and so on. This may not be noted in the certification matrix as long as the reported problem is reproducible with versions that are listed in the matrix. CA reserves the right to refuse support of new point releases should the reported problem require a major rework or redesign to function properly. Both Technical Support and Sustaining Engineering does their best to resolve any issues that occur in a timely manner. If the resolution to the problem is determined to be outside the realm of their support responsibilities, they may ask you to escalate your request for certification to your local account team.

3. Unzip apache-tomcat-7.0.59.zip and copy the files at <drive>:\<install_directory>\CA\SC\tomcat\7.0.59

   Note: After unzipping, ensure that <drive>:\<install_directory>\CA\SC\tomcat\7.0.59 contains conf, bin, webapps, and other directories.

   <drive>:\<install_directory>\CA\SC\tomcat\7.0.59 must NOT contain <drive>:\<install_directory>\CA\SC\tomcat\7.0.59\apache-tomcat-7.0.59. Presence of this directory indicates that the unzipping was done incorrectly.

4. Take a backup of the NX.ENV directory, located at the CA SDM install directory (NX_ROOT).

5. Modify NX.ENV as follows:

   ```
   @NX_TOMCAT_INSTALL_DIR=C:\Program Files\CA\SC\tomcat\7.0.59
   ```

6. Backup NX_ROOT\bopcfg\www\CATALINA_BASE\conf and the following directories (whichever exist):

   - $NX_ROOT\bopcfg\www\CATALINA_BASE_SA\conf
   - $NX_ROOT\bopcfg\www\CATALINA_BASE_REST\conf
   - $NX_ROOT\bopcfg\www\CATALINA_BASE_VIZ\conf
   - $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\conf
   - $NX_ROOT\bopcfg\www\CATALINA_BASE_WF\conf

7. Copy all files from **<drive>:\<install_directory>\CA\SC\tomcat\7.0.59\conf** to **NX_ROOT\bopcfg\www\CATALINA_BASE\conf**

8. Verify that the server.xml file located in directory NX_ROOT\bopcfg\www\CATALINA_BASE\conf has the same startup (connector) and shutdown ports as defined in the original server.xml file. Complete the following steps to verify:

   a. <Server port="8085" shutdown="SHUTDOWN">

   b. <Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="8443" />

   c. Ensure no other ports are used as follows. If it is used, you must comment them according to the original server.xml file.

      ```
      <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
      ```

   Note: If any other changes were made to the original server.xml file, then make the same changes to the new server.xml file.

9. Edit NX_ROOT\bopcfg\www\CATALINA_BASE\conf\catalina.properties using the text editor and modify **shared.loader=** as **shared.loader=${catalina.base}/shared/lib/*.jar.** Save the file.

10. If CA Support Automation is installed, verify that the server.xml file located at NX_ROOT\bopcfg\www\CATALINA_BASE_SA\conf has the same startup (connector) and shutdown ports as defined in the original server.xml file.

    Note: If any other changes were made to the original server.xml file, then they would need to be made to the new server.xml file.

11. Modify config.properties located at NX_ROOT\site, as follows:

```
web.tomcat_home=<drive>\:\\<install_directory>\\CA\\SharedComponents\\tomcat\\7.
0.59
web.tomcat.version=7.0.59 web.cawf_tomcat_home==<drive>\:
\\<install_directory>\\CA\\SharedComponents\\tomcat\\7.0.59
```

12. For CA Visualizer, copy the CMDBVisualizer.xml file from the backup conf directory that you created in step 7 to NX_ROOT\bopcfg\www\CATALINA_BASE_VIZ\conf\Catalina\localhost

> **Important!** If this step is not performed then the applications will not deploy properly when Tomcat is started.

13. If CA Advanced Workflow is installed, copy the pm.xml and wl.xml files from the backup of the conf directory you created in step 6 to the following location:

```
<drive>:\<install_directory>\CA\Service Desk
Manager\bopcfg\www\CATALINA_BASE_WF\conf\Catalina\localhost
```

> **Important!** If this step is not performed then the applications will not deploy properly when Tomcat is started.

14. Start Service Desk.

> **Note:** Similar to Support Automation, if Visualizer, Federated Search or REST Tomcats are installed, then appropriate changes can be performed similar to the approaches as suggested from step 1 to step 9.

15. Apply the following Support Automation Digital Patches:

- For CA SDM 12.9:

OS	Patch
Windows	RO81494
Linux	RO81495
AIX	RO81496
Solaris	RO81497

- For CA SDM 14.1:

OS	Patch
Windows	RO81482
Linux	RO81483
AIX	RO81484
Solaris	RO81485

Install and Configure Apache Tomcat 7.0.59

CA SDM 14.1 provides out-of-the-box Apache Tomcat 7.0.23. This topic provides information to upgrade to Apache Tomcat 7.0.59.

Follow these steps:

1. Shut down CA SDM Daemon Service or CA SDM Proctor Service, or both on the relevant CA SDM server (primary or secondary, or both).

2. Download Tomcat 7.0.59 (apache-tomcat-7.0.59.zip) from http://archive.apache.org/dist/tomcat/tomcat-7/v7.0.59/bin/

   Note: CA SDM supports service packs and point releases of Operating Systems, Databases, Web Servers, Web Browsers, Java, Servlets, and so on. This may not be noted in the certification matrix as long as the reported problem is reproducible with versions that are listed in the matrix. CA reserves the right to refuse support of new point releases should the reported problem require a major rework or redesign to function properly. Both Technical Support and Sustaining Engineering does their best to resolve any issues that occur in a timely manner. If the resolution to the problem is determined to be outside the realm of their support responsibilities, they may ask you to escalate your request for certification to your local account team.

3. Unzip apache-tomcat-7.0.59.zip and copy the files at <drive>:\<install_directory>\CA\SC\tomcat\7.0.59

   Note: After unzipping, ensure that <drive>:\<install_directory>\CA\SC\tomcat\7.0.59 contains conf, bin, webapps, and other directories.

   <drive>:\<install_directory>\CA\SC\tomcat\7.0.59 must NOT contain <drive>:\<install_directory>\CA\SC\tomcat\7.0.59\apache-tomcat-7.0.59. Presence of this directory indicates that the unzipping was done incorrectly.

4. Take a backup of the NX.ENV directory, located at the CA SDM install directory (NX_ROOT).

5. Modify NX.ENV as follows:

```
@NX_TOMCAT_INSTALL_DIR=C:\Program Files\CA\SC\tomcat\7.0.59
```

6. Backup NX_ROOT\bopcfg\www\CATALINA_BASE\conf and the following directories (whichever exist):
   - $NX_ROOT\bopcfg\www\CATALINA_BASE_SA\conf
   - $NX_ROOT\bopcfg\www\CATALINA_BASE_REST\conf
   - $NX_ROOT\bopcfg\www\CATALINA_BASE_VIZ\conf
   - $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\conf
   - $NX_ROOT\bopcfg\www\CATALINA_BASE_WF\conf
7. Copy all files from **<drive>:\<install_directory>\CA\SC\tomcat\7.0.59\conf** to **NX_ROOT\bopcfg\www\CATALINA_BASE\conf**
8. Verify that the server.xml file located in directory NX_ROOT\bopcfg\www\CATALINA_BASE\conf has the same startup (connector) and shutdown ports as defined in the original server.xml file. Complete the following steps to verify:
   a. <Server port="8085" shutdown="SHUTDOWN">
   b. <Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="8443" />
   c. Ensure no other ports are used as follows. If it is used, you must comment them according to the original server.xml file.

      ```
      <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
      ```

Note: If any other changes were made to the original server.xml file, then make the same changes to the new server.xml file.

9. Edit NX_ROOT\bopcfg\www\CATALINA_BASE\conf\catalina.properties using the text editor and modify **shared.loader=** as **shared.loader=${catalina.base}/shared/lib/*.jar.** Save the file.
10. If CA Support Automation is installed, verify that the server.xml file located at NX_ROOT\bopcfg\www\CATALINA_BASE_SA\conf has the same startup (connector) and shutdown ports as defined in the original server.xml file.

Note: If any other changes were made to the original server.xml file, then they would need to be made to the new server.xml file.

11. Modify config.properties located at NX_ROOT\site, as follows:

```
web.tomcat_home=<drive>\:\\<install_directory>\\CA\\SharedComponents\\tomcat\\7.
0.59
web.tomcat.version=7.0.59 web.cawf_tomcat_home==<drive>\:
\\<install_directory>\\CA\\SharedComponents\\tomcat\\7.0.59
```

12. If CA Advanced Workflow is installed, copy the pm.xml and wl.xml files from the backup of the conf directory you created in step 6 to the following location:

    ```
    <drive>:\<install_directory>\CA\Service Desk
    Manager\bopcfg\www\CATALINA_BASE_WF\conf\Catalina\localhost
    ```

    Important! If this step is not performed then the applications will not deploy properly when Tomcat is started.

13. Start Service Desk.

    Note: Similar to Support Automation, if Visualizer, Federated Search or REST Tomcats are installed, then appropriate changes can be performed similar to the approaches as suggested from step 1 to step 9.

14. Apply the following Support Automation Digital Patches:

    - For CA SDM 12.9:

OS	Patch
Windows	RO81494
Linux	RO81495
AIX	RO81496
Solaris	RO81497

    - For CA SDM 14.1:

OS	Patch
Windows	RO81482
Linux	RO81483
AIX	RO81484
Solaris	RO81485

Step 4- Post-Installation Requirements

Complete the following steps after you install CA SDM:

1. Run the *cmdb_update_ambiguity* utility. Use the -h command to view the mandatory options.

> **Note:** If configuration fails during the Validate Extension Tables step, database connectivity can be an issue. Retry the installation and verify that you provided the correct database connectivity information.

2. Restart the services for the integration changes to come to effect.
3. You may need to perform some manual steps to finalize the integration (see page 548).

Step 5- Configure the Servers

As a system administrator, you configure the CA SDM servers under the following circumstances:

- You completed a new installation of CA SDM or upgraded to the latest version of CA SDM and want to implement the advanced availability (see page 508) or conventional (see page 505) configuration.

> You must configure the servers before you start using CA SDM. If you do not configure the servers, you cannot access the application.

- You convert from conventional configuration to advanced availability (see page 516).
- You convert from advanced availability to conventional configuration (see page 514).

Configure Servers for Conventional Configuration

The conventional configuration contains one primary server and one or more secondary servers, all of which you need to configure.

Follow these steps:

1. Configure the Primary Server
2. Add a Server
3. Configure the Secondary Server
4. Verify the Server Details

Configure the Primary Server

Primary server must be configured before you configure any secondary servers.

Follow these steps:

1. Log in to the server that you want to configure as the primary server.

2. Use the pdm_configure command to start the configuration.
   The **Select Server Configuration** screen opens.

3. Select **Conventional** as the configuration type and follow the prompts to complete the configuration. For more information about the configuration, see *Server Configuration Utility (see page 869)*.
   The primary server is now configured.

Add a Server

If you want to install a new server in your CA SDM deployment, you must first add the corresponding server record before you configure it.

Follow these steps:

1. Log in to the following server, depending on your CA SDM configuration:
   - Conventional: Primary server
   - Advanced availability: Background server
2. Select System, Servers from the Administration tab.
3. Click Create New to add a server record for the following server, depending on CA SDM configuration:
   - Conventional: Secondary server
   - Advanced availability: Application or standby server
4. Complete the fields as appropriate for the server.
5. Click Save to add the server detail.

Create Server Fields

The following fields appear when you create or update a server:

- **Host Name**
  Specifies the local host name of the server. The local host name is stored in the usp_servers table in local_host column.

  Important! Ensure that host name is entered as case-sensitive in the usp_servers table.

- **Attachment Servlet Path**
  You must specify the fully qualified domain name of a server using this field:
  http://<host>:<port>/CAisd/Upload/Servlet
  Where <host> is the fully qualified domain name of a server.
  We recommend that you configure this field.

- **Time Zone**
  Specifies the time zone where the server is located. This time zone value is used to trigger events in the application. This value is used only if the Use End User Time Zone option is not selected, or if no time zone is specified for the service type.

- **Record Status**
  Indicates the state of the server. Active status indicates that the server is a part of the CA SDM deployment.

  Important! If you have inactivated any server, it is recommended not to start CA SDM services on that server. This action may result in unexpected behaviour.

- **Server Type**
  Specifies the type of server that you want to configure. Following server types can be selected, depending on your CA SDM configuration:

  - Advanced Availability: Application or standby server
  - Conventional: Secondary server

- **Configured**
  Available only for advanced availability configuration. This field indicates the state of the configured server. The default value of this field is No. The value is updated to Yes after you successfully run pdm_configure on that server. If you edit any of the automatically entered field values of a server record, the Configured field turns to No.

Configure the Secondary Servers

You configure each secondary server after configuring the primary server. This configuration is required to establish communication with the primary server.

Follow these steps:

1. (If you are adding a new secondary server) Ensure that you added the server record of the secondary server that you are configuring. For more information, see the Add a Server section.
2. Log in to the server that you want to configure as the secondary server
3. Use the pdm_configure command to start the configuration.
4. The **Select Server Configuration** screen opens.
5. Select **Conventional** as the configuration type and follow the prompts to complete the configuration. For more information, see *Server Configuration Utility (see page 869)*.
   The secondary server is now configured.
6. Repeat steps 1-3 on each of servers that you want to configure as the secondary server.

Verify Server Details

After you have configured all the servers, ensure that each one is properly configured and available.

Follow these steps:

1. Make sure that primary and all secondary servers are running.
2. Log in to the primary server Web UI.
3. Select **System**, **Servers** on the **Administration** tab.
   The **Server List** page opens.
4. If **Record Status** is set to inactive, edit the server and set to **Active**. If you change the record status, ensure that you reconfigure that server again.
   You have successfully configured the servers.

Configure Servers for Advanced Availability

The advanced availability configuration offers more resilience to server outages, higher application availability, and supports rolling maintenance with minimal end-user disruption. This configuration requires one background server, one or more standby servers, and one or more application servers, all of which you need to configure.

Follow these steps:

1. Configure the Background Server.
2. Add a Server.
3. Configure the Standby or Application Servers.
4. Verify the Server Details.

Configure the Background Server

Configure the background server before configuring the application or standby servers.

Follow these steps:

1. Log in to the server that you want to configure as the background server.
2. Use the pdm_configure command to start the configuration.
   The **Select Server Configuration** screen opens.
3. Select **Advanced Availability** as the configuration type and follow the prompts to complete the configuration. For more information, see *Server Configuration Utility (see page 869)*.
   The background server is configured.

Add a Server

If you want to install a new server in your CA SDM deployment, you must first add the corresponding server record before you configure it.

Follow these steps:

1. Log in to the following server, depending on your CA SDM configuration:
   - Conventional: Primary server
   - Advanced availability: Background server
2. Select System, Servers from the Administration tab.
3. Click Create New to add a server record for the following server, depending on CA SDM configuration:
   - Conventional: Secondary server
   - Advanced availability: Application or standby server
4. Complete the fields as appropriate for the server.
5. Click Save to add the server detail.

Create Server Fields

The following fields appear when you create or update a server:

- **Host Name**
  Specifies the local host name of the server. The local host name is stored in the usp_servers table in local_host column.

  Important! Ensure that host name is entered as case-sensitive in the usp_servers table.

- **Attachment Servlet Path**
  You must specify the fully qualified domain name of a server using this field:
  http://<host>:<port>/CAisd/Upload/Servlet
  Where <host> is the fully qualified domain name of a server.
  We recommend that you configure this field.

- **Time Zone**
  Specifies the time zone where the server is located. This time zone value is used to trigger events in the application. This value is used only if the Use End User Time Zone option is not selected, or if no time zone is specified for the service type.

- **Record Status**
  Indicates the state of the server. Active status indicates that the server is a part of the CA SDM deployment.

  Important! If you have inactivated any server, it is recommended not to start CA SDM services on that server. This action may result in unexpected behaviour.

- **Server Type**
  Specifies the type of server that you want to configure. Following server types can be selected, depending on your CA SDM configuration:
  - Advanced Availability: Application or standby server
  - Conventional: Secondary server
- **Configured**
  Available only for advanced availability configuration. This field indicates the state of the configured server. The default value of this field is No. The value is updated to Yes after you successfully run pdm_configure on that server. If you edit any of the automatically entered field values of a server record, the Configured field turns to No.

Configure the Standby or Application Servers

You configure each standby and application server after configuring the background server. This configuration is required to establish communication with the background server.

Important! (Recommended) Ensure that both background server and all other standby servers have similar configuration. This process ensures that during a failover when a standby server becomes the new background server, it can function exactly like the old background server.

Follow these steps:

1. (If you are adding a new standby or application server) Ensure that you added the server record of the standby or application server that you are configuring. For more information, see the Add a Server section.
2. Log in to the server that you want to configure as the standby or application server.
3. Use the pdm_configure command to start the configuration.
   The **Select Server Configuration** screen opens.
4. Select **Advanced Availability** as the configuration type and follow the prompts to complete the configuration. To enable and use the federated search feature, select the federated search option. For more information, see *Server Configuration Utility (see page 869)*.
5. Repeat steps 1-3 on each of the servers that you want to configure as the standby and application server.
   You have configured the standby and application servers.
6. Suppose that you have one or more application servers. You can configure a load balancer (see page 511) to track the requests to and from the different application servers.

Note: To use a load balancer URL or an application server URL for the links in the CA SDM notifications, complete the following steps:

a. Log in to the background server.

b. Select **Options Manager**, **Notifications** on the **Administration** tab.

c. Change the value of the web_cgi_url option to point to:

- The load balancer if you have more than one application servers.
- The application server, if you have only one application server.

Verify the Server Details

After you have configured all the servers, ensure that each one is properly configured and available.

Follow these steps:

1. Make sure that all background, standby, and application servers are running.
2. Log in to the background server Web UI.
3. Select **System**, **Servers** on the **Administration** tab.
   The **Server List** page opens.
4. Verify that the **Configured** field displays Yes for the standby and application server records.
5. If **Record Status** is set to inactive, edit the server and set to Active. If you change the record status of any server, reconfigure it.
   You have successfully configured servers for the advanced availability configuration.

Note: You can click any of the Local Host entries on the Server Details page to view the details of the server.

Configure the Load Balancer

If you have one or more application servers, configure the load balancer to monitor the traffic on these application servers.

Follow these steps:

1. Install Apache Tomcat on an application server.

Note: Ensure that Tomcat is using JRE 1.7 and ensure that the Tomcat is not using the port number that is configured for the CA SDM components.

2. (Optional) Configure SSL on the Tomcat servers that you have installed. For more information about configuring SSL, see How to Configure SSL Authentication (see page 935).

3. Deploy the health servlet. Complete the following steps:

   a. Copy the HealthServlet.war file from the $NX_ROOT/samples/HealthServlet folder to the *TOMCAT_HOME*/webapps folder.

   b. Restart Tomcat.

Note: The HealthServlet.war file is deployed in the webapps folder. To confirm the deployment, verify that the HealthServlet folder is created in the same webapps folder. After the successful deployment, the health servlet is ready to perform the health checks. It includes checking the status of the SLUMP and health of the CA SDM processes that are defined in the health.xml file. Find the health.xml file at TOMCAT_HOME/webapps/HealthServlet/WEB-INF/classes directory.

You can modify this health.xml file, based on your organization needs. Ensure that the XML does not have any errors and that you restart Tomcat to reflect the changes that are made to the XML.

Example: Modify the health.xml File to Monitor the Webengine Process

4. Repeat steps 1-3 on all the other application servers.

5. Configure the load balancer to monitor the following healthservlet URL on each application server:

   ```
   http://<Machine_name>:<Port_number>/HealthServlet/GetHealth
   ```

6. Each application server has its own set of processes.

   - If the SLUMP and all the CA SDM processes are working properly, the load balancer tool receives an HTTP 200 response from the application server with a predefined payload as follows:

     ```
     AA-Server-Status: All OK!

     AA-Server-Role: APP
     ```

   - If a SLUMP or any of the CA SDM processes (listed in health.xml) stop working and cannot resume, the third-party tool receives an HTTP 503 response from the application server with a predefined payload as:

     ```
     AA-Server-Status: NOT OK!

     AA-Server-Role: APP
     ```

- If the healthservlet URL of an application server sends a quescing response, the load balancer must redirect requests from that server to the other application servers. For example, the following response is received when the application server is quesced for 58677 seconds.

  ```
  Quiesce time remaining :58677 seconds
  ```

- If an application server is healthy and no quescing is required, then the following response is received from the healthservlet of the server:

  ```
  Currently no Quiesce time set. Return code : -1
  ```

7. Configure the session persistence on each load balancer. For more information, see your load balancer document. This process ensures that a request coming from one application server is routed back to the same application server.

Example: Modify the health.xml File to Monitor the Webengine Process

Add the process in the health.xml file with the correct tagname, as defined in CA SDM. Complete the following steps to find the tagname:

1. a. Open the pdm_startup.i and pdm_startup files from the $NX_ROOT/pdmconf directory.

   b. Look for the process that you want to monitor in both the files.

   c. Find the corresponding tagname by matching the variables in both the files. For example, webengine process is defined in the pdm_startup.i file as follows:

   ```
   #define WEBENGINE(_TAG,_HOST,_SLUMP_NAME,_DOMSRVR, _CFG, _WEBDIRECTOR,
   _RPC_NAME)
   ```

   The webengine process is defined in the pdm_startup file as follows:

   ```
   WEBENGINE(webengine, $NX_LOCAL_HOST, web:local, domsrvr, $NX_ROOT/bopcfg
   /www/web.cfg, "", "rpc_srvr:%h")
   ```

   From the example, we can find out that the tagname for webengine process is webengine.

   Important! For creating a new process, the existing process is commented out in the pdm_startup file and new entries are added. Ensure that you look for the tagname in the new process entrie

At the end of this topic, you have successfully configured the load balancer.

Convert from Advanced Availability to Conventional Configuration

You can revert to conventional configuration from the advanced availability configuration. Similarly, you can convert a conventional configuration to advanced availability. This article gives the procedures for both types of conversions.

Convert from Advanced Availability to Conventional

Follow these steps:

1. Verify the Prerequisites (see page 514)
2. Stop all services on the application and standby servers.
3. Inactivate all Application and Standby Servers (see page 514).
4. Configure the Primary Server (see page 515).
5. Change the Application and Standby Server Types (see page 515).
6. Configure the Secondary Servers (see page 515).
7. Verify Server Details (see page 516)

Verify the Prerequisites

Complete planning for the conventional configuration. For more information, see Plan the CA SDM Installation (see page 450).

Note: You can configure only the background server as the primary server. You can configure only the standby and application servers as the secondary servers.

Inactivate All Application and Standby Servers

Before you configure the servers for the conventional configuration, ensure that you inactivate all the application and standby servers.

Follow these steps:

1. Log in to the web interface of the background server.
2. Select **System**, **Servers** on the **Administration** tab.
   The **Server List** page opens.
3. Click the host name of the application server.
   The **Server Detail** page opens.
4. Click **Edit**.

5. Change the **Record** status to **Inactive**.

> **Important!** If you have inactivated any server, it is recommended not to start CA SDM services on that server. This action may result in unexpected behaviour.

6. Click **Save**.
   The application server is set to inactive.

7. Perform steps 3-6 for all the other application and standby servers.
   All application and standby servers are set to inactive.

Configure the Primary Server

Primary server must be configured before you configure any secondary servers.

Follow these steps:

1. Log in to the background server web interface and inactivate it.

2. Use the pdm_configure command and start the configuration.
   The **Select Server Configuration** screen opens.

3. Select **Conventional** as the configuration type and follow the prompts to complete the configuration. For more information about the configuration, see the *Server Configuration Utility (see page 869)*.
   The primary server is now configured.

Change the Application and Standby Server Types

After you configure the primary server, change the server type for all the application and standby servers to secondary servers and then activate them.

Follow these steps:

1. Make sure that the primary server is running.

2. Log in to the primary server web interface.

3. Select **System**, **Servers** on the **Administration** tab.
   The **Server List** page opens.

4. Set the **Record Status** for all application and standby servers as **Active**.

5. Change the server type of all the application and standby servers to secondary servers.
   The server type for all application and standby servers are changed.

Configure the Secondary Servers

You configure each secondary server after configuring the primary server. This configuration is required to establish communication with the primary server.

Follow these steps:

1. Log in in to the application or standby server that you want to configure as the new secondary server.

2. Use the pdm_configure command to start the configuration.
   The **Select Server Configuration** screen opens.

3. Select **Conventional** as the configuration type and follow the prompts to complete the configuration. For more information, see the *Server Configuration Utility (see page 869)*.
   The secondary server is now configured.

4. Repeat steps 1-3 on each of servers that you want to configure as the secondary server.

Verify Server Details

After you have configured all the servers, ensure that each one is properly configured and available.

Follow these steps:

1. Make sure that primary and all secondary servers are running.

2. Log in to the primary server Web UI.

3. Select **System**, **Servers** on the **Administration** tab.
   The **Server List** page opens.

4. If **Record Status** is set to inactive, edit the server and set to **Active**. If you change the record status, ensure that you reconfigure that server again.
   You have successfully configured the servers.

Convert from Conventional Configuration to Advanced Availability

Before converting from the conventional to the advanced availability configuration, upgrade to or install CA SDM 12.9 on all the servers.

Follow these steps:

1. Plan for the Advanced Availability Configuration. For more information, see the CA SDM Installation Planning (see page 450).

2. Stop all services on the secondary servers.

3. Inactivate All the Secondary Servers (see page 517).

4. Configure the Background Server (see page 517).

5. Change Secondary Server Type (see page 517).

6. Configure the Standby and Application Servers (see page 518).

7. Verify Server Details (see page 519).

Inactivate All the Secondary Servers

Before you configure the servers for the advanced availability configuration, ensure that you inactivate all the secondary servers.

Follow these steps:

1. Log in to the web interface of the primary server.

2. Select **System**, **Servers** on the **Administration** tab.
   The **Server List** page opens.

3. Click the host name of the secondary server.
   The **Server Detail** page opens.

4. Click **Edit**.

5. Change the **Record** status to **Inactive**.

   Important! If you have inactivated any server, it is recommended not to start CA SDM services on that server. This action may result in unexpected behaviour.

6. Click **Save**.
   The secondary server is set to inactive.

7. Perform steps 3-6 for all the other secondary servers.
   All secondary servers are set to inactive.

Configure the Background Server

Configure the background server before configuring the application or standby servers.

Follow these steps:

1. Log in to the primary server.

2. Use the pdm_configure command to start the configuration.
   The **Select Server Configuration** screen opens.

3. Select **Advanced Availability** as the configuration type and follow the prompts to complete the configuration. For more information, see the *Server Configuration Utility (see page 869)*.
   The background server is configured.

Change Secondary Server Type

After you configure the background server, change the server type for all the secondary servers to application and standby servers and activate them.

Follow these steps:

1. Make sure that the background server is running.
2. Log in to the web interface of the background server.
3. Select **System**, **Servers** on the **Administration** tab.
   The **Server List** page opens.
4. Set the Record Status for all secondary servers as Active.
5. Change the server type of all the secondary servers to application or standby servers, as required.
   The server type of all the secondary servers is changed.

Configure the Standby and Application Servers

You configure each standby and application server after configuring the background server. This configuration is required to establish communication with the background server.

Important! (Recommended) Ensure that both background server and all other standby servers have similar configuration. This process ensures that during a failover when a standby server becomes the new background server, it can function exactly like the old background server.

Follow these steps:

1. Log in to a secondary server.
2. Use the pdm_configure command to start the configuration.
   The **Select Server Configuration** screen opens.
3. Select **Advanced Availability** as the configuration type and follow the prompts to complete the configuration. For more information, see the *Server Configuration Utility (see page 869)*.
4. Repeat steps 1-3 on each of the servers that you want to configure as the standby and application server.
   You have configured the standby and application servers.
5. If you want to use a load balancer to track the requests to and from the different application servers, configure the load balancer (see page 511).

Note: To use a load balancer URL or an application server URL for the links in the CA SDM notifications, complete the following steps:

a. Log in to the background server.

b. Select **Options Manager**, **Notifications** on the **Administration** tab.

c. Change the value of the web_cgi_url option to point to:

- The load balancer if you have more than one application servers.
- The application server, if you have only one application server.

6. Verify the Server Details (see page 519).

Verify Server Details

After you have configured all the servers, ensure that each one is properly configured and available.

Follow these steps:

1. Make sure that all background, standby, and application servers are running.
2. Log in to the background server Web UI.
3. Select **System**, **Servers** on the **Administration** tab.
   The **Server List** page opens.
4. Verify that the **Configured** field displays Yes for the standby and application server records.
5. If **Record Status** is set to inactive, edit the server and set to Active. If you change the record status of any server, reconfigure it.
   You have successfully configured servers for the advanced availability configuration.

Note: You can click any of the Local Host entries on the Server Details page to view the details of the server.

Step 6- Verify the Installation

After you install CA SDM, use the following information to verify that the installation was successful.

1. (If you have selected to install Unified Self-Service along with CA SDM) After the installation is complete, to verify the Unified Self-Service installation, log in to the following URL as an administrator:

   `http://<CA_Unfied_Self_Service_Server_Name>:<Port_Number>/`

   The default tenant Home Page is displayed.

2. Verify that a system environment variable for the path is set for the product to the installation directory you specified. The default home directory is C:\Program Files\CA\Service Desk Manager. For a 64-bit Windows operating system, the path is C:\Program Files (x86) \CA\Service Desk Manager. For a non-Windows operating system, the path is /opt/CAisd/.

3. Verify the following information:

    a. In the Control Panel (Add or Remove Programs), verify that an entry appears for the product.

    b. From the Start menu, verify that the following options appear:

    - View the documentation.
    - Start the Configuration Wizard.
    - Start the Web Interface.
    - Contact Technical Support.
    - Start the Web Screen Painter.
    - Uninstall CA SDM.

4. From the Windows Start menu, click Start, CA, Service Desk Manager, Service Desk Manager Web Client. If the Web Interface starts properly, then your installation is successful. For more information about the default user accounts created at the time of installation, see the CA SDM Default User List topic. If you cannot verify this information, the product has not been installed correctly. In this case, start the CA SDM installation again to modify the installation.

5. When CA SDM is up and running, it is recommended to check the process memory. For optimal performance, we recommend the following method:

    a. Set a notification when the process memory exceeds 1.25 GB and begin a check on the processes that are running.

    b. Set a warning notification when the process memory exceeds 1.5 GB and take corrective actions to check the memory usage.

6. Review the CA SDM Default User List (see page 520)

7. Check the Status of the Required Ports (see page 521)

Review the CA SDM Default User List

The following table lists default user information for typical CA SDM implementations:

OS	Product	Default Username	OS Level?	How it is Created
Windows	CA SDM	ServiceDesk	Yes	Automatically
	CA EEM	EiamAdmin	No	Default Password: EiamAdmin
		ServiceDesk	No	Created in the MDB during configuration

OS	Product	Default Username	OS Level?	How it is Created
	CA MDB SQL Server			
	CA MDB Oracle	mdbadmin	No	Created in the MDB during configuration
	CA SDM	CASMAdmin	No	Manually created
UNIX	CA SDM	srvcdesk	Yes	Manually created
	CA MDB Oracle	mdbadmin	No	Created in the MDB during configuration
	CA SDM	CASMAdmin	No	Manually created
Linux	CA SDM	srvcdesk	Yes	Manually created
	CA MDB Oracle	mdbadmin	No	Created in the MDB during configuration
	CA SDM	CASMAdmin	No	Manually created

Check the Status of the Required Ports

The CA SDM installation requires various ports and port ranges to be opened on your firewall. Ensure that following ports are open before you start implementing CA SDM:

The ports opened on the firewall depends on the *NX.env* file settings. By default, CA SDM chooses the port that is readily available. The system reserves ports less than 1024, but can request a port number as high as 65335.

Note: The NX.env file is located in the default CA SDM installation folder.

The following *NX.env* variables set the starting port (2100) and the incremental increase (plus 1) to find an open port:

- NX_SLUMP_FIXED_SOCKETS=1
- NX_SLUMP_SECONDARY_SOCKET=2100

The following list displays default and recommended ports (and port ranges) for a typical CA SDM installation:

- **Database**
  - Oracle: 1521
  - SQL Server: 1433
- **CA SDM**
  - FTP: 21
  - SMTP: 25

- HTTP: 80
- HTTPS: 8080
- HTTPS (secondary): 8081
- POP3: 110
- IMAP: 143
- LDAP: 389
- WebEx: 1270
- mstsc: 1389
- oaserver: 1706
- Slump Socket: 2100
- qserver: 2234
- Proctor Socket: 2300
- Communications: 2365
- Apache Tomcat: 8080
- Apache Tomcat Shutdown:
- SSL on Apache Tomcat: 8443

- **EBR Search**
  - Base Port: 13000
- **Portal Server**
  - Apache Tomcat: 8080
  - Apache Tomcat Shutdown: 8085
  - SSL Functionality: 8443
  - Portal_Safe_List: 8444
- **Support Automation**
  - Main Server (Socket Server) Internal: 7005
  - Main Server (Socket Server) External: 10443
  - Socket Proxy Server (Socket Configuration Main Server) Internal: 7005

- Socket Proxy Server (Socket Configuration Main Server) External: 10444
- Message Routing Server (Socket Configuration) External: 10444
- Apache Tomcat: 8070
- Apache Tomcat Shutdown: 8075

- **Visualizer**
  - Apache Tomcat: 9080
  - Apache Tomcat Shutdown: 9085

At the end of this step, you must have opened the required ports.

Troubleshooting the Installation

Accessing the Installation Log File

When you install CA SDM, an installation log file is created, which includes the actions, events, and system changes that occurred during the installation. If the product does not install correctly, you can view the errors in the log file and can fix the problems.
You can find the Service Desk Manager_r14_1_Install.log file in the \log folder of the installation directory. For Remote Components installations, the log is located in the %TEMP% directory. Open the file with a text editor such as Notepad or the vi editor.

Note: If you cancel the installation before it is finished, the installation log is created on your desktop for Windows. For UNIX and Linux, the log file is created in the root directory.

Troubleshooting Tips

Use the following tips to troubleshoot the installation of CA SDM:

- If you receive an Install Shield error during CA SDM installation, wait until msiexec.exe stops running. Then try installing the product.
- Suppose that you have upgraded from Argis 8.0 to CA Asset Portfolio Management r11.2 and you are sharing the CA MDB (database) with CA SDM. You may encounter problems when you add or update assets in asset families using CA SDM. To avoid errors, you must define the asset extension tables to CA SDM using one of the following methods:
- - Use WSP to define the tables and the forms to view and edit the table entries.
- - Manually edit the tables and forms using the following guidelines:
- - The file $NX_ROOT\bopcfg\majic\assetx.maj contains a template that can be used to create a majic file to identify the columns in the asset extension table to CA SDM. Copy this file and edit as appropriate, following the instructions that are available in the file.

- Create a .sch file in $NX_ROOT\site\mods directory to define the database columns. The files $NX_ROOT\site\assetx_schema.sch and $NX_ROOT\site\assetx_index.sch can be used as templates which can be copied and edited as appropriate for your asset extension tables.

  Note: References to NX_ROOT pertain to the environmental variable containing the installation path of CA SDM. This NX_ROOT variable is set in the NX.env configuration file that is used to set environmental variables for CA SDM.

  Example: NX_ROOT Definition

  @NX_ROOT=C:\Program Files\CA\Service Desk Manager

- (Internet Explorer 8 on Windows 2008) If the internet security level is set to high, the CA SDM URL and about:blank must be added as Trusted Sites.

- (Google Toolbar) The CA SDM web interface may have a problem displaying the title bar text at the top of the window.

- (Internet Explorer 8.0) You may experience periodic increased memory use when accessing the CA SDM web interface. This is a known issue with the current release of Internet Explorer. To release the memory, periodically minimize your main CA SDM web page.

- You may receive an Unprivileged Script error when you use cut, copy, and paste functionality on the HTML editor page in Knowledge Categories. Click OK to view a technical note at mozilla.org (http://mozilla.org), which shows you how to allow a script to access the clipboard.

- When viewing the content of a file attachment in which the file name contains Latin-1 extended characters, a save as popup appears. You can either save to disk or click open and select an application to open the attachment.

Secure CA SDM from Cross-Site Scripting Vulnerabilities

The CA SDM installation is susceptible to reflected cross-site scripting vulnerabilities, which might result in the infected URL being reflected back to the user. To secure CA SDM from such vulnerabilities, validation parameters exist in the web.cfg file. These parameters perform a white list validation in the webengine. Also, install the NX option on the primary and secondary servers to secure CA SDM.

Points to consider before you proceed with securing CA SDM:

- The SDM URL parameters that are defined in the web.cfg file are validated for securing CA SDM.

- You can add SDM URL parameters in the web.cfg file with required validation pattern. You can also add validation patterns, if necessary.

Secure CA SDM from Cross-Site Scripting Vulnerabilities in Conventional and Advanced Availability Mode

Follow these steps:

1. Stop the CA SDM services.

2. On the primary server, execute the following command to install the NX option.

   ```
   pdm_options_mgr -c -a pdm_option.inst -s VALIDATE_REQUEST_PARAMETER -v 1
   ```

   Note: For each secondary server, manually add or update the NX option in the *NX.env* file that is located in *$NX_ROOT* directory.

3. (Optional) To avoid losing the changes when you run the *pdm_configure* command with the *-t* flag.

   ```
   pdm_options_mgr -c -a pdm_option.inst -s VALIDATE_REQUEST_PARAMETER -v 1 -t
   ```

4. Restart the CA SDM services.

5. (Optional) In Advanced Availability mode, perform rolling maintenance to apply the NX option on all servers.

Install and Configure JRE 1.8.0_45

Complete the following steps to install and configure JRE 1.8.0_45 (32-bit) to use with CA SDM release 14.1:

1. Shut down the CA SDM Daemon or CA SDM Proctor Service, or both on the relevant CA SDM server (primary or secondary, or both).

2. Download JRE 1.8.0_45 (jre-8u45-windows-i586 via the Download JRE link) from http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html

3. During the installation, select the Change destination folder option and enter the destination folder as <drive>:\<install_directory>\CA\SC\JRE\1.8.45

4. Take a backup of NX.env, located at <drive>:\<install_directory>\CA\Service Desk\

5. Modify NX.env as follows:

   ```
   @NX_JRE_INSTALL_DIR=C:/Program Files (x86)/Java/jre1.8.0_45
   ```

6. Start Service Desk.

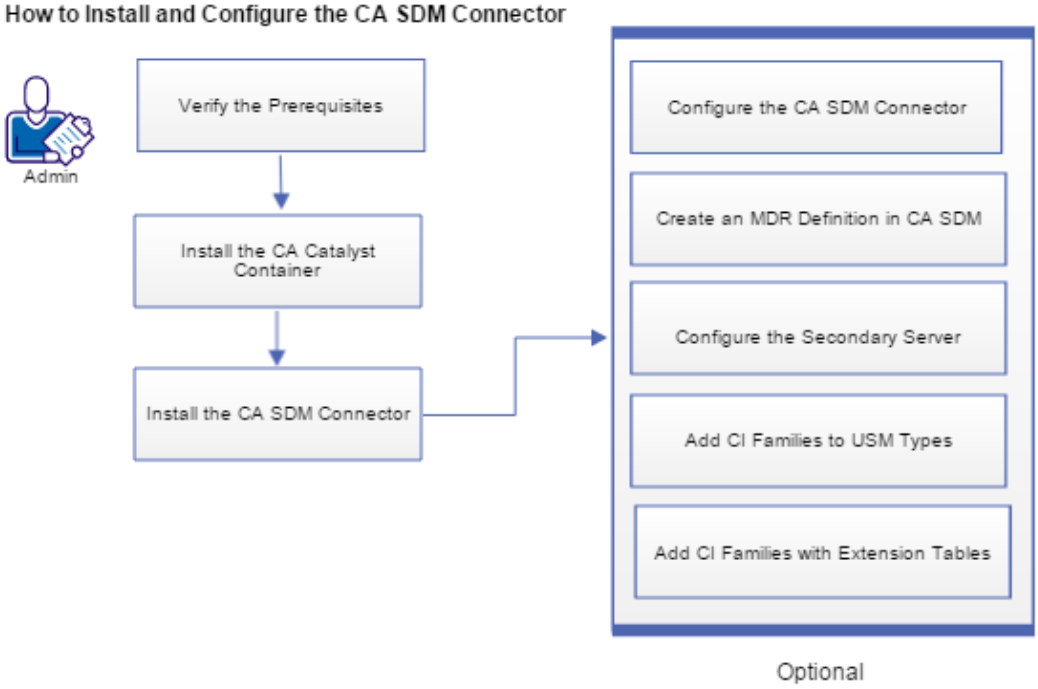
7. Install and configure Apache Tomcat 7.0.59 (see page 502) for Support Automation to work properly.

How to Install CA SDM Connector

CA SDM notifies the CA SDM connector when changes occur to incidents, problems, change orders, CIs, and relationships. The CA SDM connector queries CA SDM for information about the object (router, for example) and transmits the information through the connector framework and publishes to CA Catalyst.

The CMDB module of CA SDM provides a repository of CIs and their relationships. Organizations can use the repository to view the CIs (printers, computer systems, network services, for example). CI relationships can be viewed on the CI detail form or through the MDR Launcher in CA CMDB Visualizer. For more information about the MDR Launcher in CA CMDB Visualizer, see MDR Management (see page 2679).

The following diagram shows how to install and configure the CA SDM Connector:



Follow these steps:

1. Verify the Prerequisites to Install (see page 527)
2. If you plan to install the CA SDM Connector and the CA Catalyst Server on different computers, install the CA Catalyst Container on the same computer where you plan to install the CA SDM Connector (For more information about installing the CA Catalyst Container, see the *CA Catalyst documentation*).
3. Install the CA SDM Connector (see page 533)
4. Restart the CA Catalyst Container service on the CA Catalyst server.
5. (Optional) Configure the CA SDM Connector (see page 525)
6. (Optional) Create an MDR Definition in CA SDM (see page 3409)
7. (Optional) Configure the Secondary Server (see page 534)
8. (Optional) Add CI Families to USM Types (see page 538)

9. (Optional) Add CI Families with Extension Tables (see page 541)

Verify the Prerequisites to Install

This topic contains the following information:

Operating System Support

The CA SDM Connector supports installation on the following operating systems:

- Windows Server 2008 SP1 and SP2 (x64-bit and x86-bit)
- Windows Server 2008 R2 (x64-bit)
- Windows Server 2012 R2 (64-bit only)
- Windows Server 2012 (64-bit only)

Supported Versions of the Associated Products

The CA SDM Connector installation requires the following product versions:

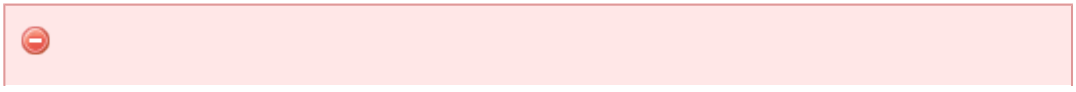
- CA Catalyst Server r3.2
- CA Catalyst Container r3.2 and r3.4.1
- CA Configuration Automation r12.8 SP1 and r12.8 SP2
- CA EEM r8.4, r12.5, r12.5.1
- CA SDM r12.9 CUM1, r14.1.01
- CA SOI r3.1, r3.2, r3.2 CUM3, r3.3, r3.3 CUM1

The supported versions of these products can be downloaded from http://support.ca.com (http://support.ca.com/).

CA SDM Connector Installation Considerations

Before you install the CA SDM Connector, verify that you have the following prerequisites:

- Install and configure the supported version of CA Catalyst. For more information about the installation procedure, see the CA Catalyst documentation.



Important! If you are using CA Catalyst Container r3.4.1, you do not need to install the CA Catalyst server.

- If you plan to install the CA SDM Connector and CA Catalyst Server on different computers, install the CA Catalyst Container on the computer where CA SDM Connector will be installed. For more information about installing procedure of the CA Catalyst Container, see the CA Catalyst documentation.

Note: Container installation cannot be performed on Windows 2012 OS. To support Windows 2012 OS, right click on <*Container Installation Location* >\Disk1\InstData\Windows\VM\install.exe and select Properties, Compatibility. Change the compatibility mode to Windows XP and then start the installation by double clicking the .exe file.

- For CA SDM connector to function for CA SDM installed in supported locales, you must first apply RO72246 (Language Independent) and RO72249 (Language Combo) patches on CA SDM 12.9. Then apply the following patches:

Language	Patch
German	T52Y442
Simplified Chinese	T52Y443
Japanese	T52Y444
English	T52Y445
French	T52Y446
French Canadian	T52Y447
Spanish	T52Y448
Italian	T52Y449
Brazilian Portuguese	T52Y450

- You must upgrade to CA SDM 14.1.01 (see page 633) and first apply RO80318 (Windows Master) patch. Then apply the following patches:

Language	Patch
German	T52Y463
Japanese	T52Y464
French	T52Y465
French Canadian	T52Y466
Spanish	T52Y467
Italian	T52Y468
Brazilian Portuguese	T52Y469

- You install the CA SDM Connector on the same server that runs CA SDM to get access to the interfaces used for the connector-management data repository (MDR) communication.

  Note: (Conventional configuration) You can configure the CA SDM connector to communicate with CA SDM on a primary or secondary server. We recommend a dedicated secondary server to serve requests of the connector and notify the connector with the updates on the objects that are processed. For more information about the secondary server configuration, see Configure the Secondary Server (see page 534).

  Important! (Advanced availability configuration) It is recommended to install the CA SDM connector on any ONE of the application servers and not on the background or standby server. So. i f the CA SDM server (application server on which this connector is installed) goes down, then the CA SDM connector service will also go down.

- You have the login credentials of a CA SDM user with either administrator privileges or belonging to an Access Type that has rights to CA SDM Web Services and APIs. In addition to the Administrator role, the Level 2 Analyst role has the appropriate rights.

- (For CA Catalyst Container r3,2) Verify that the CA Catalyst Registry Server is up and running before you start the CA SDM Connector installation.You cannot install the connector on an existing CA SDM Connector installation. Uninstall the existing CA SDM Connector and then install the supported version of the CA SDM Connector.

  Important! If you uninstall the CA SDM Connector, the existing settings (for example, configuration and policy file changes) are not restored. To restore the settings, ensure that you keep a backup of the modified files from the existing installation and migrate it to the newly installed CA SDM Connector data. For more information, see (Optional) Migrate Data from CA SDM Connector r2.5 (see page 529) or (Optional) Migrate Data from CA SDM Connector r3.1 or r3.2 (see page 530)

- (For CA Catalyst Container r3.4.1) Ensure that CA SOI r3.3 is up and running before the CA SDM Connector installation.

(Optional) Migrate Data from CA SDM Connector r2.5

If you have customized the configuration and policy files of the CA SDM Connector r2.5 and want to restore the changes for the new installation, manually migrate the existing data. The migration is a mandatory step to restore existing data since CA SDM Connector does not support upgrade upon reinstallation.

Note: The directory structure of CA SDM Connector r2.5 is different from CA SDM Connector r3.1 or r3.2. CA SDM Connector r2.5 does not store the policy and configuration files in the CA Catalyst registry.

Follow these steps:

1. Download and backup the following files:
   - ServiceDeskManager_<ComputerName>.xml from the SOI_HOME/resources /configurations directory. SOI_HOME is the path where the CA SDM Connector is installed.
   - ServiceDeskManager_policy.en, ServiceDeskManager_policy.xml, ServiceDeskManager_policySB.en, and ServiceDeskManager_policySB.xml files from the SOI_HOME/resources/core/CatalogPolicy directory.
   - USM-CMDB.xml and ServiceDeskObject.xml files from the SOI_HOME/resources directory.
2. Uninstall the existing CA SDM Connector (see page 542).
3. Install the supported version of the CA SDM Connector (see page 533).
4. Log in to the CA Catalyst Registry UI and navigate to the following directory:

   ```
   \topology\physical\<CA_Catalyst_Server>\modules\configuration\
   ```

5. Compare each property from the ServiceDeskManagerConnector.xml file with the backup ServiceDeskManager_<ComputerName>.xml file.Ensure that you correctly add the customized contents from the backup file to the ServiceDeskManagerConnector.xml file.
6. Navigate to the following directory:

   ```
   \topology\physical\<CA_Catalyst_Server>\modules\policy\
   ```

7. Compare the ServiceDeskManager_policy.en, ServiceDeskManager_policy.xml, ServiceDeskManager_policySB.en, and ServiceDeskManager_policySB.xml files with their respective backup files. Ensure that you correctly add the customized contents from the backup files to the new policy files.
8. Navigate to the CATALYST_CONTAINER_HOME/resources directory and compare the USM-CMDB.xml and ServiceDeskObject.xml files with their respective backup files. CATALYST_CONTAINER_HOME is the path where the CA SDM Connector is installed. Ensure that you correctly add the customized contents from the backup file to the new USM-CMDB. xml and ServiceDeskObject.xml files.
9. Restart CA SDM Connector Container service.

(Optional) Migrate Data from CA SDM Connector r3.1 or r3.2

If you have customized the configuration and policy files of the existing CA SDM Connector (for example, CA SDM Connector r3.1) and want to restore the changes for the new installation, manually migrate the existing data. The migration is a mandatory step to restore existing data since CA SDM Connector does not support upgrade upon reinstallation.

Follow these steps:

1. Log in using one of the following steps:

- (Applicable for CA Catalyst Container r3.2) Log in to the CA Catalyst Registry UI using the following URL:

  ```
  https://<registryserver:port>/registry/carbon/admin/login.jsp
  ```

- (Applicable for CA Catalyst Container r3.4.1) Log in to the CA SDM connector machine.

2. Download and backup the ServiceDeskManagerConnector.conf and ServiceDeskManagerConnector.xml files from the following directory:

   - (Applicable for CA Catalyst Container r3.2) \topology\physical\<CA_Catalyst_Server>\modules\configuration\

   - (Applicable for CA Catalyst Container r3.4.1) CA\Catalyst\CatalystConnector\registry\topology\physical\<CA_Connector_Machine>\mod

3. Download and backup the ServiceDeskManager_policy.en, ServiceDeskManager_policy.xml, ServiceDeskManager_policySB.en, and ServiceDeskManager_policySB.xml files from the following directory:

   - (Applicable for CA Catalyst Container r3.2) \topology\physical\<CA_Catalyst_Server>\modules\policy\

   - (Applicable for CA Catalyst Container r3.4.1) CA\Catalyst\CatalystConnector\registry\topology\physical\<CA_Connector_Machine>\mod

4. Download and backup the USM-CMDB.xml and ServiceDeskObject.xml files from the CATALYST_CONTAINER_HOME/resources directory. CATALYST_CONTAINER_HOME is the path where the CA SDM Connector is installed.

5. Uninstall the existing CA SDM Connector (see page 542).

6. Install the supported version of the CA SDM Connector (see page 533).

7. Log in to the CA Catalyst Registry UI and navigate to the following directory:

   a. (Applicable for CA Catalyst Container r3.2) \topology\physical\<CA_Catalyst_Server>\modules\configuration\

   b. (Applicable for CA Catalyst Container r3.4.1) CA\Catalyst\CatalystConnector\registry\topology\physical\<CA_Connector_Machine>\r

8. Compare each property from the ServiceDeskManagerConnector.conf and ServiceDeskManagerConnector.xml files with the respective backup files. Ensure that you correctly add the customized contents from the backup files to the new ServiceDeskManagerConnector.conf and ServiceDeskManagerConnector.xml files.

9. Navigate to the following directory:

   ```
   \topology\physical\<CA_Catalyst_Server>\modules\policy\
   ```

10. Compare the ServiceDeskManager_policy.en, ServiceDeskManager_policy.xml, ServiceDeskManager_policySB.en, and ServiceDeskManager_policySB.xml files with their respective backup files. Ensure that you correctly add the customized contents from the backup files to the new policy files.

11. Navigate to the following directory:

    - (Applicable for CA Catalyst Container r3.2) CATALYST_CONTAINER_HOME/resources
    - (Applicable for CA Catalyst Container r3.4.1) CA\Catalyst\CatalystConnector\registry\topology\physical\<CA_Connector_Machine>\mod

12. Compare the USM-CMDB.xml and ServiceDeskObject.xml files with their respective backup files. Ensure that you correctly add the customized contents from the backup files to the new USM-CMDB.xml and ServiceDeskObject.xml files.

13. Restart CA SDM Connector Container service.

(Optional) Map the Unknown Classes in CMDB

The following families have been identified to have “Unknown” class. Since CA SDM has unique class names, these are not included in the policy files.

- Hardware.DiskPartition
- Hardware.VMDataStore
- Hardware.Processor
- Hardware.File
- Hardware.Memory

If you require these classes to be mapped and created in the CA SDM CMDB, you must create a new class in CA SDM and provide the mapping in the policy files.

Example: Create a class for Hardware.File

Follow these steps:

1. Create a new class in CA SDM. For example, UnknownFile.

2. Edit and provide the following mapping in ServiceDeskManager_policySB.xml (SouthBound) file:

```
<Normalize>
<Field output="class" type="map" input="FileType" >
<mapentry mapin="Unknown" mapout="UnknownFile" />
</Field>
</Normalize>
```

3. Edit and provide the following mapping in ServiceDeskManager_policy.xml (NorthBound) file:

```
<Normalize>
<Field output="FileType" type="map" input="class">
```

```
<mapentry mapin="UnknownFile" mapout="Unknown" />
</Field>
</Normalize>
```

Note: Similarly there are two classes, “Linux” and “AIX” under Hardware.Diskpartition which are not mapped as these have the same name as in Hardware.Server family. If you require these, you must add in policy files similar to that of “Unknown” classes.

Install CA SDM Connector

Ensure that you follow the CA SDM Connector Installation Considerations (see page 527) correctly before installing the CA SDM Connector.

Note: Based on the language in which CA SDM is installed, the appropriate connector policy files are now installed by the modified CA SDM connector installer. However, the connector installation screens will still remain in English.

Follow these steps:

1. Log in to the following server, depending on your CA SDM configuration:

   Important! Verify that the user has complete administrative privileges, such as the ServiceDesk user.

   - (Advanced availability) Application server
   - (Conventional) Primary or Secondary server

2. Go to http://support.ca.com (http://support.ca.com/) and complete the following steps:

   a. Download and unzip the Connector_CAServiceDeskManager zip file.

   b. Execute the Connector_CAServiceDeskManager.exe file.
   The Introduction screen appears.

3. Click Next, accept the terms of the License Agreement, and click Next.
   The Choose Container Node screen appears.

4. Select a custom container node and click Next.
   The CA SDM Configuration screen appears.

5. Enter the following CA SDM information and click Next.

   - **CA Service Desk Manager User**
     Specifies the CA SDM user.

- **CA Service Desk Manager Password**
  Specifies the corresponding password of the CA SDM user.

- **Enable TWA Flag**
  Specifies to enable or disable the Transaction Work Area (TWA) flag. TWA (see page 2531)is an intermediate storage system for the data.

The Service Startup screen appears.

6. Keep the check box selected to start the CA SDM Connector services automatically after the installation. To perform the post installation steps, clear the check box. Click Next.
   The Installation Summary screen appears.

7. Review your selections and click Install.
   The CA SDM Connector installs on the system and integrates with the appropriate product database and CA Catalyst instance.
   The Install Complete screen appears.

8. Click Done.

Note: If the installation summary page displays installation errors, view the CATALYST_*HOME\CA_ Service_Desk_Manager_Connector_Install_<Date (MM-DD-YYYY)> <Time(HH:MM:SS)>.log* file to troubleshoot the installation. CATALYST_HOME specifies the folder where you installed the CA SDM Connector. This file is created after you complete the installation.

The CA SDM Connector is installed.

Note: For more information about USM data mapping, see USM Data Mapping for CA Service Desk Manager Connector (see page 4730).

(Optional) Configure the Secondary Server

If you installed the CA SDM Connector on a secondary CA SDM server, complete the following post-installation steps:

1. Complete the following steps to locate the Domsrv name of the secondary server:

   a. Open a command prompt on the CA SDM server (primary or secondary) and navigate to the *SDM_HOME/bin* directory.

   b. Execute pdm_status (see page 3889) from the command line. This command shows the status of all the processes on the system.

   c. Locate the Domsrvr name that corresponds with the secondary server host name.

2. Launch the CA Catalyst Registry UI by entering the following URL:

   ```
   https://<registryserver:port>/registry/carbon/admin/login.jsp
   ```

3. Open the ServiceDeskManager_Connector.xml file from the following directory in the CA Catalyst Registry UI:

   ```
   /topology/physical/<NODE-NAME>/module/configuration/
   ```

   Note: <NODE-NAME> displays the host name where you installed CA SDM Connector.

4. Click Edit as Text.

5. Locate Domsrvr_name in the file and specify the name identified by pdm_status in step 1.

6. Click Save Content.
   The secondary server is configured.

7. (Optional) Follow these steps to change the Domsvr name after the CA SDM Connector is online:

   a. Click Administration, Connector Configuration.

   b. In the Domsrv field on the connector details page, specify the Domsvr name of the secondary server.
      The configuration settings are updated.

   c. Click Stop, Start.

   The CA SDM Connector is restarted.

(Optional) Configure the CA SDM Connector

After the CA SDM Connector installation, you can modify the CA SDM Connector properties that you defined during the installation. You can customize the integration by introducing new CMDB families to participate in the integration, deploying the CA SDM Connector on the secondary server, excluding certain CI types, and so on.

Follow these steps:

1. Log in to the CA Catalyst Registry UI using the following URL:

   ```
   https://<registryserver:port>/registry/carbon/admin/login.jsp
   ```

   - **registryserver**
     Specifies the name of the server where you installed the CA Catalyst Registry.

- **port**
  Specifies the CA Catalyst Registry port.

The Registry Browse page appears.

2. Click ServiceDeskManagerConnector.xml from the following directory:

```
/topology/physical/<NODE-NAME>/modules/configuration
```

> **Note:** <NODE-NAME> indicates the hostname where you installed the CA SDM Connector.

3. Click Edit as Text.

4. Change any of the following properties from the Connection Details table and click Save:

   - **deviceXXXFamilies**
     Specifies the list of CMDB families with mapped USM CI types that require device properties defined by USM import standards in CA Catalyst. When device properties are not defined for the CI, the CA SDM Connector uses this property to obtain the information from the system on which the CI is hosted.
     For example, the application configuration manager discovers the software that uses the COTS class and Software.COTS family and populates the system with the host name (or DNS name) of the computer on which the application is running. If the system name is not found, the CA SDM Connector uses this property to retrieve the information.
     Default: Software.Application, Software.Operating System, Software.COTS, Software. Database, Software.Application Server, Hardware, Network.Port, Software, Network. Network, Interface Card, Hardware.Storage

   - **deviceXXXRelationships**
     Specifies the list of CMDB CI relationship types. CA SDM Connector queries the CI to obtain its device properties based on the relationship type.
     Default: runs, runs on, hosts, is hosted by, contains, is contained by.

   - **domsrv_name**
     Specifies the Domserver name to which the CA SDM Connector sends queries and registers for change notifications.
     Default: Primary server name.
     Format: Domsrv name specified for the Object Manager during the CA Service Desk Manager configuration.

   - **database query parameter size**
     Specifies the CA SDM database parameter list size (integer only) in the where clause query. For more information about the database parameter list size, see your database documentation.

   - **childtoparent**
     Specifies the relationship of the service CI and associated CIs. In CMDB, you can configure a service CI for either consumption or composition. If configured for consumption, the

service CI is the provider to consumers and the associated CIs are dependents in the service graph. If the service CI is configured for composition, the service is the ultimate dependent and the provider CIs impact the service.
Specify True if the service CI is configured for composition (child-to-parent).
Specify False if the service CI is configured for consumption (parent-to-child).

Note: For more information about configuring CI services, see the Configuration Items (see page 2470)

- **exclude_usm_ci_types**
  Specifies the USM entity name that the CA SDM Connector excludes from processing. You can exclude any CMDB supported CI type.
  Default: Incident, Problem, Request, Change Order, Alert

- **exclude_cmdb_relationship_types**
  Specifies the CMDB relationship types that the CA SDM connector excludes from processing. (For each relationship type, provide both Provider-to-Dependent and Dependent-to-Provider attributes separated by comma (,)).

- **class**
  Specifies the CMDB class which refers to the service CI type (separated by comma (,)).
  Default: Business Service, Infrastructure Service, Other Service

- **family**
  Specifies the CMDB family which refers to the service CI type (separated by comma(,)).
  Default: Enterprise Service

- **open_incident_threshold**
  Specifies the threshold value for the total number of open Incidents per service (including the graph CIs) and a "Too Many Open Incident" alert is sent to CA SOI.
  Default: 1

- **Password**
  Specifies the password that is associated with the CA SDM user.

- **User name**
  Specifies the user name for connecting to CA SDM.
  Default: The value entered during installation

- **window_offset**
  Specifies the offset value which is used to calculate the predicted maintenance windows and an alert is sent to CA SOI. The CA SDM Connector will not alert CA SOI about the predicted maintenance windows until the next day from the present time.
  Default: 1440 (one day in minutes).

- **enable_twa**
  Specifies whether the incoming CIs and CI relationships should be saved to TWA or to CMDB.
  Default: false (The data is loaded in the CMDB module of CA SDM)

- **excluded_activity_types**
  Specifies the activities in CA SDM that the CA SDM Connector excludes from publishing to the Catalyst. Provide the activity codes separated by comma (,).
  Default: INIT

- **time_reporting_min_allowed_value**
  Specifies the minimum value (in seconds) to be entered for the time spent on any activity in CA SDM.
  Default: 180

- **enable_SDI**
  Specifies whether CA SDI functionalities can be accessed while using the CA SDM connector. Enter **true** to enable the use of CA SDI.

- **scope_enabled_relationship_types_startup**
  Specifies to publish the relationship scopes of the selected property at the startup or restart of CA SDM. Provide the property values separated by comma (,).

  Important! Ensure that you provide only the CA SDM ProviderToDependent relationship type as the property value, irrespective of the childtoparent value. For example, financially belongs to.

5. Import the CA SDM server certificate to the client-truststore.jks keystore file located under $CATALYST_HOME\registry on the CA SDM server. The password for the keystore is located in the $CATALYST_HOME\registry\repository\conf\axis2.xml file.

6. Set the NX.env file on the CA SDM server to the following value:

   ```
   @NX_SERVLET_SERVER_URL=https://sdm_server_host:8443
   ```

7. Restart the CA SDM Connector Container.
   The changes are applied and the configuration is updated.

(Optional) Add CI Families to USM Types

This topic contains the following information:

Important! Adjustment of the Service Desk Policy is a customization, and not specifically supported by CA Support.

To add a CMDB family to a USM type, enter the family name in the configuration file and policy file.

Follow these steps:

1. Locate the USM-CMDB.xml configuration file in the following directory:

   ```
   CATALYST_HOME/container/resources
   ```

2. Add the CI families to the file and save your changes.

3. Launch the CA Catalyst Registry UI by entering the following URL:

   ```
   https://<registryserver:port>/registry/carbon/admin/login.jsp
   ```

4. Locate the ServiceDeskManager_policy.xml file in the following directory:

   ```
   /topology/physical/<NODE-NAME>/modules/policy
   ```

   Note: <NODE-NAME> displays the host name where you installed the CA SDM Connector.

5. Add the CI families to the file and save your changes.

6. Restart the CA Catalyst Container service running on the CA SDM Connector host.

Example Add the Hardware.TestSystem CMDB Family to the ComputerSystem USM Type

The following example shows how to add the Hardware.TestSystem CMDB family to the ComputerSystem USM type.

Follow these steps:

1. Open the USM-CMDB.xml configuration file and complete the following steps to add the CMDB to the file:

   a. Click Edit as Text.
   The list of USM names and CMDB families appear.

   b. Locate "ComputerSystem" and add the Hardware.TestSystem family delimited by a comma as shown in the following example:

   ```
   <usm name="ComputerSystem" cmdbFamilies="Hardware.Server,Computer,
   Hardware.TestSystem" cmdbClasses="*" />
   ```

   c. Click Save Content.

2. Launch the CA Catalyst Registry UI by entering the following URL:

   ```
   https://<registryserver:port>/registry/carbon/admin/login.jsp
   ```

3. Open the ServiceDeskManager_policy.xml file and complete the following steps to add the CMDB family to the file:

a. Click Edit as Text.

b. Locate outval="ComputerSystem" and add the Hardware.TestSystem family as shown in the following example:

```
<Field input="familyName" pattern="^Hardware.Server$|^Hardware.
Mainframe$|^Hardware.Workstation$|^Hardware.Virtual Machine$|Hardware.
TestSystem" output="eventtype" outval="ComputerSystem" />
```

c. Navigate to EventClass name="ComputerSystem" as shown in the following example:

```
<EventClass name="ComputerSystem" extends="GenericIPDevice">
```

d. Locate outval="GenericIPDevice" and add the Hardware.TestSystem family as shown in the following example:

```
Field input="familyName" pattern=" ^Hardware.Server$|^Hardware.
Mainframe$|^Hardware.Workstation$|^Hardware.Printer$|^Hardware.Virtual
Machine$|^Network.Router$|^Network.Switch$|^Network.Hub$|Hardware.
TestSystem" output="eventtype" outval="GenericIPDevice"
```

e. Locate local.ENTITY_NR.Classify.pattern and add the Hardware.TestSystem family as shown in the following example:

```
local.ENTITY_NR.Classify.pattern.^Hardware.Server$|^Hardware.
Mainframe$|^Hardware.Workstation$|^Hardware.Printer$|^Hardware.Virtual
Machine$|^Network.Router$|^Network.Switch$|^Network.Hub$|Hardware.
TestSystem=^Hardware.Server$|^Hardware.Mainframe$|^Hardware.
Workstation$|^Hardware.Printer$|^Hardware.Virtual Machine$|^Network.
Router$|^Network.Switch$|^Network.Hub$|Hardware.TestSystem
```

f. Click Save Content.

4. Restart the CA Catalyst Container service running on the CA SDM Connector host.
The Hardware.TestSystem CI family is added to the CA SDM Connector configuration.

Example Add the Hardware.CustomSystem Custom CMDB Family to the USM-A Custom USM Type

The following example shows how to add the Hardware.CustomSystem custom CMDB family to the USM-A custom USM type.

Follow these steps:

1. Open the USM-CMDB.xml configuration file and complete the following steps to add the custom CMDB family:

   a. Click Edit as Text.
   The list of USM names and CMDB families appear.

   b. Insert a new line and add the custom USM name and CMDB family name as shown in the following example:

```
<usm name="USM-A" cmdbFamilies="Hardware.CustomSystem" cmdbClasses="*" />
```

c. Click Save Content.

2. Launch the CA Catalyst Registry UI by entering the following URL:

   ```
   https://<registryserver:port>/registry/carbon/admin/login.jsp
   ```

3. Open the ServiceDeskManager_policy.xml file.

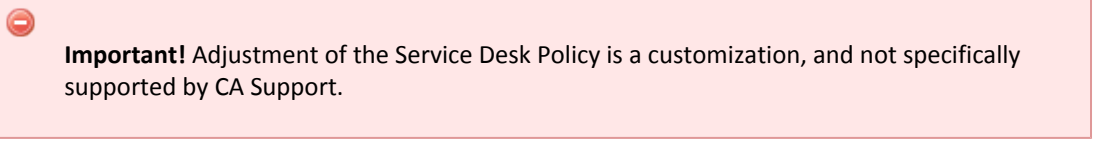
4. Click Edit as Text and add the CMDB family name, as appropriate.

5. Click Save Content.

6. Restart the CA Catalyst Container service running on the CA SDM Connector host.
   The Hardware.CustomSystem CI family is added to the CA SDM Connector configuration.

(Optional) Add CI Families with Extension Tables

Each CI family has a set of family-specific attributes that reside in an extension table in the MDB. The family-specific attributes describe the unique characteristics of each type of CI. When you configure the CA SDM Connector, you can add CI families with extension tables through a configuration file.



Important! Adjustment of the Service Desk Policy is a customization, and not specifically supported by CA Support.

Follow these steps:

1. Locate the ServiceDeskObject.xml configuration file in the following directory:

   ```
   CATALYST_HOME/container/resources
   ```

2. Add the extension table attributes to the CMDB family in the file.

3. Save the file.

4. Restart the CA Catalyst Container service running on the CA SDM Connector host.

Example Add the HAR_TESX Extension Table to the Hardware.TestSystem CI Family

The following example shows how to add the HAR_TESX Extension Table to the Hardware.TestSystem CI Family.

Follow these steps:

1. Open the ServiceDeskObject.xml configuration file for editing.
   The configuration file opens.

2. Add the extension table attributes to the CMDB family. For example, if the extension_table for the Hardware.TestSystem family is HAR_TESX, then the entry appears as shown in the following example:

```
<factory name=" HAR_TESX_extension   ">
      <attribute type="UUID" name="id"/>
      <attribute type="String" name="name"/>
      <attribute type="Date" name="last_mod_dt"/>
   </factory>
```

3. Save your changes and close the file.

4. Restart the CA Catalyst Container service running on the CA SDM Connector host.
   The HAR_TESX extension table is added to the Hardware.TestSystem CI family.

Uninstall the CA SDM Connector

You uninstall the CA SDM Connector when it is no longer required in your environment.

Follow these steps:

1. Click Start, All Programs, CA Catalyst, and uninstall in the following order:

   a. Uninstall CA SDM Connector.

   b. Uninstall CA Catalyst Container (You *must* uninstall the CA Catalyst Container only when the CA SDM Connector is installed standalone and not installed with any CA Catalyst component).

2. If you have installed the CA SDM Connector and CA Catalyst on different computers, complete the following step to delete the CA SDM node from the CA Catalyst Registry UI:

   Important! Perform this deletion step only if no other connectors are installed on the same container containing CA SDM Connector.

   a. Delete the Catalyst folder from the machine where CA SDM connector is installed.

   b. (Applicable for CA Catalyst Container r3.2) Delete the CA SDM node from the CA Catalyst Registry UI.

3. (Applicable for CA Catalyst Container r3.2) If you have installed the CA SDM Connector and CA Catalyst on the same computer, delete specific files from the CA Catalyst Registry UI after uninstalling the CA SDM Connector. Complete the following steps:

   a. Delete the ServiceDeskManagerConnector.conf and ServiceDeskManagerConnector.xml files from the following directory:

      ```
      \topology\physical\<CA_Catalyst_Server>\modules\configuration\
      ```

   b. Delete the ServiceDeskManager_policy.en, ServiceDeskManager_policy.xml, ServiceDeskManager_policySB.en, and ServiceDeskManager_policySB.xml files from the following directory:

```
\topology\physical\<CA_Catalyst_Server>\modules\policy\
```

c. Click the connector-modules.xml file name from the following directory:

```
\topology\physical\<CA_Catalyst_Server>\
```

d. Complete the following steps to edit the connector-modules.xml file.

i. Click Edit as Text.

ii. Delete the lines from the <feature name="ServiceDeskManager-connector"...> tag to the </feature> tag.

iii. Delete the lines from the <feature name="Slump...> tag to the </feature> tag.

iv. Click Save Content.

e. Click the startup.properties file name from the following directory:

```
\topology\physical\<CA_Catalyst_Server>\
```

f. Complete the following steps to edit the startup.properties file.

i. Click Edit as Text.

ii. Delete the Slump;12.7,ServiceDeskManager-connector;3.2.0 text.

iii. Click Save Content.

4. (Applicable for CA Catalyst Container r3.2) Revert CA Catalyst Server Configuration Steps (see page 543)

5. (Applicable for CA Catalyst Container r3.2) Restart the CA Catalyst Container service on the CA Catalyst server.
The CA SDM Connector is uninstalled.

Revert CA Catalyst Server Configuration Steps

The steps that the CA SDM Connector installation performs to configure the CA Catalyst server *must* revert to its original state. Complete the following steps:

- Remove the Reconciled Instance for CMDB (see page 543)
- Remove the Synchronization Policy for the Custom Reconciled Instance (see page 544)
- Remove the Inbound Filter Used for Suppressing the CMDB Projection Updates (see page 545)
- Remove the Customized Correlation Rules for the ProvisionedSoftware (see page 546)

Remove the Reconciled Instance for CMDB

To complete the CA SDM Connector uninstallation, remove the reconciled instance that is created for CMDB. For more information about reconciled views, see the *CA Catalyst Administration Guide*.

Follow these steps:

1. Log in to the CA Catalyst Registry UI and click the reconciledViews.xml file name from the following directory:

   ```
   \topology\physical\<CA_Catalyst_Server>\reconciler
   ```

2. Click Edit as Text.

3. Delete the following code from the file:

   ```
   <reconciledView>
       <instanceName>CMDB-view</instanceName> <defaultSheetURL>registry:///topology
   /physical/${catalyst.container.name}/reconciler/cmdb_defaultsheet.xml<
   /defaultSheetURL>   <existenceURL>registry:///topology/physical/${catalyst.
   container.name}/reconciler/existenceSourcesOfTruth.xml</existenceURL>
   <!--     The default correlation rules do not update the co-relatable
   attributes across MDRs, for example, serviceName of Service CI type. The
   <handleDecorrelation/> tag allows the catalyst to update such co-relatable
   attributes -->
   <handleDecorrelation />
   </reconciledView>
   ```

4. Click Save Content.

5. Click the reconciler folder from the path on the top pane to navigate to the /topology/physical /<CA_Catalyst_Server>/reconciler directory.

6. Locate the cmdb_defaultsheet.xml registry file.

7. Click Actions, Delete.
   The reconciled instance for CMDB is removed.

Remove the Synchronization Policy for the Custom Reconciled Instance

To complete the uninstallation of the CA SDM Connector, remove the synchronization policy that is created for the custom reconciled instance.

Important! If you reinstall the CA SDM Connector without removing the synchronization policy during the uninstallation, the file containing the policy is appended with duplicate policies. If these duplicate policies exist, the CA SDM Connector does *not* work properly.

Follow these steps:

1. Log in to the CA Catalyst Registry UI and click the plannerpolicy.xml file name from the following directory:

   ```
   \topology\physical\<CA_Catalyst_Server>\synchronizer
   ```

2. Click Edit as Text.

3. Delete the following code from the file:

```
<tns:plannerPolicy id="CMDB-sync">
    <tns:plannerPolicyConfig xsi:type="tns:InnerPlannerPolicyConfig">
      <tns:reconciledInstanceName>CMDB-view</tns:reconciledInstanceName>
      <tns:mdr>
        <tns:MdrProduct>CA:00020</tns:MdrProduct>
      </tns:mdr>
    </tns:plannerPolicyConfig>
  </tns:plannerPolicy>
```

4. Click Save Content.
   The synchronization policy is removed.

Remove the Inbound Filter Used for Suppressing the CMDB Projection Updates

To complete the uninstallation of the CA SDM Connector, remove the inbound filter that is added to suppress the updates from the CMDB projections.

Important! If you reinstall the CA SDM Connector without removing the Inbound filter during the uninstallation, the file containing the filter is appended with duplicate filters. If these duplicate filters exist, the CA SDM Connector does *not* work properly.

Follow these steps:

1. Log in to the CA Catalyst Registry UI and click the plancontrol.xml file name from the following directory:

   ```
   \topology\physical\<CA_Catalyst_Server>\synchronizer
   ```

2. Click Edit as Text.

3. Locate the following line between the <planControl> and </planControl> tags:

   ```
   <defaultAction defaultBehavior="send">
   ```

4. Delete the following code that is added before the <defaultAction defaultBehavior="send"> line:

   ```
   <filter name="blockCMDBUpdates">
       <condition>
           <operationSet shouldMatch="true">
               <operation>update</operation>
           </operationSet>
         <xpath>
           <namespace value="http://ns.ca.com/2009/07/usm-core" prefix="usm"/>
           <path>//*[local-name()='MdrProductLastUpdated']</path>
           <value>CA:00020</value>
         </xpath>
       </condition>
       <action defaultBehavior="drop" />
   ```

```
</filter>
```

5. Click Save Content.
   The inbound filter is removed.

Remove the Customized Correlation Rules for the ProvisionedSoftware

To complete the uninstallation of the CA SDM Connector, remove the customized correlation rules that are assigned for the ProvisionedSoftware.

Follow these steps:

1. Log in to the CA Catalyst Registry UI and click the correlation.properties file name from the following directory:

   ```
   \topology\physical\<CA_Catalyst_Server>\correlation
   ```

2. Click Edit as Text.

3. Add the comment character (#) at the beginning of following line:

   ```
   ruleForInstanceNameComparision=registry:///topology/logical/tenant0/usmschema
   /InstanceNameRules.json
   ```

4. Click Save Content.

5. If you have added a custom content in the InstanceNameRules.json file that you need for some other integration, then complete the following steps:

   a. Browse to the following directory:

      ```
      \topology\logical\tenant0\usmschema\InstanceNameRules.json
      ```

   b. Locate, edit, remove the following line in the InstanceNameRules.json file:

      ```
      "ProvisionedSoftware":{"OR":["InstanceName",{"AND":["ProductName",
      {"ANDALLEXIST":["DeviceDnsName","SoftwarePathUrl"]}]}]}
      ```

   c. Click Save Content.

   The customized correlation rules are removed.

Step 5 - Finalize the Integration with the Common Components

If one of the product installed is integrated with any common component, for example CA Process Automation then all the other products are also integrated with the same CA Process Automation. A new product installed is automatically integrated with all the existing products.

Note: Restart the services for CA Asset Portfolio Management, CA Service Desk Manager, and CA Service Catalog for auto-integration changes to come into effect after installing these products.

Auto-Integration Considerations:

Consider the following, if you are integrating:

- **CA EEM and CA Process Automation Considerations:** If you have installed CA EEM and CA Process Automation and integrate one or more CA Service Management products with these common components, ensure that you provide the same CA EEM information that you provided while installing CA Process Automation for auto-integration to be successful.

- **CASM_Policy File**: Do not modify or edit the CASM_Policy file from **CA SDM**, **Administration**, **SOAP Web Services Policy**, **Policies**, **CASM_Policy File**. If you modify the file, generate a new CASM_policy file and manually copy this file from the CA SDM installation directory to the installation directory of all CA Service Management products.

Depending upon your deployment, see the following sections for some additional manual steps to be performed to finalize the integration:

- Integrate CA Asset Portfolio Management with the Common Components (see page 547)
- Integrate CA Service Desk Manager with the Common Components (see page 548)
- Integrate CA Service Catalog with the Common Components (see page 553)

Integrate CA Asset Portfolio Management with the Common Components

The integration between CA Asset Portfolio Management and all the common components is completely automated. You do not have to perform any manual steps to finalize this integration.

However, if you are migrating from CA Business Intelligence 3.3 to 4.1, you have to update the custom universe as follows:

Important! This step applies only if you are migrating from CA Business Intelligence 3.3 to CA Business Intelligence 4.1.

If you have Custom Universe based on the OOTB Universe, refresh the link with CA Service Management 14.1 Universe.

1. Launch Universe Design Tool from the machine where CA Business Intelligence Release 4.1 SP3 client tools are installed.

2. Copy the backup Custom Universe to this machine.

3. Click File, Open.

4. Click File, Parameters.

5. Click the Links Tab

6. From the Name column, click the universe of your product,
   The Change Source button is enabled.

7. Click the Change Source button.

8. Select the location of the universe file.

   Note: The .unv file is typically located in the CA Universes folder.

9. Click Open, OK.
   The universe link is updated.

10. Export the custom universe.

Integrate CA Service Desk Manager with the Common Components

After the auto-integration steps performed by the CA Service Management installer, you need to perform few manual steps to finalize the integration of CA SDM with other components or products. Perform the following integration steps, depending on the products that you have selected for integration:

- Integrate CA Service Desk Manager with CA EEM on Solaris (see page 548)
- Integrate CA Service Desk Manager with CA Business Intelligence (see page 549)

Integrate CA Service Desk Manager with CA EEM on Solaris

If you are planning to auto-integrate CA SDM with CA EEM on Solaris, install the CA SDM Secondary or Application Server on Windows or any other Operating System other than Solaris. If you are planning to upgrade CA SDM on Solaris to CA Service Management, upgrade the CA SDM Primary or Background server. Move the bopuath_nxd authentication module daemon to the Secondary Server. Complete the following based on your CA SDM configuration:

- Move the Authentication Module Daemon for CA SDM Conventional Configuration (see page 548)
- Move the Authentication module Daemon for CA SDM Advanced Availability Configuration (see page 549)

Move the Authentication Module Daemon for CA SDM Conventional Configuration

On the CA SDM Conventional Setup, complete the following:

1. Upgrade CA SDM Primary Server to CA Service Management.
   or
   Install CA SDM Secondary on Windows.
   You can perform a fresh CA SDM Installation or upgrade an earlier CA SDM release to CA Service Management.

2. Log in to CA SDM web user interface as an administrator on the Primary server with srvcdesk credentials of the local host.

3. Navigate to System, Configurations on the Administration tab.
4. Click Create New to add the primary server details.
5. In the Host Name field, specify the primary host name for the configuration. Click Save.
6. On the Configuration Detail page, select the Additional Processes tab.
7. Select and edit the Login User Authentication and in the Update Process page provide the secondary server name.
8. Launch the *pdm_configure* on the Primary Server.
   The Config Options page drop-down has the last configuration that you created. Select the configuration and click Finish.
   After successful configuration, user login is successfully authenticated by CA EEM.

Move the Authentication module Daemon for CA SDM Advanced Availability Configuration

For CA SDM Advanced Availability, move the bopauth_nxd authentication daemon from the background server to any other server (such as application server). Complete the following:

Follow these steps:

1. Log in to the CA SDM background server web interface as an administrator.
2. Select the Administration tab. Expand Options Manager, Security.
3. Click *the bopauth_nxd_host* entry in the Options List. Click Edit.
4. Select the host name of the target server from the Option Value drop-down list. Click Save.
5. Restart the background server after changing the default value of *bopauth_host*.
6. Start version control as a client on the application server using the following command:
   pdm_ver_nxd -c
7. Restart the application server.
   You have successfully configured the redirection of authentications requests to an external server.
   Note: By default, the authentication module runs on the background server.

Integrate CA Service Desk Manager with CA Business Intelligence

This step loads the CA SDM universe and reports and creates groups. The step also optionally creates one user for each group and establishes group authorizations.

(For Linux/ UNIX/ AIX/ Solaris) After CA SDM installation, you need to create srvcdesk user in CA Business Intelligence Release 4.1 SP3 and assign it to the following groups manually:

- Change Manager
- Customer Service Manager

- Incident Manager
- Knowledge Analyst
- Knowledge Manager
- Problem Manager
- Service Desk Manager
- Support Automation Admin
- Support Automation Analyst

Follow these steps:

1. Launch the CA Service Management installer.
2. Select **CA Business Intelligence (CA BI) Configuration for CA Service Desk Manager** option from the **Select the required Installer** screen.

   Depending on the server where you run CA Business Intelligence configuration, the configuration performs the following tasks and you need the following DNS:

   - (Server where CA Business Intelligence 4.1 SP3 is only installed) Configuration imports the OOTB Universe, Reports, Groups/Users and installs 32 bit ODBC or 64 bit ODBC Client. Create 32bit/64bit DSNs pointing to the CA SDM machine.
   - (Server where CA Business Intelligence 4.1 SP3 and CA SDM are installed) Configuration imports the OOTB Universe, Reports, Groups/Users and installs 64 bit ODBC Client. Create 64bit DSN pointing to CA SDM machine.
   - (Server where CA Business Intelligence 4.1 SP3 and Client Tools are installed) Configuration imports the OOTB Universe, Reports, Groups/Users and installs 32 bit ODBC /64 bit ODBC Client. Create 32bit/64bit DSNs pointing to CA SDM machine.
   - (Server where CA Business Intelligence 4.1 Client Tools is installed) Configuration installs 32 bit ODBC Client. Create 32bit DSN pointing to CA SDM machine.
   - (Server where CA Business Intelligence 4.1 Client Tools and CA SDM are installed) Configuration does not perform any action. Required 32 bit ODBC Client and DSN are already available.

3. Complete the fields on the CA Business Intelligence configuration UI. If you installed CA Business Intelligence on a different computer than CA SDM, the following fields appear on the CA Business Intelligence configuration:

   Service Desk Primary Host: Provide the host name of the CA SDM server depending on your configuration:

   - **For conventional:** primary server

- **For advanced availability:** application server

ODBC Port: Specifies the port number of the CA SDM ODBC driver. **Recommended:** 19987.
ODBC Install Location: Specifies the custom location for the ODBC installation when it is different from the default location.

4. Verify the CA Business Intelligence configuration.

Configure Failover Settings

This process is only applicable for advanced availability configuration. If multiple application servers are configured, you can configure failover settings. You configure failover to redirect active user sessions to the other application server. You can also configure load balancing between multiple application servers.

Follow these steps:

1. Invoke the command prompt as an administrator.
2. Execute odbcad32.exe from the following location on the CA Business Intelligence server:
   - (For 32bit DSN) C:\Windows\System32
   - (For 64bit DSN) C:\Windows\SysWOW64

   The DataDirect OpenAccess SDK ODBC Driver Setup dialog opens
3. Enter the application server details in the **General** tab.
4. Enter the alternate application server details in the **Failover** tab with the following syntax: (Host=AppServer1:Port=19987,Host=AppServer2:Port=19987,..)
5. Select **Load Balancing** to distribute the load among the server. The load is balanced between servers whose details are provided in the **General** tab and the **Failover** tab. The servers are picked randomly.

   Note: Select Force SQL_DRIVER_NOPROMPT for failover or load balancing configuration.

6. Click **Apply** and **OK**.
   You have configured the post configuration settings for the advanced availability configuration.

How to Configure Date Range Values and Join Parameters

After you install CA Business Intelligence, complete the following tasks:

- Configure the date range values so that the date range filters in CA Business Intelligence work correctly.

- Configure the join parameters so that universe outer joins are supported.

Follow these steps:

1. On the computer on which CA Business Intelligence server has been installed, navigate to the following location:

   ```
   C:\Program Files (x86)\CA\SC\CommonReporting4\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\odbc\extensions\qt
   ```

2. Using a text editor, open the odbc.prm file and navigate to the <Configuration> section. Locate the following line to configure date range values:

   ```
   <Parameter Name="USER_INPUT_DATE_FORMAT">{\d 'yyyy-mm-dd'}</Parameter>
   ```

3. Modify the line to include "hh:mm:ss am/pm" as shown in the following example:

   ```
   <Parameter Name="USER_INPUT_DATE_FORMAT">{\d 'yyyy-mm-dd hh:mm:ss am/pm'}</Parameter>
   ```

4. Open odbc.prm from the Program Files (x86)\CA\SC\CommonReporting4\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\odbc directory.

5. Locate the following line to configure join parameters:

   ```
   <Parameter Name="EXT_JOIN">NO </Parameter>
   ```

6. Locate the following and replace NO with YES:

   ```
   <Parameter Name="FULL_EXT_JOIN">NO</Parameter>
   <Parameter Name="LEFT_EXT_JOIN">NO</Parameter>
   <Parameter Name="RIGHT_EXT_JOIN">NO</Parameter>
   ```

7. Add the following three lines after the OUTERJOINS_GENERATION parameter:

   ```
   <Parameter Name="LEFT_OUTER"></Parameter> <Parameter Name="RIGHT_OUTER"></Parameter> <Parameter Name="OUTERJOINS_COMPLEX">Y</Parameter>
   ```

8. Save the odbc.prm file.

9. Restart the Business Objects Enterprise services.
   Date range values and join parameters are configured. Date range filters work with CA Business Intelligence and universe outer joins are supported.

Update the Custom Universe Link

Important! This step applies only if you are migrating from CA Business Intelligence 3.3 to CA Business Intelligence 4.1.

If you have Custom Universe based on the OOTB Universe, refresh the link with CA Service Management 14.1 Universe.

1. Launch Universe Design Tool from the machine where CA Business Intelligence Release 4.1 SP3 client tools are installed.
2. Copy the backup Custom Universe to this machine.
3. Click File, Open.
4. Click File, Parameters.
5. Click the Links Tab
6. From the Name column, click the universe of your product,
   The Change Source button is enabled.
7. Click the Change Source button.
8. Select the location of the universe file.

   Note: The .unv file is typically located in the CA Universes folder.

9. Click Open, OK.
   The universe link is updated.
10. Export the custom universe.

Integrate CA Service Catalog with the Common Components

After you install CA Service Catalog and the common components, review the following sections to understand how to integrate the common component with CA Service Catalog

- Integrate CA Service Catalog with CA EEM (see page 553)
- Integrate CA Service Catalog with CA Process Automation (see page 553)
- Integrate CA Service Catalog with CA Business Intelligence (see page 554)

Integrate CA Service Catalog with CA EEM

CA EEM is a mandatory component for CA Service Catalog. Hence, CA EEM is automatically integrated with CA Service Catalog.

Integrate CA Service Catalog with CA Process Automation

After the CA Process Automation processes are loaded and configured, update the CA Service Catalog login credentials in the CA Process Automation Dataset, to complete the integration between the two products. For more information, see the Integrate CA Service Catalog with CA Service Desk Manager (see page 560) topic.

Integrate CA Service Catalog with CA Business Intelligence

Follow these steps after you have installed both CA Service Catalog and CA Business Intelligence, to complete the integration between the two products:

Step 1 - Update the Custom Universe Link

Important! This step applies only if you are migrating from CA Business Intelligence 3.3 to CA Business Intelligence 4.1.

If you have Custom Universe based on the OOTB Universe, refresh the link with CA Service Management 14.1 Universe.

1. Launch Universe Design Tool from the machine where CA Business Intelligence Release 4.1 SP3 client tools are installed.
2. Copy the backup Custom Universe to this machine.
3. Click File, Open.
4. Click File, Parameters.
5. Click the Links Tab
6. From the Name column, click the universe of your product,
   The Change Source button is enabled.
7. Click the Change Source button.
8. Select the location of the universe file.

   Note: The .unv file is typically located in the CA Universes folder.

9. Click Open, OK.
   The universe link is updated.
10. Export the custom universe.

Step 2 - Update the CA Service Catalog Universe Connection

Important! If both your CA Service Catalog and CA Service Desk Manager are configured to use the same instance of CA Business Intelligence server, and the date format in odbc.prm file is changed to the CA SDM date format, perform the following steps.

The following procedure applies to MS SQL Server only

Update the CA Service Catalog Universe connection Database Middleware after you run the CA Service Management installer to integrate CA Service Catalog with CA Business Intelligence. In the following procedure, you update the connection Database Middleware for MS SQL Server 2008.

1. Log in to the Universe Design tool.
2. Go to **File**, **Import**.
3. Navigate to CA Universes, CA Service Catalog.
4. Go to **File**, **Parameters**.
5. Click **Edit** to edit the login parameters in the **Edit CA SLCM connection** screen.
6. Click **Back**.
7. Navigate to Microsoft, MS SQL Server 2008, ODBC Drivers to select the Data Access driver.
8. Click **Next**.
9. Provide the appropriate MDB credentials and test the Connection.
10. Click **Next**.
11. Click **Next**, **Finish**.
12. Click **OK** to close the Parameters window
13. Click **File**, **Save**.
14. Click **File**, **Export**.
15. Navigate to CA Universes, CA Service catalog
16. Click OK
17. Click OK when you see the message.
    You have updated the CA Service Catalog Universe connection Database Middleware for MS SQL Server 2008. Follow a similar procedure for other supported versions of MS SQL Server.

The following procedure applies to Oracle only

Update the CA Service Catalog Universe connection Database Middleware after you run the CA Service Management installer to integrate CA Service Catalog with CA Business Intelligence. In the following procedure, you update the connection Database Middleware for Oracle.

1. Log in to the Universe Design tool.
2. Go to **File**, **Import**.
3. Navigate to CA Universes, CA Service Catalog.
4. Go to **File**, **Parameters**.
5. Click **Edit** to edit the login parameters in the **Edit CA SLCM connection** screen.
6. Click **Back**.
7. Navigate to Oracle 11, Oracle ODBC Drivers to select the Data Access driver.
8. Click **Next**.
9. Provide the appropriate MDB credentials and test the Connection.
10. Click **Next**.
11. Click **Next**, **Finish**.
12. Click **OK** to close the Parameters window
13. Click **File**, **Save**.
14. Click **File**, **Export**.
15. Navigate to CA Universes, CA Service catalog
16. Click OK
17. Click OK when you see the message.
18. Update the oracle.prm file at <CABI_Home>\SAP BusinessObjects Enterprise XI 4.0 \dataAccess\connectionServer\odbc\extensions\qt as follows:

    a. Replace <Parameter Name="USER_INPUT_DATE_FORMAT">'dd-Mmm-yyyy'< /Parameter> with existing USER_INPUT_DATE_FORMAT tag.

    b. Restart the Apache Tomcat for BI 4 and Server Intelligence Agent services in Central Configuration Manager.

    You have updated the CA Service Catalog Universe connection Database Middleware for Oracle.

Step 3 - Configure Trusted Authentication

Configure CA Service Catalog and CA Business Intelligence to use trusted authentication for the integration between the two products. Trusted authentication provides Single Sign-On. Single Sign-On enables CA Service Catalog users to access the Launch Pad application of CA Business Intelligence directly from the CA Service Catalog GUI.

CA Service Catalog uses standard CA Business Intelligence login if trusted authentication is not set up or if it is not working properly.

Note: The following login methods do *not* apply to CA Business Intelligence: CA EEM token, CA SiteMinder Integration, and NTLM authentication on Windows.

Follow these steps:

1. Log on to the CA Business Intelligence Central Management Console as a user with administrative rights.
2. Go to **Manage**, **Authentication** area of the Central Management Console.
3. Click the **Enterprise** tab.
4. Check **Trusted Authentication is Enabled** to enable trusted authentication.
5. Click **New shared secret** and you see that **Download Shared Secret** is enabled.

   Note: The CA Business Intelligence client and the Central Management Console use the shared secret password to create a trusted authentication password. The value of this password and the frequency with which you update it meet your password security standards.

6. Click **Download Shared Secret** to generate TrustedPrincipal.conf file.
7. Perform the remaining steps on *every* Catalog Component computer.
8. Open the file that is named USM_HOME\reporting\CABI\TrustedPrincipal.conf using a text editor.
9. Scroll to the following line and specify the same shared secret password that you downloaded on the CA Business Intelligence Central Management Console.

   ```
   SharedSecret=password
   ```

10. Save the TrustedPrincipal.conf file.

11. Restart the Catalog Component computer.

Important! Whenever you update the password on the CA Business Intelligence Central Management Console, make the same change to the password in the TrustedPrincipal.conf file on every Catalog Component computer.

Step 4 - Run Pre-Defined Reports

Before you run the pre-defined reports, you must create a DSN and ODBC Connection for the MDB on either SQL Server or Oracle. For more information, see Import the BIAR File (see page 3299) topic. Now, to verify the CA Service Catalog - CA Business Intelligence integration, run the pre-defined reports from CA Service Catalog.

Optionally view the pre-defined reports in localized format. To do so, set the language configuration in the **Preferences**, **Locales and Time Zone**, **Preferred Viewing Locale** section of CA Business Intelligence.

Note: Some fields remain in English even when you view reports in localized format. These fields include Request Status, Billing Status, Account Status, Account Type, and fields related primarily to payment and adjustment. In addition, in both English and localized reports, custom status values do appear in the reports; however, their descriptions do not.

Follow these steps:

1. Select **Home**, **DashBoards**, **Administration Quick Start**, **BI Launch Pad** in CA Service Catalog.
2. Click **Documents**, **Folders**, **Public Folders**, **CA Reports**, **CA Service Management, CA Service Catalog**.
3. Click **Admin Reports** or **User Reports**, as required.
   The Admin Reports folder and its reports are visible only to users who are members of the Administrator groups.
   The User Reports folder and its reports are visible only to users who are members of either the Administrator groups or the End User groups.
4. Double-click the report which you want to run.
5. Specify the parameters for your report.
6. Click Run Query and view the report.

> **Note:** In a multi-tenant (business unit) implementation, your reports display only the data of tenants to which you have access. If you run a report for an integrated product (such as CA Service Desk Manager or CA Asset Portfolio Management), but that product has not been integrated with CA Service Catalog, then the report typically fails.

(For Linux/ UNIX/ AIX/ Solaris) After CA SDM installation, you need to create srvcdesk user in CA Business Intelligence Release 4.1 SP3 and assign it to the following groups manually:

- Change Manager
- Customer Service Manager
- Incident Manager
- Knowledge Analyst
- Knowledge Manager
- Problem Manager
- Service Desk Manager
- Support Automation Admin
- Support Automation Analyst

Step 6 - Finalize the Integration with the Products

This section contains the following articles:

Integrate CA Asset Portfolio Management with CA Service Catalog

The integration between CA Asset Portfolio Management and CA Service Catalog is completely automated. You do not have to perform any manual steps to finalize this integration.

In the rare event that the integration between the two products fail, see integrate CA Asset Portfolio Management with CA Service Catalog manually (see page 3470) to troubleshoot the integration.

Integrate CA Service Desk Manager with CA Asset Portfolio Management

The integration between CA Service Desk Manager and CA Asset Portfolio Management is completely automated. You do not have to perform any manual steps to finalize this integration.

In the rare event that the integration between the two products fail, see integrate CA Service Desk Manager with CA Asset Portfolio Management manually (see page 3251) to troubleshoot the integration.

Integrate CA Service Catalog with CA Service Desk Manager

Ensure that you have selected both CA SDM and CA Service Catalog during the CA Service Management installation. After the successful installation of CA Service Management, perform the following manual steps to ensure that CA SDM and CA Service Catalog are integrated successfully.

- Update Login Credentials in CA Process Automation Dataset (see page 560)
- Create Groups in CA Service Desk Manager (see page 561)

Update Login Credentials in CA Process Automation Dataset

Important! Ensure that you have CA SDM Connector installed before you proceed with the following procedure.

Follow these steps:

1. Log in to CA Process Automation as an Administrator.
2. Click Library from the Home page.
3. Select the CA SDM folder and double click SDM_GlobalDataset.
4. Click Check out and enter the CA Service Catalog user credentials.
5. Click Save.
6. Click Check in and Close.
7. From the CA SDM SRF folder, double click HWSW_FilledFormInventory.
8. Click Check Out from the Common menu.
9. On the properties tab, enter the details of Tags field as chgcat and save.
10. Click Check in and Close.
11. From the CA Service Catalog folder, double click CA SLCM.
12. Click Check out and enter the CA Service Catalog user credentials
13. Click Save.
14. Click on Check in and close.

Important! Ensure that you have CA SDM connector installed to complete steps 15 and 16.

15. On the Configuration tab, click Modules.
16. Click Lock and double click CA ServiceDesk.
17. Give the CA SDM Host name In the Default ServiceDesk WebService URL.
18. Enter the password for Default User.
19. Save and close.
20. Click Unlock.

Create Groups in CA Service Desk Manager

Follow these steps:

1. Log in to CA SDM as an Administrator.
2. From the Administrator tab select Security and Role Management, Groups.
3. Click Create New and enter the group name for CA Service Catalog
4. Click Members, Service contracts, Auto Assignment.
5. Click Update Members.
6. Search and update the members.
7. Click OK and Save.
8. Associate this group with the following categories, and add CA SDM administrator as the assign of these categories:
   - SLCM.HWFFI
   - SLCM.SWFFI

Important! Ensure that you restart CA SDM and CA Service Catalog services after performing all the steps.

At the end of this topic, you have successfully integrated CA Service Catalog with CA Service Desk Manager.

In the rare event that the integration between the two products fail, see integrate CA Service Catalog with CA Service Desk Manager manually (see page 3255) to troubleshoot the integration.

Rules Enabled in Integrated Environment

When you auto-integrate CA Service Management components, some of the rules that are defined in the Event-Rule-Action page of CA Service Catalog are enabled. The rules that are enabled are required for the common administration components and for the integration to work properly. The rules are enabled in the following scenarios:

- When you install CA Service Management for the first time and auto-integrate the components
- When you upgrade from a standalone CA Service Catalog to the integrated environment
- When you upgrade from a standalone CA SDM to the integrated environment

When you upgrade to the integrated environment, some of the rules that you had disabled may also be enabled. We recommend that you do not disable such rules, as disabling them may cause the common administration and the integration to not work properly.

The following table gives the list of rules that are enabled:

Rule with filter that fires once for each HW request item when status goes from approval range to Pending Fulfillment (WFHWCheckAvailability)

Rule	Description
Common Administration and Content Pack Related rules	
CASM Auto Integration Rule	Rule with filter that fires once for CASM Auto Integration service
CASM Common Configuration Rule	Rule with filter that fires once for CASM Common Configuration service
CASM Contact Sync Rule	Rule with filter that fires once for each CASM Contact Sync service
CASM Create LDAP Rule	Rule with filter that fires once for each CASM add LDAP service
CASM Create Role Rule	Rule with filter that fires once for each CASM Custom Role service
CASM Custom Role Mapping Rule	Rule with filter that fires once for each CASM Custom Role Mapping service
CASM Custom Tenant Mapping Rule	Rule with filter that fires once for each CASM Custom Tenant Mapping service
CASM Import LDAP Users Rule	Rule with filter that fires once for each CASM import LDAP users service
CASM Manage LDAP Rule	Rule with filter that fires once for each CASM manage LDAP service
CASM Tenant Mapping Rule	Rule with filter that fires once for each CASM tenant onboarding service
CASM Tenant Onboarding Rule	Rule with filter that fires once for each CASM tenant onboarding service
CASM Update MT Options	Enable Multi Tenancy Options for Common Administration
CASM Update Role Rule	

Rule	Description
	Rule with filter that fires once for each CASM Create Role Service
CASM Update Tenant	Rule with filter that fires once for each CASM tenant update service
CASM Update User Rule	Rule with filter that fires once for each CASM update user service
CASM User Onboarding Rule	Rule with filter that fires once for each CASM user onboarding service
When Category is Service Management Content and Status is Canceled	Rule with filter that fires once for each service option of Service Management Content category when status updates to Canceled
When Category is Service Management Content and Status is Completed	Rule with filter that fires once for each service option of Service Management Content category when status updates to Completed
When Category is Service Management Content and Status is Pending Fulfillment	Rule with filter that fires once for each service option of Service Management Content category when status updates to Pending Fulfillment
Out-of-The-Box rules The out-of-the-box rules include multiple actions and only the actions mentioned here are enabled.	
When Category is Hardware and Status is Filled from Inventory Action: Launch HWSWFilledFromInv_SDM_SYNC SRF	Rule with filter that fires once for each HW request item when status goes to Filled From Inventory (WFHWFulfillment)
When Category is Hardware and Status is Pending Fulfillment Actions: Launch CheckAvailability SRF for Hardware Auto assign the selected asset to the user	Rule with filter that fires once for each HW request item when status goes from approval range to Pending Fulfillment (WFHWCheckAvailability)
When Category is Software and Status is Filled from Inventory Action: Launch HWSWFilledFromInv_SDM_SYNC SRF for Software	Rule with filter that fires once for each SW request item when status goes to Filled From Inventory (WFSWFulfillment)
When Category is Software and Status is Pending Fulfillment Action: Launch CheckAvailability SRF for Software availability	Rule with filter that fires once for each SW request item when status goes from approval range to Pending Fulfillment (WFSWCheckAvailability)
When Status is Submitted and Approval Process is driven by Workflow Action: Launch Approval SRF	Rule with filter that fires once for each service when a request is submitted for approval (WFAllSubmit)
Notes and Attachment Synchronization rules	

Rule	Description
When notes is added to Service Catalog request	When notes are added to CA Service Catalog request, add them to the corresponding CA Service Desk ticket
When attachment is added to Service Catalog request	When attachment is added to CA Service Catalog request, add it as a link to the corresponding CA Service Desk ticket

Implementing CA Service Catalog

The CA Service Catalog products and components are an integrated set of business applications that a Service Delivery Manager uses to manage services. To optimize your use of CA Service Catalog and the system resources that it uses, carefully prepare to install or upgrade the product. Plan for CA Service Catalog Installation by following the instructions outlined in Plan your CA Service Catalog Installation (see page 564). Determine the following:

- Understand your current Business process and requirements.
- System architecture you plan to use.
- Determine the CA EEM authentication method to use.
- The CA Service Catalog components you plan to install.
- Review the Hardware and Software Requirements.

After you complete the planning for installing CA Service Catalog , install or upgrade CA Service Catalog, using the scenario that applies to your implementation:

- Install CA Service Catalog
- Upgrade CA Service Catalog on Existing Computers (traditional upgrade)
- Upgrade CA Service Catalog on New Computers (migration-model upgrade)

Follow these steps:

- Step 1 - Plan your CA Service Catalog Installation (see page 564)
- Migrate Data Between CA Service Catalog Systems (see page 576)
- How to Upgrade CA Service Catalog (see page 579)
- Step 2 - Install CA Service Catalog (see page 590)
- Step 3 - Perform CA Service Catalog Post-Installation Tasks (see page 596)

Step 1 - Plan your CA Service Catalog Installation

CA Service Catalog products and components are an integrated set of business applications that a Service Delivery Manager uses to manage services. To optimize your use of CA Service Catalog and the system resources that it uses, prepare to install the product. Ensure that the following implementation planning tasks are implemented before you install CA Service Catalog:

CA Service Catalog 14.1 Installation Planning Checklist
▪ Determine the Type of Business Process and System Architecture (see page 565) to Use.

CA Service Catalog 14.1 Installation Planning Checklist
▪ .Determine the Failover Mechanisms and Session Management (see page 572).
▪ Determine the Number of Servers required for installation.
▪ Ensure that at least one CA EEM is installed (see page 283) in the environment.
▪ (If you have CA Business Intelligence 3.3 and if you want reporting capability) Installed CA Business Intelligence Release 4.1 SP3 (see page 285) and then install CA Service Catalog.
▪ (If you want process automation) Installed CA Process Automation (see page 292).
▪ Ensure that the required ports are open.
▪ Ensure that the hardware requirements (see page 573) are met.Ensure that at least one CA EEM is installed (see page 283) in the environment.
▪ Install the Database Server of your choice (MS SQL or Oracle Database Server). Ensure that you have the database information depending upon the database you are using: ▪ ▪ SQL Server ▪ SQL Serverdatabaseusernameandpassword ▪ SQL Server database port number ▪ Oracle ▪ Whether the Oracle database is local or remote ▪ Whether you need to create tablespaces ▪ The Net Service Name ▪ The DBAusernameandpassword ▪ The data and index tablespace name ▪ The complete path for the tablespace ▪ JDBC connection information, including the system identifier (SID) and listener port
▪ Decided to use widgets for Request Management (see page 2176).
▪ (If you plan to install Unified Self-Service with CA Service Catalog) Downloaded Liferay CE 6.1.2 GA3 edition zip file (https://www.liferay.com/downloads/liferay-portal/available-releases). ⚠ **Note:** Do not Install Liferay manually as the installer unzips the downloaded file and installs Liferay.
▪ Review the CA Service Catalog Hardware Requirements (see page 573).

Step 1a - Determine your Business Process and System Architecture to Use

This article contains the following topics:

Business Process

Implementing CA Service Catalog requires an understanding of your current business processes. Often this effort requires a discovery process to research and obtain this information. During this process, you ask questions and collate information about your business processes. Use top-down analysis to define your business and your business needs. After you determine your business needs, implement the catalog system to address them.

Review CA Service Catalog components (see page 571) to determine the catalog components that are required for your implementation.

System Architecture

The number of *catalog requests per minute* is the key criterion for determining the size of the architecture as small (see page 566), medium (see page 567), or large (see page 569). This criterion is much more important than the number of users in the system or other criteria. The higher the number of catalog requests per minute, the larger the recommended architecture.

Availability refers to the ability of an organization to deliver consistent, predictable access to applications and data.

Demonstration-Only Deployment

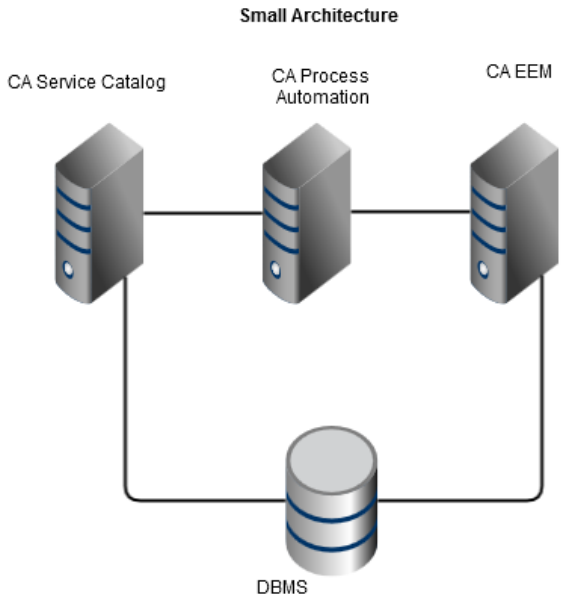
In addition to small, medium, and large architectures, CA Service Catalog also supports a standalone deployment. In a standalone deployment, all the components, including the database server, are installed on a single physical computer. This deployment is for demonstration *only* and is *not* suitable for a production environment.

Important! Verify that the DBMS is tuned for maximum performance. This directive applies to all size architectures.

Small Architecture

An small architecture can include the following servers:

- Server 1 hosts CA Service Catalog, including Service Accounting Component.
- Server 2 hosts CA Process Automation.
- Server 3 hosts the DBMS.
- Server 4 hosts CA EEM. You use configuration parameters to connect CA Service Catalog and CA Process Automation with CA EEM.



This model applies to systems with an expected average load of 1 to 10 catalog requests per minute. Clustering does *not* apply to small architecture.

Also consider, any performance-related information and other stress test data that you have from implementing previous releases of CA Service Catalog

Medium Architecture

If you expect more than a small percentage of the requests to be complex, consider moving to medium architecture. Complex requests include one or more of the following items:

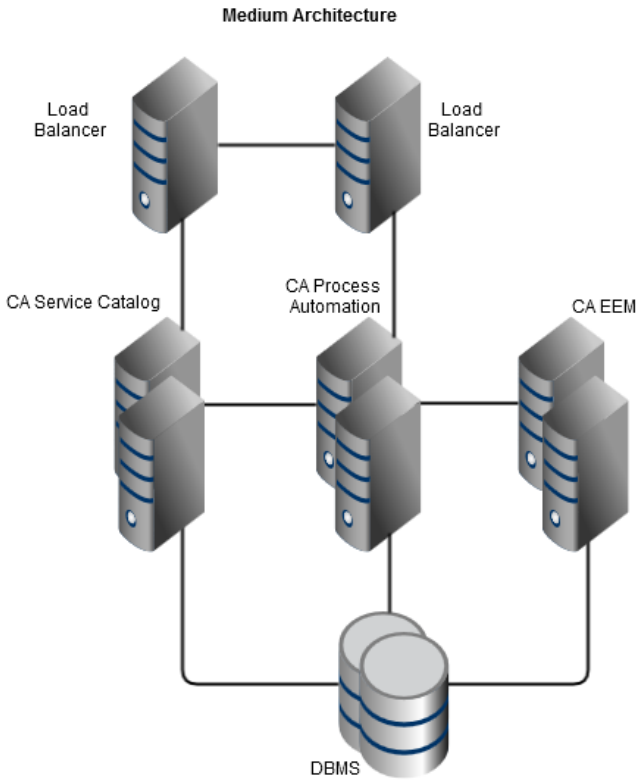
- Multiple (two or more) services or service options.
- Attachments.
- Long forms or multiple forms.
- Long web service calls or multiple web service calls.
- Multiple CA Process Automation processes.

Similarly, consider moving to a medium architecture if both of the following conditions exist:

- Your implementation includes more than 5,000 users.
- You expect more than a small percentage of these users to access the catalog simultaneously.

The medium architecture can efficiently process a load of 11-50 catalog requests per minute. The medium architecture expands the small architecture by implementing clustering and adding load balancers.

The following diagram illustrates an example of medium architecture:



The medium architecture setup is as follows: *Two clustered servers* refers to two virtual computers that are clustered.

- Two clustered servers host CA Service Catalog.
- Two clustered servers host CA Process Automation. Install and cluster CA Process Automation according to the specifications in the CA Process Automation documentation.
- One or preferably two load balancers are the front ends to the clusters for CA Process Automation and CA Service Catalog, respectively. Both the CA Process Automation and CA Service Catalog clusters require a load balancer, which can be an existing instance. CA Process Automation and CA Service Catalog can share a load balancer.
- Two clustered servers host CA EEM. CA EEM is clustered but is not used with a load balancer. We recommend clustering CA EEM to provide failover protection. You use configuration parameters to connect CA Service Catalog and CA Process Automation with the CA EEM cluster. You can increase CA EEM performance by pointing each CA Process Automation domain server to different CA EEM servers. Install and cluster CA EEM according to the specifications in the CA EEM documentation (https://wiki.ca.com/display/eem1251/Failover+Configuration).
- Two clustered servers host the DBMS. You cluster the DBMS to improve throughput and responsiveness. Verify that you cluster your DBMS using a method that improves performance. For example, using an active-active database cluster can reduce performance, especially on write operations. For more information about clustering your DBMS, see its documentation.

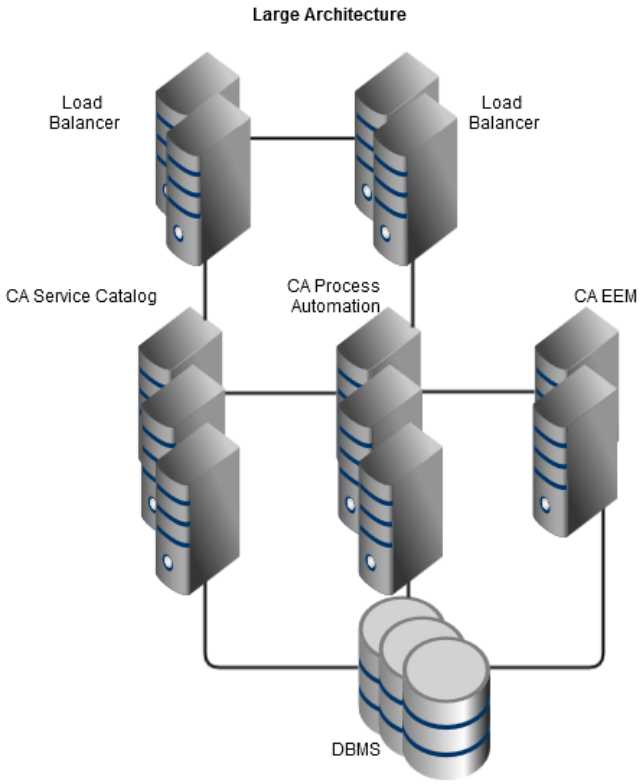
- Some virtual machine software uses scheduling algorithms that result in decreased performance when the number of CPUs increases. This performance loss is most noticeable when the virtual machines are sharing systems with other virtual machines that also have a lower number of CPUs allocated. Typically, in such cases, increasing the number of virtual machines in the cluster improves performance more than increasing the number of CPUs per virtual machine.

Large Architecture

Consider the factors for moving from a small architecture to a medium architecture. The same factors in greater magnitude can cause you to add computers and clusters to a large architecture. The large architecture can efficiently process an average load of 50 or more catalog requests per minute.

The large architecture includes multiple web server clusters and a database cluster.

The following diagram illustrates an example of large architecture:



The large architecture setup is as follows:

- Two or more clustered servers host CA Service Catalog.
- Two or more clustered servers host CA Process Automation.
- You install and cluster CA Process Automation according to the specifications in the CA Process Automation documentation. Alternatively, you install CA Process Automation on three physical computers and place them in a separate cluster.

- Two or more load balancers are the front ends to the clusters for CA Process Automation and the Catalog Component of CA Service Catalog, respectively. Both the CA Process Automation and CA Service Catalog clusters require a load balancer, which can be an existing instance.

- Two or more clustered servers host CA EEM. CA EEM does not *use* a load balancer. We recommend clustering CA EEM to provide failover protection and high availability. You use configuration parameters to connect CA Service Catalog and CA Process Automation with the CA EEM cluster. You can increase CA EEM performance by pointing each CA Process Automation domain server to different CA EEM servers.

- Two or more clustered servers host the DBMS.

- Some virtual machine software uses scheduling algorithms that result in decreased performance when the number of CPUs increases. This performance loss is most noticeable when the virtual machines are sharing systems with other virtual machines that also have a lower number of CPUs allocated. Typically, in such cases, increasing the number of virtual machines in the cluster improves performance more than increasing the number of CPUs per virtual machine.

- A filestore serves as the single location for all shared files.

Review CA Service Catalog Architecture Example (see page 570)for more information about a typical catalog implementation.

CA Service Catalog Architecture Example

This article contains the following topics:

This topic explains how to architect the CA Service Catalog system to meet the requirements for the following scenario:

I have 60,000 end users who are distributed across the country. My system is located in a centralized data center that the service provider owns. We want to integrate with CA Service Desk Manager, CA Asset Portfolio Management, and other products. Our expected load is about 100 requests per day with an average of 1000 concurrent connections. We are planning to define CA Process Automation processes to meet our requirements.

This scenario is common. Because of the variability around usage patterns and architecture there is no simple calculator that can generate sizing estimates. However, the CA Service Catalog components are dynamically scalable.

The CA Service Catalog architecture is n-tier, stateless, and web-based. Users make HTTP requests. These HTTP requests are passed to one or more application servers. The application server performs the processing logic using a pool of connections to the database. The web server can be co-located with application server instances. Also, several computational engines run independently from any user interactions; examples include the billing and SLA correlation engines. Other web servers, application servers, and computational engines can be added, as required. The database, where state is maintained, is the potential performance bottleneck. The scalability of the database platform is important. Therefore, the sizing and architecture of the MDB is the most critical factor.

Metrics

First, consider the concurrent connection metric: Because HTTP is connectionless, there is no "concurrent user" metric.

Next, consider the metric of 100 requests per day: This metric does not provide the peak usage, a critical factor. If the 100 requests are evenly distributed through the day, system impact would be minimal. However if the 100 requests are all made at the same time of day, then the system could be challenged. Also, the type of request has a direct impact on the resource utilization.

Variations

Variations in usage and architecture are important. Consider them carefully and tune your system. Adjust your tuning over time as changes in demand or system load occur, if necessary.

Business Requirements and Updates

When you are implementing CA Service Catalog, it is critical to capture accurate business requirements. Use the business requirements to formulate efficient technical architectures. Therefore, you start an implementation with a discovery phase per module to capture the business requirements. Next, you study the limitations and capabilities of the client operational infrastructure, and you formulate an efficient implementation architecture. Once you obtain all the information, you can formulate an initial sizing estimate.

Based on the possible variations in usage and architecture, organizations must start with two instances of each component. One component for fail-over and one component for load balancing. Because the components can be co-located, start with at least two server class machines in addition to the database servers. If computational engines are heavily used during peak activity times, they require their own server or servers. The usage-patterns typically change over time as the clients grow to understand the features and use them more heavily. As you discover usage patterns over time, you can dynamically add and distribute components as needed.

CA Service Catalog Components

The CA Service Catalog components are as follows:

- **Service Catalog**
  Service Catalog provides a container that consists of services for one, several, or all business units. Services are built of one or more service option groups that describe IT services and how to charge for them. The service catalog also enables an organization to model its business units or departments and manage the users accounts contained within those units. Services in the service catalog can be organized into folders. The services contain detailed information about the price of a service. Services can represent one or more metrics and can include Service Level Agreements (SLAs).
  Service Catalog provides required common functions such as management of users, business units and accounts, reporting, and event handling.

- **Service Catalog Accounting**
  Service Catalog Accounting is the financial component of CA Service Catalog. You can use it to for billing, chargeback, cost allocation, budgeting, and planning of services in the catalog.

- **Service Catalog Content**
  Service Catalog Content is a set of best practice model services to help you start your catalog quickly. Using these model services helps you better align your services with business goals, improve internal customer satisfaction, and standardize your processes to achieve greater operational efficiency.

Step 1b - Determine the Authentication Methods to use

Administrators can authenticate users in CA Service Catalog by any one of the following methods:

- CA EEM alone
- CA EEM with an external directory. For example: an LDAP directory, such as Microsoft Active Directory
- Windows NTLM authentication

You specify whether to use CA EEM standalone or with an external directory. When you use CA EEM standalone, CA EEM stores the user information and passwords in its data store. When you use CA EEM with an external directory, such as Microsoft Active Directory, the external directory stores the users and passwords in its data store. If the client system uses a Windows domain, you can configure CA Service Catalog to use NTLM authentication. NTLM authentication enables a user who has been authenticated to the domain to skip the login page.

Step 1c - Understand Failover Mechanisms and Session Management

This article contains the following topics:

Failover Mechanisms

As part of your implementation, you can perform the following tasks to provide failover mechanisms:

- Deploy CA Service Catalog in a cluster.
- If you use CA Process Automation, deploy clustering in CA Process Automation.
- Use *database* clusters. CA Service Catalog components are also compatible with database clusters which are recommended for environments experiencing heavy load.

  Note: For information about database clustering, see your DBMS documentation.

- Use a load balancer. Clustering requires a load balancer. To maximize the uptime of CA Service Catalog, include the load balancer and cluster computers in your failover plan.
- Implement clustering on the load balancer computer.
- Move user-generated files from the local file system to a filestore (see page) (a central location) on a high-availability network shared file system. CA Service Catalog maintains several user-generated files on the local file system. These files include forms and XSL and XML customizations.
- If you are using CA EEM for authentication, cluster CA EEM, using operating system level clustering.

Note: For information about clustering and implementing failover with CA EEM, see CA EEM documentation (https://wiki.ca.com/display/eem1251/Failover+Configuration).

- Improve the robustness of the hardware used in your environment, by using all applicable means, including RAID hard disks, redundant power supply, and network cards. For more information, see your hardware documentation.

Session Management

Session management is very important for performance. Use a process automation tool such as CA Process Automation to handle session management effectively.

Effective use of web service sessions is crucial for maintaining throughput as your environment scales up. Creating a web service session is a task which requires multiple invocations of authentication and authorization logic and accounts for the majority of time and effort spent when using web services. Design CA Process Automation processes and other web service clients to avoid creating extra web service sessions. Exception handling should create a session only when the exception is known to be the result of an invalid or expired session.

Step 1d - Review the Hardware Requirements

Ensure that your system meets the following hardware requirements before proceeding with the CA Service Catalog installation:

- CPU: Intel Platform —3 GHz Processor or higher (Multi-processor recommended)
- Memory: 4 GB or higher recommended. Additional 2 GB, if you plan to install Unified Self-Service.
- Hard disk: Minimum 80 GB with at least 4 GB free space

Important! For production, we strongly recommended that you install each required application on its own computer. For example, you install Catalog Component on server 1, CA Process Automation on server 2, and Accounting Component on server 3. You install the DBMS server software on server 4.

Step 1e - Verify the Prerequisites for CA Service Catalog Installation

The term *CA Service Catalog computer* means the DBMS server and any computer on which you plan to install any CA Service Catalog product or component.

The following installation considerations and requirements typically apply to all implementations.

- As a best practice, verify that all CA Service Catalog computers are *geographically collocated* - that is, are located in the same building, in the same room. Geographically collocated CA Service Catalog computers prevent possible performance problems caused by network latency.
- Record the following data for every installation of CA Service Catalog. The installation program prompts you to provide this data.

- Installation path name, if you do not want to use the default path name
  Default: C:\Program Files\CA\Service Catalog

- Startup and shutdown port numbers, if you do not want to use the default ports 8080 and 8085.

  Important! We recommend that you do *not* use port 7777 as the startup or shutdown port. Port 7777 is reserved for Java Messaging Service (JMS).

  If you must use port 7777 for the startup or shutdown port, reset the JMS port number after you have finished running the setup utility. Otherwise, port conflicts occur, and the product does not function correctly.

- No host name is needed because you install the product locally.

- Record the CA EEM Server details.

  Note: Ensure that you have at least one CA EEM in your environment because CA EEM is mandatory for CA Service Catalog.

- If you are planning to use Oracle database, ensure that you identify the system identifier (SID) and verify that the ORACLE_HOME and ORACLE_SID variables are set correctly.

- In a distributed implementation, any computer on which you install CA Service Catalog must have either your DBMS server or DBMS client installed. This requirement applies to both SQL Server and Oracle.

- When you install CA Service Catalog products and components on a network share, map a drive letter to this share. Alternatively, copy the installation image to a local folder with a short path name, for example, C:\ or C:\Temp. Run the installation programs locally from this folder.

  Note: Avoid long path names because they can cause problems during the installation process.

  The maximum length of a path name in Windows is 260 characters. If the path names exceed this limit, the installation (or upgrade) can fail. Verify that the path name where you install CA Service Catalog does not exceed this limit.

- If you want to install Unified Self-Service, we recommend that you install Unified Self-Service and CA Service Catalog on different computers.

- If you want to integrate CA Service Catalog with CA Process Automation, ensure that:

- - The CA Service Catalog computer name does not begin with a number.

- The computer name of the load balancer does not begin with a number, if you are using a load balancer for CA Service Catalog or CA Process Automation.

If you do not meet these requirements, web service calls for the integration can result in errors, for example:

```
Caused by: com.sun.xml.messaging.saaj.util.JaxmURI$MalformedURIException: Host is
not a well formed address!
```

Required Open Ports

On each host computer where you install CA Service Catalog, specify the port number for CA Service Catalog to communicate with the web server. You can change the default values during installation. If these ports are not available, have other non-conflicting port numbers available.

- 8080 and 8085 - For the Catalog Component service for communication

After the installation, if applicable, you also specify the port number for CA Service Catalog to communicate with other CA products, when you configure the integration with them.

The following port number is the default value for use by CA EEM. You cannot change it during installation.

- 5250 - for the iTechnology iGateway service

CA Service Catalog requires the following ports for communication with products and components. If you have disabled these ports, for hardening purposes or for any other reasons, enable them.

Note: For more information about how to enable ports, see your Windows documentation.

Product or Component	Default Port
CA Service Catalog startup port (includes access for CA Service Catalog and Service Accounting Component)	8080
CA Process Automation, CA Service Desk Manager, CA Business Intelligence, and other CA products that integrate with CA Service Catalog	8080
CA Service Catalog shutdown port	8085
Visualizer port for CA Service Desk Manager	9080
SQL Server server	1433
Oracle server	1521
CA EEM	5250
IMQ port of CA EEM	7676

If you are not using the default ports, verify that they are open. You do not need to open the shutdown ports for the products and components listed.

If you plan to implement clustering for CA Service Catalog, open all Apache JServ Protocol (AJP) and load balancing ports.

Decide the Service Provider Business Unit ID

During the CA Service Catalog installation, you specify a “service provider” business unit ID. This ID specifies the top level (root) business unit. All other business units are structured under the root business unit. As a best practice, specify your company domain name or a short version of your company name for this ID.

Note: After you have installed CA Service Catalog, you cannot change the business unit ID of the service provider. But, you can change the business unit login ID and the business unit name service provider.

Migrate Data Between CA Service Catalog Systems

You can migrate CA Service Catalog from one system to another system, to replicate your environment. You perform such a migration to move from a test system to a production system or as part of disaster recovery. You can also perform such a migration as part of upgrading using a migration model.

For clarity, use these terms:

- *test system* refers to all computers *from* which you are migrating
- *production system* refers to all computers *to* which you migrating

Thus, these terms describe a typical scenario where you migrate from a test system to a production system. If you are migrating for other reasons, the test system is the *source* system. The production system is the *target* or *destination* system.

This documentation assumes a multi-computer system architecture. For example, one computer for the DBMS, one computer for CA Service Catalog and Service Accounting Component and one computer for CA Process Automation. Unless indicated otherwise, *system* refers to *all* CA Service Catalog computers in your test or production, including the DBMS computer. If you are migrating one stand-alone CA Service Catalog system to another stand-alone system, ignore references to multiple computers.

Follow these steps:

- Step 1 - Verify Prerequisites for Data Migration (see page 576)
- Step 2 - Migrate the Data (see page 577)

Step 1 - Verify Prerequisites for Data Migration

Perform the following prerequisite tasks before you migrate CA Service Catalog. These tasks are required to help ensure that you can complete the migration process successfully.

1. Verify that the setup on the production system matches the setup on the test system. Verify that the production system has CA Service Catalog installed on the same number of computers as the test system. Verify that the same products and components are installed on each computer in the production system as its "matching" computer in the test system. You migrate from the old system to the new system incrementally in pairs.
   For example, suppose that the first test computer has installed CA Service Catalog, the Catalog Content, and Service Accounting Component. In that case, the first production computer must also have each of these components installed. Moreover, the production computer must not have any *additional* CA Service Catalog products and components installed.

2. Verify that the business unit ID of the service provider is *the same* in both systems.

   Important! The service provider business unit ID for the new installation *must match* the previous installation.

Verify that all computers in both systems are at the same patch level for all important software.

- Verify that the CA EEM Application Name for CA Service Catalog is the same on both the test and production systems. By default, the name is *Service Catalog*.
  If necessary, update the Application Name, on either or both systems.

- Stop the CA Service Catalog services on all CA Service Catalog computers using the Windows Control Panel.

- Back up the MDB of your *production* system and also your *test* system, on the computer where the MDB is installed. This requirement applies, regardless of whether the system is installed on one computer or multiple computers.

You have performed the prerequisite tasks for migrating CA Service Catalog.

Step 2 - Migrate the Data

You can migrate CA Service Catalog products and components from one system to another.

Follow these steps:

1. Restore the MDB database backup of the test system into your production system. During this process, select the option for overwriting the existing MDB database.

Unregister the CA EEM application that the production system uses, as follows:

1. Log in to the Global Application of CA EEM as the EiamAdmin user.
   If your systems use a different name than *Service Catalog* for the CA Service Catalog application name, use that name.

2. Select Configure, Applications, Service Catalog application and click the UnRegister button.

- Back up the CA EEM data on the CA Service Catalog computer in your test system, as follows.
  If you have multiple CA Service Catalog computers, perform this step on the *first* CA Service Catalog computer. You run this command once, regardless of how many CA Service Catalog computers your system has.

  1. Open the CA Service Catalog command prompt by clicking Start, Programs, CA, Service Catalog, Service Catalog Command Prompt.
  2. Run the following command at the command prompt:

     ```
     ant backup-eem-app
     ```

     This action generates a file that is named eem-backup.xml in the USM_HOME directory.

- Copy the following files from the test CA Service Catalog computer to the production CA Service Catalog computer.
  If you have multiple CA Service Catalog computers, perform this step on the *first* CA Service Catalog computer in each system. You copy these files once, regardless of how many CA Service Catalog computers your system has.

  - USM_HOME\seeddata.properties
  - USM_HOME\filestore folder
    This folder can exist on a different computer than the current computer. To verify its location, select Administration, Configuration, Filestore Information. As a best practice, soon after the migration, set up a single location for shared files (see page).
  - USM_HOME\eem-backup.xml

- Run the following commands on all CA Service Catalog computers in the production system, one computer at a time.

  1. Update the password of the database user (see page 1514) to ensure that CA Service Catalog continues to run efficiently throughout your environment. (see page 1511)
  2. Update the database host, password, instance, service name, or port (see page 1511) for the database, as needed.

     Important! The database host name that you specify must be different from the one used in the test system. Updating the other settings is optional.

  3. Run the ant restore-eem-app command.
     This command restores the CA EEM database from test to production, using the eem-backup.xml that you copied.
  4. Run the ant update-usm-host command.
     This command enables you to change the host name and port number for a computer running CA Service Catalog.

Important! All host names for production CA Service Catalog must be different from the ones in the test system. Updating the other settings is optional.

For more information about this command, see Update the Host Name and Port Number Using the ant Command (see page 1513) section.

- Start all CA Service Catalog services on all computers in the production system.
- Log in to CA Service Catalog in the production system. Select Administration, Configuration. Update the configuration sections for Filestore, CA Service Desk Manager Integration, and CA CMDB Integration.

Important! If your post-migration environment does *not* include any option in the list, update the configuration settings to *remove* the integration! Similarly, if your post-migration environment *does* include any of these options, perform the following step: Verify that the host names, port numbers, and other configuration data are correct for your post-migration environment. Remember that setting up a filestore location is a best practice.

- Test by verifying that the same users, services, and requests, that existed in test also exist in production.

How to Upgrade CA Service Catalog

Decide whether to perform a traditional or migration model upgrade (see page 580). Note the value of all parameters for all business units in your implementation before you upgrade. After you upgrade, set the parameters accordingly.

- If you are running CA Service Catalog 12.6 through 12.9, you can upgrade directly to the current release using *either* a traditional model or migration model upgrade (see page 580).
- If you are running CA Service Catalog 12.5, the following options apply:
  - Upgrade directly to the current release using a migration model.
  - *First* upgrade to 12.6. Next, use a traditional model to upgrade to the current release.
- You *cannot* upgrade from one DBMS to another. For example, you cannot upgrade a CA Service Catalog 12.7 installation running SQL Server to the current release of CA Service Catalog installation running Oracle.
- The installer upgrades CA Service Catalog in its existing installation directory, except in the following case: If you perform a migration model upgrade to the current release of CA Service Catalog on a 64-bit computer, CA Service Catalog is upgraded to a 64-bit application, and its default installation directory is updated accordingly. (CA Service Catalog Release 12.6 and 12.7 were supplied as 32-bit applications.)

If required, also review the Hardware Requirements (see page 573) and Installation Prerequisites (see page 573) before you proceed with upgrading CA Service Catalog.

Traditional and Migration Model Upgrades

You can upgrade CA Service Catalog to the current release using *either* a migration model or a traditional model.

- In a traditional model, you upgrade on existing CA Service Catalog computers.
- In a migration model, you install the current release of CA Service Catalog on *new* computers. When you install CA Service Catalog on the new computers, you use the Catalog database and CA EEM computers.

The migration model works as follows:

Consider this sample scenario: Your setup has Catalog Component and the Catalog database on existing Computer 1. Catalog Component and Service Accounting Component are on existing Computer 2, and CA Process Automation on existing Computer 3. Perform the following actions:

- Verify that the current release of CA Service Catalog Release supports the DBMS version on existing Computer 1.
- Verify that the DBMS client software is installed on the new computers on which you plan to run the upgrade.
- Install Catalog Component on new Computer 4, pointing to the existing Catalog database on existing Computer 1. Similarly, install Catalog Component and Service Accounting Component on new Computer 5. When you are prompted for information about the Catalog database or CA EEM, use the *existing* Catalog database and CA EEM specifications, such as the CA EEM host name and application name.
- Utilize CA Process Automation on Computer 3.

> **Note:** Do *not* upgrade or delete CA Service Catalog on existing Computer 1 until all other computers are upgraded to the current release of CA Service Catalog and are running successfully.

Follow these steps :

- Step 1 - Plan your CA Service Catalog Upgrade (see page 580)
- Step 2 - Upgrade CA Service Catalog (see page 586)
- Step 3 - Perform CA Service Catalog Post-Upgrade Tasks (see page 587)

Step 1 - Plan your CA Service Catalog Upgrade

This article contains the following topics:

Preparing for the upgrade is a required task whether you upgrade using a migration model or a traditional model.

Follow these steps:

1. Find and list all computers in your implementation that have one or more CA Service Catalog components installed. Use this list to help verify that you upgrade all required computers efficiently and in the correct sequence.

2. Stop all Windows services for your existing release of CA Service Catalog.

3. Review whether you have shared any of the folders under CA Service Catalog and Shared Components. If the folders are shared, unshare them before the upgrade and restore the share after the upgrade is finished.

4. Verify that your *user ID* is defined as an administrator with *elevated privileges* on each *applicable Windows computer*, as follows:

   - ***user ID***
     Specifies your administrative user ID for the Windows computer (*not* your user ID for CA Service Catalog).

   - ***elevated privileges***
     Specifies additional rights in Windows that are available to administrative users only. To install or upgrade CA Service Catalog, administrators require the elevated privilege named Log on as Service.

   - ***applicable Windows computer***
     Specifies a Windows computer on which you plan to install or upgrade CA Service Catalog and which supports elevated privileges for administrators.

5. Verify that your administrative user ID has Log on as Service rights on each applicable Windows computer, as follows:

   a. Click Start, All Programs, Administrative Tools, Local Security Policy, Security Settings, Local Policies, User Rights Assignment, Log on as Service.

   b. Verify that your administrative user ID is listed.

6. (Migration Model Upgrade Only) If you have an existing filestore that you want to continue using after the upgrade, perform this step. Otherwise, skip this step.
   Record the computer name and the complete pathname of the filestore. Save them for reference after the upgrade.
   For traditional upgrades, the filestore is backed up to the following location:
   C:\Program Files (x86)\CA\Service Catalog\SCA_Backup\previous_release\r12.*n*\Service Catalog
   r12.*n* is 12.6, 12.7, 12.8, or 12.9 depending on the version from which you are upgrading.

7. Perform the following actions in your current implementation:

   - Prepare the catalog database and the DBMS (see page 582)

   - Back up CA EEM data (see page 584)

8. Record any customizations that you made to XML, XSL, or other CA Service Catalog files, for example, server.xml. The upgrade program installs new versions of these files. After the upgrade, you can make the same customizations to the new versions of these files. Follow the same process for any customizations that you made to related third-party files such as Tomcat files.

9. If you have copied the installation media to a network share, map a drive letter to this share. This mapping is required because a batch file runs as part of the upgrade, and batch files cannot run from a UNC path.

You have prepared for the upgrade.

Prepare the Catalog Database and the DBMS

Prepare the Catalog database and the DBMS for the upgrade.

Follow these steps:

1. Review the contents of the Catalog database:
   - The Management Database (MDB) tables that apply to CA Service Catalog; their names typically begin with a CA_ prefix. The MDB is the common, shared database for CA Technologies products. The MDB provides the database schema for CA Service Catalog and other CA Technologies products.
   - The CA Service Catalog-specific tables; their names typically begin with a USM_ prefix. These tables are not included in the MDB.
2. Back up your existing Catalog database on the computer where it currently resides.
3. Optimize the System Change Detail tables (see page 583).
4. If applicable, on your DBMS server, upgrade your Oracle or SQL Server software to a supported version.
5. Apply all patches and other maintenance for your DBMS (SQL Server or Oracle).

Note: For more information, see your SQL Server or Oracle documentation.

6. Remove replication in your DBMS.

Important! When replication has been added, the database tables are locked from any schema changes, even if replication is turned off. As a result, the upgrade cannot run successfully. For information about how to remove replication, see your DBMS documentation. Also see that documentation for more information about how to add it again, after you have completed the upgrade.

7. Verify that the DBMS client software is installed on the computer from which you plan to run the installation program.

Optimize the System Change Detail Tables

The System Change Detail tables are important for auditing and database performance. You can optimize the System Change Detail tables by eliminating redundant or obsolete records. This procedure helps optimize the performance of the database and CA Service Catalog.

Follow these steps:

1. Determine the number of each type of record, as follows:

    a. Enter the following command to determine the number of useful records:

    ```
    select count(*) from usm_system_change_detail where old_value!=new_value
    ```

    b. Enter the following command to determine the number of obsolete records:

    ```
    select count(*) from usm_system_change_detail where old_value=new_value
    ```

    Complete the remaining steps if a significant number of obsolete records exist, especially If more obsolete records than useful records exist. Otherwise, skip the remaining steps and finish preparing the Catalog database and the DBMS.

2. Enter the following command to filter the useful records from usm_system_change_detail table into a temporary table:

    ```
    Select * into usm_system_change_detail_temp from usm_system_change_detail where old_value!=new_value
    ```

3. Drop usm_system_change_detail table, as follows:

    a. Back up the indexes and database constraints for the following tables:

    - usm_system_change_detail
    - usm_system_change_detail_ext

    Note: For more information about how to perform the backup, see your DBMS documentation. For a sample script that restores indexes and constraints, see the sample script for SQL Server that follows these steps.

    b. Drop the foreign key constraints for the usm_system_change_detail_ext table.

    c. Drop the usm_system_change_detail table.

4. Rename the usm_system_change_detail_temp table to usm_system_change_detail.

5. Use the script that you created in Step 3a to restore the indexes and database constraints for the following tables.

   - usm_system_change_detail
   - usm_system_change_detail_ext

Sample Script

The following sample script applies to SQL Server. This script backs up indexes and database constraints. You can use this script as a model for backing up the indexes and database constraints in Step 3a.

```
ALTER TABLE [dbo].[usm_system_change_detail]
ADD CONSTRAINT [XPKusm_system_change_detail] PRIMARY KEY CLUSTERED
(
[id] ASC,
[name] ASC
)
WITH
(
PAD_INDEX = OFF,
STATISTICS_NORECOMPUTE = OFF,
SORT_IN_TEMPDB = OFF,
IGNORE_DUP_KEY = OFF,
ONLINE = OFF,
ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON
)
ON [PRIMARY]
ALTER TABLE [dbo].[usm_system_change_detail]
WITH CHECK ADD CONSTRAINT [$usm_s_r00002c5700000000] FOREIGN KEY
(
[id]
)
REFERENCES [dbo].[usm_system_change] ([id])
ALTER TABLE [dbo].[usm_system_change_detail]
CHECK CONSTRAINT [$usm_s_r00002c5700000000]
ALTER TABLE [dbo].[usm_system_change_detail_ext]
WITH CHECK ADD CONSTRAINT [$usm_s_r00002c6100000000] FOREIGN KEY
(
[id],
[name]
)
REFERENCES [dbo].[usm_system_change_detail] ([id], [name])
ALTER TABLE [dbo].[usm_system_change_detail_ext]
CHECK CONSTRAINT [$usm_s_r00002c6100000000]
```

Back Up CA EEM Data

Backing up CA EEM data is a required task whether you upgrade using a migration model or a traditional model.

Important! If CA EEM is configured with high availability, perform these steps on the Primary CA EEM server.

Follow these steps:

1. Back up your existing CA EEM on the computer where it currently resides, as follows:
    a. If other CA Service Catalog components exist on the same computer, shut down their Windows services.
    b. Log in to CA EEM; on the login page, select your current CA Service Catalog release as the application instance.
2. Click Configure, EEM Server, Export Application.
3. Perform the following steps:
    a. Select all check boxes under Object List, and verify that Override the Max Search Size is *not* selected.
    If CA EEM is configured with External Directory, clear these options: Global Users, Global User Groups, Global Folders, and Global Settings.
    b. Click Export.
    c. On the File Download prompt, select a location to save the ServiceCatalog.xml file. Record the location where you saved the file, for future reference.
4. Log out of CA EEM.
5. Back up the CA EEM data on the Catalog Component computer in your test system, as follows.

    Note: If you have multiple Catalog Component computers, perform this step on the *first* (formerly *primary*) Catalog Component computer *only*. You run this command once, regardless of how many Catalog Component computers your system has.

    a. Open the CA Service Catalog command prompt by clicking Start, Programs, CA, Service Catalog, Service Catalog Command Prompt.
    b. Run the following command at the command prompt:

    ```
    ant backup-eem-app
    ```

    This action generates a file named eem-backup.xml in the %USM_HOME% directory. USM_HOME is the documentation convention that specifies the local CA Service Catalog installation directory. For 32-bit computers, the default path name is C:\Program Files\CA\Service Catalog. For 64-bit computers, the default path name is C:\Program Files (x86)\CA\Service Catalog for 32-bit installations or C:\Program Files\CA\Service Catalog for 64-bit installations.

You have backed up CA EEM data.

Step 2 - Upgrade CA Service Catalog

This article contains the following topics:

Important! If you have an existing CA Business Intelligence 3.3, review this section (see page 285) before proceeding with the CA Service Catalog upgrade. Ensure that you have prepared CA Service Catalog for upgrade (see page 580) as well.

Upgrade From Release 12.8 or 12.9

If you are upgrading from CA Service Catalog 12.8 or 12.9, use the CA Service Management Installer to install CA Service Catalog (see page 590) on all CA Service Catalog computers, in any order. Follow the prompts to complete the upgrade.

Note: If you want to use custom port numbers, specify them in the fields provided. This requirement applies even if you specified custom port numbers in the previous release.

Upgrade from Release 12.6 or 12.7

Typically, your implementation includes multiple instances of CA Service Catalog installed on multiple computers. If you are upgrading CA Service Catalog in such an environment, upgrade the computers in the correct sequence.

Follow these steps:

1. If you are upgrading in a non-clustered environment, follow this sequence:
   a. Use the CA Service Management Installer to install CA Service Catalog (see page 590) on all computers that have Accounting Component or CA Workflow installed.

      Important! The current release of CA Service Management does not support CA Workflow. However, because you cannot upgrade Service View component without upgrading CA Workflow, you run the CA Service Management Installer even on the CA Workflow computers.

   b. Use the CA Service Management Installer to install CA Service Catalog (see page 590) on all computers that have the Service View component installed.

> **Note:** In a non-clustered environment, you can upgrade the first (primary) Service View computer and the additional (secondary) Service View computers in any order.

2. If you are upgrading in a clustered environment, follow this sequence:

1. a. Determine the the first (primary) Service View computer by checking the registry entries.

   - On 32-bit systems, the registry entry for the first Service View computer is as follows:
     HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Service Catalog\View
     This key has the following value:
     PRIMARY VIEW - Yes

   - On 64-bit systems, the registry entry for the first Service View computer is as follows:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Service Catalog\View
     This key has the following value:
     PRIMARY VIEW - Yes

   b. Use the CA Service Management Installer to install CA Service Catalog (see page 590) on all computers that have Accounting Component or CA Workflow installed.

> **Important!** If one of those computers is the first Service View computer, do not upgrade it now. Instead, upgrade it after you have completed the next step.

   c. Use the CA Service Management Installer to install CA Service Catalog (see page 590) on all additional (secondary) Service View computers and then on the first (primary) Service View computer.

You have upgraded CA Service Catalog to the current release.

Step 3 - Perform CA Service Catalog Post-Upgrade Tasks

Finalizing the upgrade is the last required task when you upgrade CA Service Catalog.

Follow these steps:

1. If you upgraded to CA EEM Release 12.51 in a clustered setup, you updated the MaxKeepAliveRequests property in the Apache proxy.conf file to meet the CA EEM installation requirements. In that case, reset the MaxKeepAliveRequests property to its original value.

2. Reset the JMS port number, (see page 598)if necessary.

3. Log in to the root business unit of CA Service Catalog as a Service Delivery administrator.

4. If you are performing a migration model upgrade from CA Service Catalog 12.5, perform this step. Otherwise, skip this step.

    a. Click Catalog, Configuration, System Configuration.
    The System Configuration page appear.

    b. Set the value of the **Use Service Provider Catalog Only** option to Yes or No. You decided the value when you prepared for the upgrade (see page 580). For more information about this option, see System Configuration (see page 1461).

    Note: The value that you set applies to the entire Catalog system.

5. Verify that you and other users can log in to CA Service Catalog on the new computers. Verify that the CA Service Catalog components are working properly.

6. If you integrated CA Service Catalog with CA Service Desk Manager in the previous release, update the host computer names. Also reconfigure the other connection details between the two products.

7. If you enabled the following features in the previous release, to continue using them, enable them for this release:

    - Secure Socket Layer (SSL)
    - Windows NTLM authentication

    Note: These options are disabled by default, for both new installations and upgrades. Verify that your configuration specifications were retained and reset them, if necessary.

8. Set up shared and customized files (see page 588). This step can include re-applying customizations from the previous release and setting up the filestore, if applicable.

9. (Migration Model Upgrades Only) Uninstall (see page 626) the previous versions of CA Service Catalog products and components from the "old" CA Service Catalog computers. If you installed a new version of CA EEM, uninstall the old version of CA EEM from the old CA Service Catalog computers.

You have finalized the upgrade.

Set Up Shared and Customized Files

Setting up shared and customized files is a required task when you finalize the upgrade. For example, re-apply any customizations that you recorded for XML, XSL, or other CA Service Catalog files when you prepared for the upgrade.

Follow these steps:

1. (Multiple Catalog Component Computers) Perform the following steps:

    a. If you have not already done so, set up the filestore (the single location for shared files). Otherwise, skip this step.

    b. Click Administration, Configuration, Filestore on any Catalog Component computer. Verify that the filestore location is correct. If necessary, correct the location.

    c. Access the filestore computer and verify that the filestore folder includes the themes folder. If necessary, copy the themes folder to the filestore folder.

2. To use the old filestore location, if applicable, proceed as follows. Otherwise, skip this step.

    a. Copy the themes folder from the local filestore to the old filestore.

    b. Click Administration, Configuration, Filestore.

    c. Specify the original filestore location. You recorded this location when you prepared for the upgrade (see page 580).

3. Copy all filestore contents (files shared by all users in the environment) from the previous filestore location to the new location, as follows:

    - Documents: Copy from USM_HOME\view\documents to % USM_HOME\filestore\documents
    - Images:
        - Copy from USM_HOME\view\webapps\usm\images\offerings to % USM_HOME\filestore\images\offerings
        - Copy from USM_HOME\view\webapps\usm\images\rateplans to USM_HOME\filestore\images\rateplans
    - Forms: Copy from USM_HOME\view\forms to USM_HOME\filestore\forms
    - Custom directory: Copy any files that you want to update or replace from USM_HOME\view\webapps\usm\custom to USM_HOME\filestore\custom

    Note: Your installation can have some or all of these folders, depending on the previous version of CA Service Catalog that was installed.

4. Re-apply any customizations that you recorded for XML, XSL, or other CA Service Catalog files, such as category.xml or requestshared.xml. Restore or verify your customizations, as follows:

- (Migration model upgrade only) Compare each customized file that you backed up earlier with the files supplied in this release. Update the new file with your customizations from the backup file.
  Follow the same process for any customizations that you made to related third-party files such as Tomcat files.

  Important! You can replace certain new files with your backup files, in certain cases. However, *before* doing so, contact Technical Support and verify each file that you want to replace.

- (Traditional upgrade only) Review any CA Service Catalog files that you customized, such as custom.xml or requestshared.xml. Verify that your customizations are intact and are applicable for this release.
  The traditional upgrade automatically backs up customized files before the upgrade and restores them after the upgrade.

5. Perform this step if you customized the CA Service Repository Agent in the previous release and you want to continue using the same customizations for this release:

   Note: The CA Service Repository Agent is also named the Data Mediation Data Repository Agent. This repository agent automates the process of importing usage data in Delimiter Separated File format or Fixed Length File format.

You have set up shared and customized files.

Step 2 - Install CA Service Catalog

Important! Ensure that you have reviewed the CA Service Catalog Planning (see page 564) section before proceeding with this installation.

Use the CA Service Management Installer to install either only the CA Service Catalog product or Integrate CA Service Catalog with Unified Self-Service. Integration with CA Unified Self-Service lets you open a request and monitor the progress of this request.

Note: To connect to MS SQL database while installing the Unified Self-Service console, use the MS SQL server authentication method. Windows authentication is not supported.

Follow these steps:

1. Ensure that you complete the following steps by running the CA Service Management Installer (see page 296):

    a. Select a language and **CA Service Management** from the **Select the required installer** screen

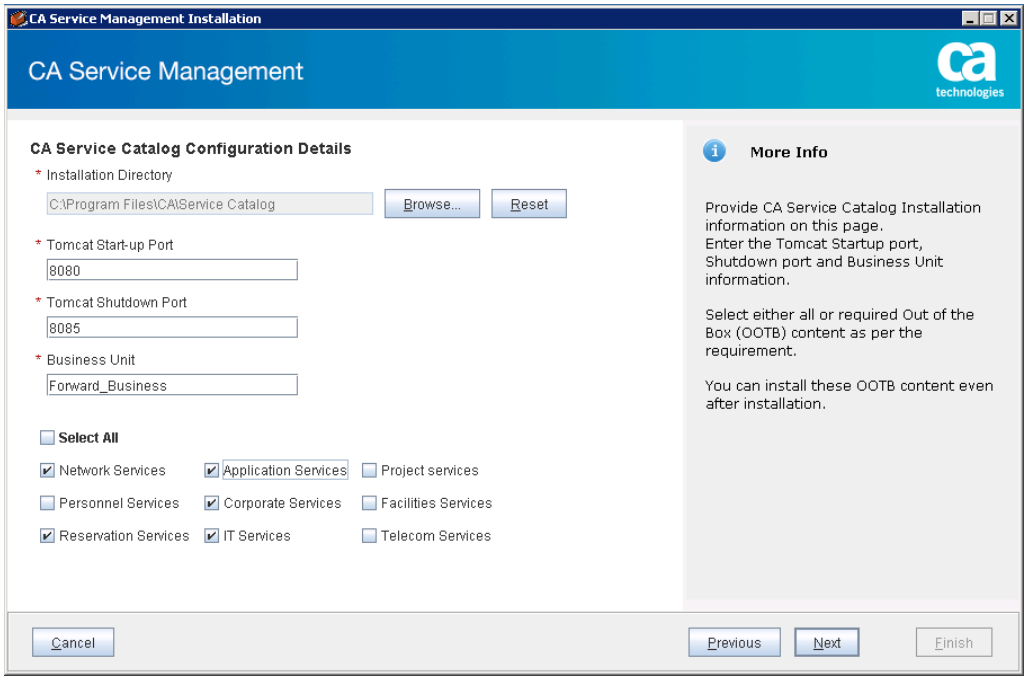
    b. Accept the license agreement.

    c. Enter the database information correctly.

    d. Select **CA Service Catalog** from the **Select the Products and Integrations** screen. If you want to integrate Unified Self-Service with CA Service Catalog, keep the check box for Unified Self-Service selected.

    e. Review the **Installation Prerequisites** report and taken corrective measures, if required, to proceed with the installation.

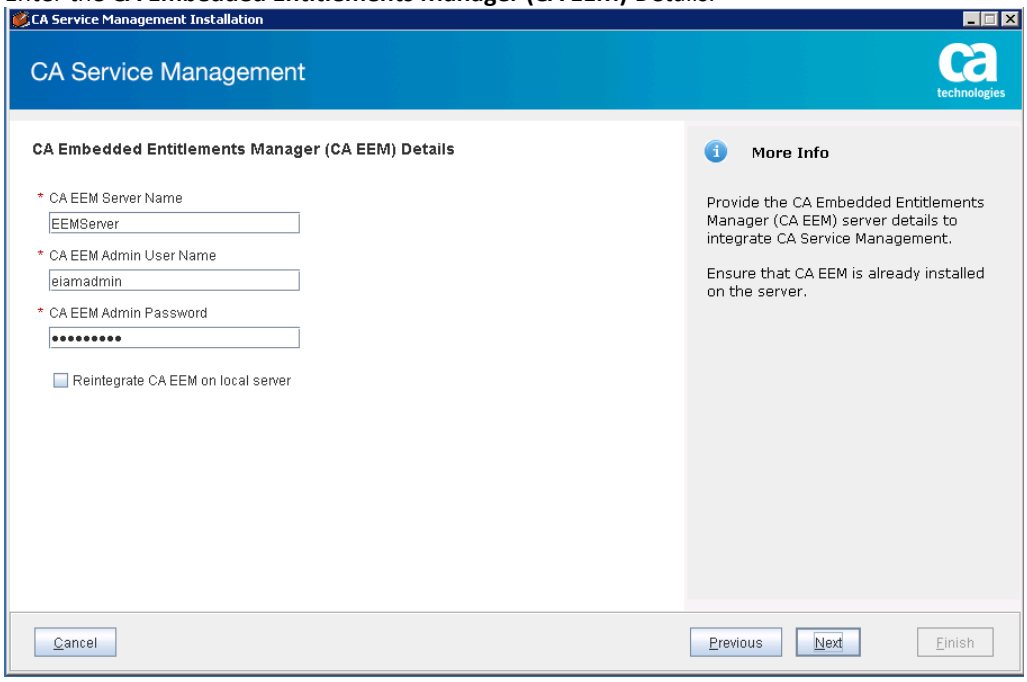
2. Specify the services you want to configure at the time of installation in the **CA Service Catalog Configuration Details** screen.



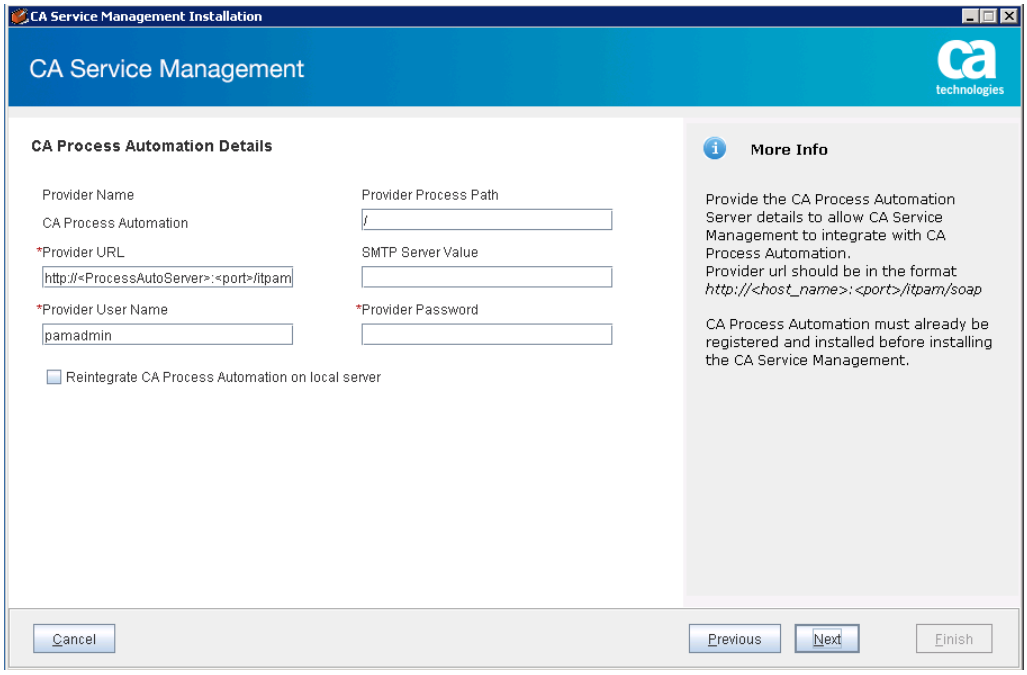
CA Service Catalog Configuration Details

3. (Optional). Enter details if you plan to integrate CA Service Catalog with Unified Self-Service. For more information, see the Install Unified Self-Service with CA Service Catalog (see page 593).

4. Enter the **CA Embedded Entitlements Manager (CA EEM)** Details.

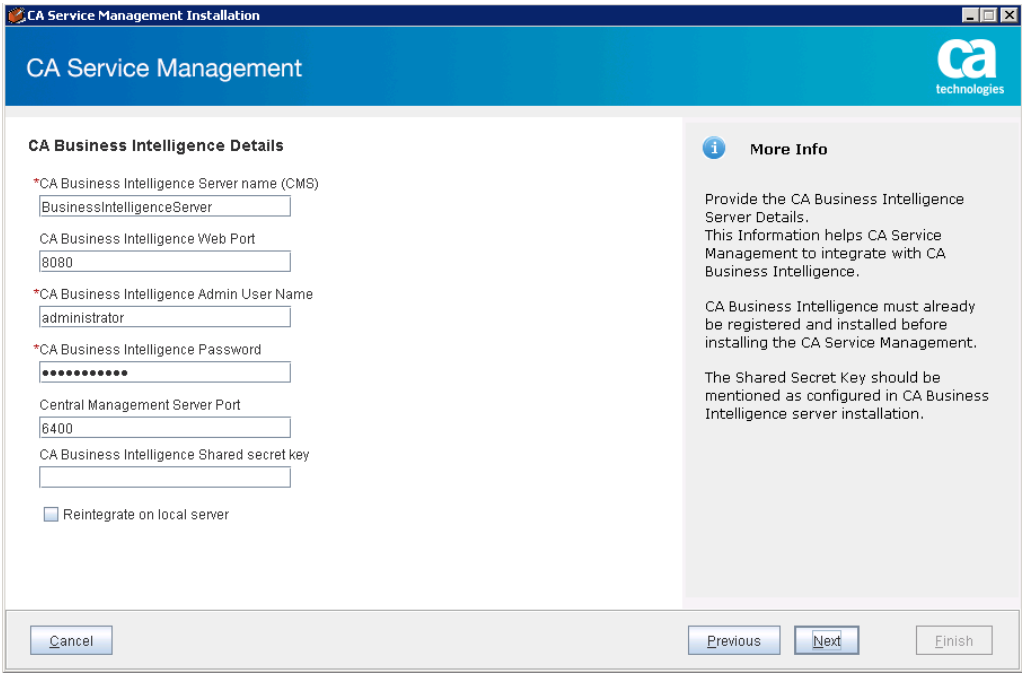


5. (Optional). Enter the CA Process Automation information in the **CA Process Automation Details** screen, if you intend to integrate CA Service Catalog with CA Process Automation.



CA Process Automation Details

6. (Optional). Enter the CA Business Intelligence information in the **CA Business Intelligence Details** screen to integrate CA Business Intelligence with CA Service Catalog.



CA Business Intelligence Details

7. Review the **Pre-Installation Configuration Summary** and verify that all the server and port information is correct.

8. Review the **Installation progress** information and click **Install** to install CA Service Catalog.

9. Review the log files stdout.txt and stderr.txt in the C:\ directory, if the installation failed. Fix the errors and click **Retry Install**.

10. Review the Installation Guidance Report summary to ensure that the installation was successful.

After the installation is complete, verify the CA Service Catalog installation by logging into the following URL as a Catalog administrator to view the CA Service Catalog User Interface:

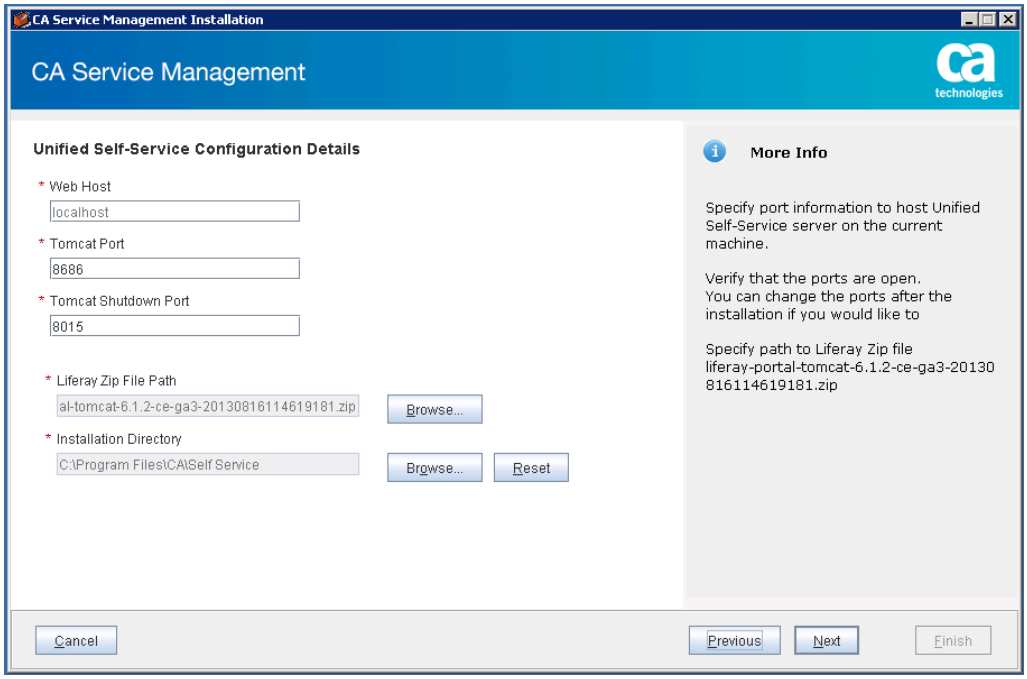
`http://<CA_Service_Catalog_Server_Name>:<Port_Number>/usm/`

You have successfully installed CA Service Catalog.

Install Unified Self-Service with CA Service Catalog

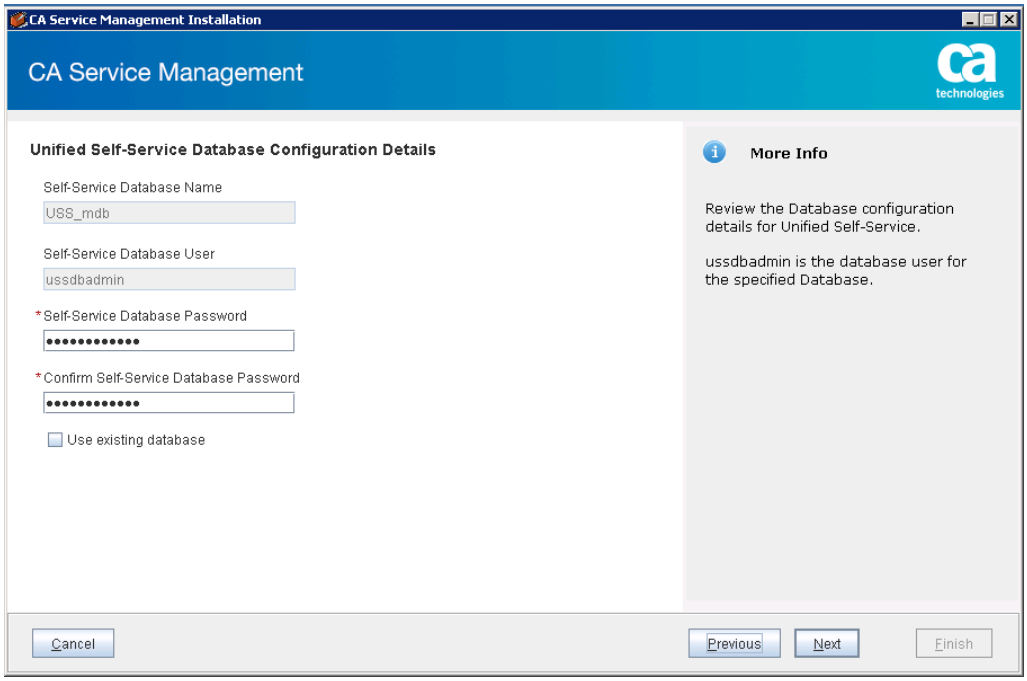
1. Enter the configuration details in the **Unified Self-Service Configuration Details** screen. Enter the Web Host as the host name of the machine where you are installing Unified Self Service.

> **Note:** Before you install Unified Self-Service, download Liferay CE 6.1.2 GA3 edition zip file (https://www.liferay.com/downloads/liferay-portal/available-releases). Do not Install Liferay manually as the installer unzips the downloaded file and installs Liferay.



Unified Self-Service Configuration Details

2. Enter the database information in the **Unified Self-Service Database Configuration Details** screen. If you have already set up a database, select the Use existing database check box and select the backup file. The database for Unified Self-Service is created during this installation.



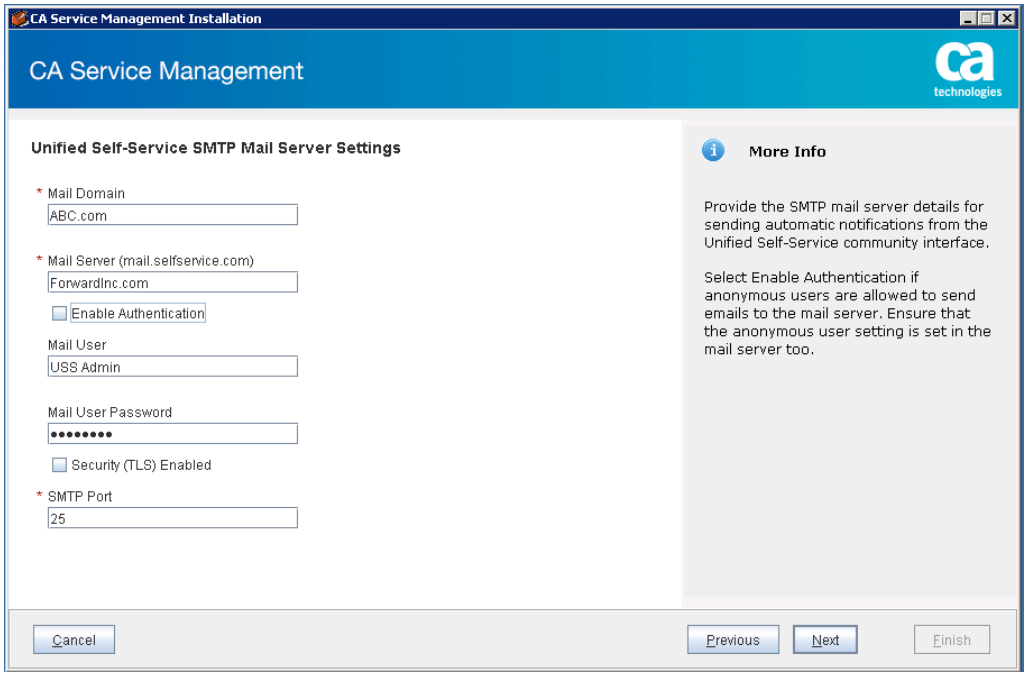
Unified Self-Service Database Configuration Details

3. Enter the SMTP mail server details to send automatic notifications from the Unified Self-Service community interface in the **Unified Self-Service SMTP Mail Server Settings** screen:

   - **Mail User**
     Defines the name of the mail user using which you want to send automatic notifications.

   - **Mail User Password**
     Defines the password of the mail user.

   - **Security (TLS) enabled**
     Specifies whether the TLS security is enabled or not for the mail server.



Unified Self-Service SMTP Mail Server Settings

You have entered all the Unified Self-Service information.

(Optional). After the installation is complete, verify the Unified Self-Service installation by logging into the following URL as an administrator to see the default tenant Home Page:

`http://<CA_Unfied_Self_Service_Server_Name>:<Port_Number>/`

Note: For optimal performance, consider setting up Unified Self-Service in a clustered environment (see page 619).

You have successfully installed the Unified Self-Service Console.

Step 3 - Perform CA Service Catalog Post-Installation Tasks

As part of implementing CA Service Catalog, review the following post-installation tasks and perform the tasks that apply:

- Update MaxKeepAliveRequests (see page 596)
- Assign the Service Delivery Administrator Role to a User (see page 596)
  - Change Your Password (see page 597)
- Create Users and Services (see page 598)
- Reset the JMS Port Number (see page 598)
- Install and Integrate Additional Process Automation Tools (see page 599)
- Configure JRE 1.8.0_45 (see page 599)
- Enhance Security (see page 600)
- Set Up Single Location for Shared Files (see page 601)
  - Retain the Default Location for Shared Files (see page 601)
  - Set Up a Custom Location for Shared Files (see page 602)
- Verify that Browser Security Settings Permit Login (see page 603)

After you perform the post-installation tasks that apply, you can also implement clustering (see page 604).

Update MaxKeepAliveRequests

If you installed CA EEM 12.51 in a clustered setup, you updated the MaxKeepAliveRequests property in the Apache proxy.conf file to meet the CA EEM installation requirements. Now, reset the MaxKeepAliveRequests property to its original value.

Note: The installation or upgrade program backs up your existing CA EEM data to the following location:

USM_HOME\conf-backup\upgrade-eem-backup.xml

Assign the Service Delivery Administrator Role to a User

Typically, the CA Service Catalog installation creates a user named *spadmin* and assigns it the Service Delivery administrator role. This user has complete control of the Catalog system. By default, the user name and the password are the same.

However, if *all* of the following conditions exist, then the installation *cannot* create this user.

- You have installed CA Service Catalog for the first time (*not* upgraded).
- CA EEM is already installed.
- CA EEM is already configured to use an external store, such as Microsoft Active Directory.

In this case, assign the Service Delivery Administrator role to another user. Doing so enables this user to log in to CA Service Catalog using the Service Delivery Administrator role. You can also assign the Service Delivery Administrator role to additional users. Doing so is optional but is beneficial if redundancy is important in your organization.

Follow these steps:

1. Open the CA Service Catalog command prompt by clicking Start, Programs, CA, Service Catalog, Service Catalog Command Prompt.

2. Enter the following command at the CA Service Catalog command prompt:

   ```
   ant add-spadmin-user
   ```

   Note: For a list of ant commands and their descriptions, enter ant -p.

3. Follow the prompts to add the spadmin administrator role to a specific user, using the following information:

   - If CA EEM *is* configured to use an external directory (such as Microsoft Active directory), specify an existing user name.
   - The command utility creates the user in the CA Service Catalog user database, if both of the following conditions exist:
     - CA EEM is *not* configured to use an external directory.
     - The user name that you specify is new.
   - The command utility does *not* prompt you for the password of the new or updated user.
   - If CA EEM *is* configured to use an external directory, the password is defined and stored in the external directory.
   - The new password is the same as the user name, if both of the following conditions exist:
     - CA EEM is *not* configured to use an external directory.
     - The user name that you specify is new.

4. If necessary, cancel and rerun the ant add-spadmin-user command to correct any errors.

5. Verify that the new or updated user can log in to CA Service Catalog as a Service Delivery Administrator and perform the spadmin functions.

6. (Optional) Instruct the new user to change the password (see page 597).

You have assigned the Service Delivery Administrator role to a user.

Change Your Password

Changing the password is especially recommended for the user named spadmin (the Service Delivery administrator). In addition, you can also change it at any time, for various security-related reasons.

Follow these steps:

1. Log in to CA Service Catalog with your current user name and password.
2. Click Profile.
3. Click the Change Password button at the top right of the page.
4. Enter your old and new passwords in the fields provided.
5. Click OK.

You have changed your password.

Create Users and Services

Once you have installed CA Service Catalog:

- Set up users, user groups, business units, and accounts.
- Create and customize services that users can request from the catalog.
- Configure the processes for managing, approving, and billing for requested services.

For more information about how to perform these tasks, see Manage Business Units and Tenant Administration (see page 1395), Manage Users and Assign Roles (see page 1408), Manage Services (see page 2987), and Service Accounting (see page 3108).

Note: Do not add users, delete users, or change user information using CA EEM. We recommend that you use CA Service Catalog for managing users. CA EEM is then updated accordingly.

Reset the JMS Port Number

Reset the JMS port number only if you specified 7777 as the CA Service Catalog startup or shutdown port when you ran the installation program. We recommend that you do *not* use port 7777 as the startup or shutdown port. Port 7777 is reserved for Java Messaging Service (JMS).

Important! If you must use port 7777 for the startup or shutdown port, reset the JMS port number after you have finished running the setup utility. Otherwise, port conflicts occur, and the product does not function correctly.

Follow these steps:

1. Open the file that is named USM_HOME/config.properties in a text editor.
2. Update the value of the jms.port property to a new value.
3. Restart the Windows service named CA Service Catalog.

You have reset the JMS port number.

Install and Integrate Additional Process Automation Tools

For best performance, CA Service Catalog requires a process automation tool. You can use CA Process Automation to automate processes in CA Service Catalog. Even though you can *install* CA Process Automation at any time, we recommend that you install CA Process Automation with CA Service Catalog using the CA Service Management Installer.

Important! If you install two or more instances of CA Service Catalog, implement clustering *before* you integrate CA Service Catalog with CA Process Automation.

Configure JRE 1.8.0_45

The CA Service Catalog installation program automatically installs the Java Runtime Environment (JRE). We recommend that you use the JRE version *1.8.0_45* that is installed by CA Service Catalog. You can configure CA Service Catalog to use or replace the JRE version, if required, as follows.

Follow these steps:

1. Install the JRE version 1.8.0_45, if not already installed.
   For example, install the JRE version from www.java.com (http://www.java.com) or one of its affiliated sites.
2. Open the Service Delivery Command Prompt from the CA Service Catalog section of the Windows Start menu. Enter the following command:

   ```
   ant upgrade-jre
   ```
3. Close all CA Service Catalog Windows services when prompted.
4. Enter the path name where you have installed the new JRE version.
5. Enter the new JRE version number. For example, 1.8.0_45.

   Wait for the CA Service Catalog system to verify that it supports the new JRE version.

   Note: If you receive a failure message, check the file Build.xml under Catalog home and check for statement new.jre.is (http://new.jre.is)**.supported**.

Check the JRE version again. If it remains unchanged even after you complete the upgrade process, change it manually.

6. Perform steps 2, 3, and 4 again. In case of failure, try using a different JRE version that is supported by CA Service Catalog.

   Note: For 32 bit JRE, change the path of jvm.dll from *<available file=${new.jre.dir} /bin.server" property="new.jre.has.server" /> to <available file="${new.jre.dir}/bin" property="new.jre.has.server" />*.

   The 64-bit JRE, jvm.dll is located in *C:\Program Files\Java\jre1.8.0_45\bin\server* and the 32-bit JRE is located in *C:\Program Files (x86)\Java\jre1.8.0_45\bin\client*.

   Close the command prompt.

7. Restart all CA Service Catalog Windows services and verify that you can log into CA Service Catalog.

   Note: If services fail to start, check the folder path *C:\Program Files\Java\jre1.8.0_45\bin*. Create a folder and name it as **Server**. Copy the contents of the **Client** folder in the **Server** folder. For 32-bit JRE, jvm is located in *C:\Program Files (x86)\Java\jre1.8.0_45\bin\client*. Check the service catalog.log in *C:\Program Files (x86)\Java\jre1.8.0_45\bin\server\jvm.dll*.

   You can log in and access CA Service Catalog using a different version of JRE.

Enhance Security

To enhance security in your CA Service Catalog implementation, *consider* making the following configuration changes:

- Disable the Apache JServ Protocol (AJP) port, port 8009 while performing the initial setup, if you are *not* implementing clustering.
  To disable AJP, edit the USM_HOME\view\conf\server.xml file and verify that the AJP tags are commented out.

- Reduce the timeout of CA Service Catalog user sessions. By default, sessions time out after 60 minutes of inactivity.
  To reduce the timeout, log in to CA Service Catalog, click Administration, Configuration, User Default. Adjust the **Session Timeout** parameter.

- Configure the CA EEM password policies to be more secure, if CA EEM is *not* configured to use an external directory.
  Specifically, consider locking user accounts after three to five failed login attempts. To set this value, log in to CA EEM and click Configure, EEM Server, Password Policies.

- Update the list of roles that can run web services. By default, only the Certificate user and users with the service provider (SP) administrator role can run web services.
  To change this list, log in to CA EEM with the Application set to Service Catalog. Click Manage Access Policies, Policies, Acess Policies, USM_Resource. Edit the policy whose permissions you want to update, and add the resource that is named usm_webservice__all to that policy.

  Note: For more information about editing these policies, see your CA EEM documentation (https://wiki.ca.com/display/eem1251/Policies).

- Enable Secure Socket Layer (SSL) for web services so that passwords are not sent in plain text when you use the logIn(String,String,String) method. If SSL is not available, consider using the logInToken(String) method instead. This method takes a CA EEM artifact as a parameter and is encrypted.

- Install antivirus software on the filestore computer, if you are using a filestore (see page) (a single location for shared files). We recommend that you use a filestore.

- Harden CA Service Catalog computers.
  Hardening is the process of securing a computer by removing or disabling components or access points, to render the computer less vulnerable to outside attacks. Hardening can include disabling all ports on a computer initially and afterwards manually enabling individual ports as needed. Other basic hardening steps include the following: Limit the number of users permitted access to a computer, strengthen password and access control, install intrusion-detection software, and close ports.

Set Up Single Location for Shared Files

If you have installed Catalog Component on multiple computers (either clustered or non-clustered), we recommend that you set up a single location for shared files. Shared files can include documents, reports, images of services, data mediation files, customizations, and forms.

By default, the location for shared files is the USM_HOME\filestore folder on *every* Catalog Component computer. This folder contains several subfolders. However, for optimal efficiency, you can specify *one* location on a single computer that all Catalog Component computers share. This single location is named the *central filestore* or *filestore*. The computer on which the filestore resides can have Catalog Component installed. However, Catalog Component is not required on that computer.

If you have installed Catalog Component on multiple computers and you do not set up a filestore, then verify that the individual filestores on all Catalog Component computers are synchronized.

If you have installed Catalog Component on a single computer, this entire process does not apply, so you can skip it.

Retain the Default Location for Shared Files

Setting up a single location for shared files helps improve the accuracy and efficiency of sharing files between computers.

Follow these steps:

1. Verify that all computers on which CA Service Catalog is installed have a trusted domain relationship. This trusted relationship enables user accounts and global groups to be used in a domain other than the domain where the accounts are defined.

2. Start the CA Service Catalog service with the login credentials of the Windows user that has read/write access to the shared location. If necessary, change the login credentials for the CA Service Catalog service to meet these requirements, as follows:

    a. Select Administrative Tools, Services.

    b. Right-click the service, click Properties, click the Log On tab, and enter the login credentials.

    c. Save the changes and restart the service.

3. Share the USM_HOME\filestore folder on the first CA Service Catalog computer as the filestore for all CA Service Catalog computers.

Set Up a Custom Location for Shared Files

You can create a custom location for shared files.

Follow these steps:

1. Share the folder to use as the filestore.

2. Verify that the Windows operating system users who are updating the filestore have read /write access to this folder.

3. Use the UNC path in the format *computer-name**folder-name* to specify the location of the filestore.

4. Start the Catalog Component service with the logon credentials of the Windows user who requires access to the folder.

5. Select Administration, Configuration, Filestore Information.

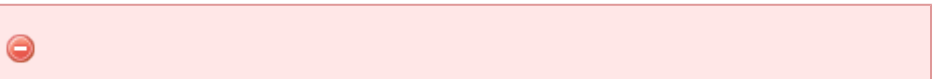
6. Perform the following steps:

    a. Click the Edit icon for the Filestore Location variable.

    b. In the Filestore Location field, specify the UNC path name of the shared drive you defined in a previous step, for example: \\big-computer\Shared_USM\filestore or \\big-computer\filestore.

    c. Click Update Configuration.

    d. Click Test to verify the validity of the share.
    This test returns a successful connection test message if the filestore can be used to store files that are uploaded by users.



Important! Testing the filestore is mandatory.

7. Perform the action that applies:
   - If the test succeeds, copy the entire contents of the USM_HOME\filestore folder to the new location.
   - If the test fails, reconfigure the share. Also, verify that all the CA Service Catalog services that are accessing the share have the same, valid credentials.
8. Recycle all CA Service Catalog services on all computers.

Verify that Browser Security Settings Permit Login

This topic applies *only* if you are using Internet Explorer to access CA Service Catalog. Your browser security settings can prevent you from seeing the user name and password prompts when you attempt to log in to CA Service Catalog. Therefore, verify your browser security settings to ensure that you can access CA Service Catalog.

Follow these steps:

1. Open Internet Explorer on the computer you want to use for accessing CA Service Catalog.
2. Enter the URL to start CA Service Catalog in the browser address field, in the following format:
   http://computer-name:port number/usm/
   - ***computer-name***
     Specifies the name of the computer that you want to log in to.
   - ***port number***
     Specifies the CA Service Catalog port number of that computer.
3. Verify that you see the CA Service Catalog login page, including the user name and password prompts.
   If Yes, this verification procedure is complete, and you can skip the remaining steps.
   If No, complete the remaining steps.
4. In Internet Explorer, open Internet Options, click Security, and perform *one* of the following steps:
   - Change the security level for the Local Intranet to Medium-High or Medium
   - Add the login URL for CA Service Catalog to your Trusted sites
5. Close and reopen your browser.
6. Enter the URL to start CA Service Catalog in the browser address field. Verify that you see the CA Service Catalog login page with the user name and password prompts.

You have verified your browser security settings to ensure that you can access CA Service Catalog.

(Optional) Implement Clustering

A *cluster* is two or more interconnected computers that create a solution to provide higher availability, higher scalability, or both.

A CA Service Catalog administrator can optionally use clustering for CA Service Catalog to improve performance and provide failover protection. Clustering means multiple computers in a group that perform the same or similar function, essentially acting as one virtual computer. Failover protection means that if one computer malfunctions, becomes heavily loaded, or loses power, its workload is transferred to the other computers in the cluster. These computers retain and complete the active sessions.

Another advantage of clustering is load-balancing. If one of the cluster components is processing a request, the load is redirected to another component in the cluster. Users of the system see no interruption of access. The loss of performance on users and business functions is minimized, even when computer availability is lost or reduced.

Clustering for CA Service Catalog is accomplished through the Catalog Component clustering. All user communications with catalog and accounting functions are accomplished through the Catalog Component. Thus, the term *Catalog Component clustering* includes both Catalog Component clustering and Service Accounting Component clustering.

In *horizontal clustering*, different physical computers comprise a cluster. As a result, the load balancer forwards requests to different computers having different IP addresses. All Catalog Component installations on all computers must use the same cluster of the MDB.

You can optionally install and cluster multiple instances of CA EEM and CA Process Automation.

Important! These instructions apply *only* to the Apache Tomcat web server version supplied with CA Service Catalog. If you are using any other web server instead, see your web server documentation for information about clustering.

Follow these steps:

- Step 1 - Verify Prerequisites for Clustering (see page 604)
- Step 2 - Set Up Horizontal Clustering for CA Service Catalog (see page 606)
- Step 3 - (Optional) Set Up NTLM Authentication for Each Cluster (see page 608)
- Step 4 - Set Up Load Balancing (see page 609)

Step 1 - Verify Prerequisites for Clustering

Perform the following preliminary tasks before you implement clustering:

1. Decide how many cluster nodes to create, depending on your design concerns and availability of resources.

2. Verify that the time and time zone on all clustered computers are the same.

3. Verify that the IPV6 protocol is disabled on all clustered computers.

4. Verify that no other application uses the following ports.
   By default, CA Service Catalog uses these ports for clustering, using the AJP protocol:

   - 8009 - for CA Service Catalog communicating with Apache HTTP Server
   - 8019 - for Service Fulfillment communicating with Apache HTTP server

5. Perform the following step if applicable:

   a. If another application uses one of these port numbers, eliminate the duplication. Use a different port number for either CA Service Catalog or the other application.

   b. If you use a different port number for CA Service Catalog, then also replace the old port number with the new port number. For example, if you change 8009 to a different port number, use the new port number instead of 8009.

6. Locate the multicast address for Tomcat in the server.xml file that is located in the USM_HOME\view\conf folder. This address is the value of the address attribute within the Membership tag.
   Default: 228.0.0.4

7. Locate the multicast address for Java Messaging Service (JMS) in the config.properties file that is located in the USM_HOME folder.
   Default: 239.255.2.3:6155

8. Run the following command at the DOS prompt of each clustered computer:

   ```
   netsh interface ip show joins
   ```

   The command lists all multicast addresses applicable to this computer.

9. Verify that this list includes the multicast addresses that you recorded from the server.xml and config.properties files:

   - If Yes, then skip the remaining steps in this topic.
   - If No, then use the list to determine a common multicast address applicable to all clustered computers. Complete the remaining steps.

10. Follow these steps:

    a. Update the multicast addresses in the server.xml files on all clustered computers and use this common address.

    b. In the config.properties files on all clustered computers, edit the JMS-related configuration section. Specify this common address, as shown in the following example.

    Important! The port number *must* be the same on each computer in the cluster.

```
#multicast://default = multicast://239.255.2.3:6155
#static:(tcp://<host1>:<port>,tcp://<host2>:<port>,...)
jms.networkConnectorUri = multicast://custom-ip-address:custom-port
jms.discoveryUri = static: multicast://custom-ip-address:custom-port
#jms.port = 7777
jms.port = custom-port
```

c. If you want to specify your nodes statically instead of using a multicast address, perform this step instead of step b.
In the config.properties files on all clustered computers, edit the JMS-related configuration section. Specify the host and port for all other computers in the cluster, as shown in the following example.
The port number can be the same value on each computer in the cluster, or it can be different.

```
#multicast://default = multicast://239.255.2.3:6155
#static:(tcp://<host1>:<port>,tcp://<host2>:<port>,...)
jms.networkConnectorUri = static:(tcp://host:custom-port)
jms.discoveryUri = static:(tcp://host:custom-port)
#jms.port = 7777
jms.port = custom-port
```

Note: Update the server.xml and config.properties files on all clustered computers before proceeding to the next step.

11. Restart the CA Service Catalog Windows service on all clustered computers.

Step 2 - Set Up Horizontal Clustering for CA Service Catalog

Perform this process on *every* computer on which you want to set up a horizontal cluster node for CA Service Catalog, including the first CA Service Catalog computer.

Note: Before you perform this procedure, verify that CA Service Catalog is installed locally.

Follow these steps:

1. As a prerequisite, if this computer is not the first-installed CA Service Catalog computer, perform the following steps:

   a. Verify that its host name is unique.

   b. Verify that its database is pointing to the database of the CA Service Catalog computer installed first.

2. Open the USM_HOME\view\conf\server.xml file for editing. Uncomment the Cluster tags, if they are commented:

3. Specify a unique port in the <Cluster> section for each CA Service Catalog computer:

```
<Receiver className="org.apache.catalina.tribes.transport.nio.NioReceiver"
      address="auto"
      port="4000"
      autoBind="100"
      selectorTimeout="5000"
      maxThreads="6"/>
```

4. Uncomment the Apache JServ Protocol (AJP) tags shown in the following lines, if they are commented:

```
<Connector port="8009" enableLookups="false" redirectPort="8443"
tomcatAuthentication="false"
      maxThreads="400" minSpareThreads="25" maxSpareThreads="100" protocol="AJP
/1.3" />
```

5. (Optional) Comment the HTTP ports Connector tags to improve security as follows:

```
<Connector port="8080" enableLookups="false" redirectPort="8443"
tomcatAuthentication="false"
      maxThreads="400" minSpareThreads="25" maxSpareThreads="100" debug="0"
connectionTimeout="15000"
      disableUploadTimeout="true" compression="on" compressionMinSize="2048"
      compressableMimeType="text/html,text/plain,text/xml,text/css,text
/javascript,image/png,image/gif,image/jpeg,application/json"
      useBodyEncodingForURI="false" URIEncoding="UTF-8" />
```

6. Save the file.

7. Review the ServiceCatalog.log file of each CA Service Catalog computer and verify that the replication cluster was added. For example:

```
INFO Cluster-MembershipReceiver org.apache.catalina.cluster.tcp.
SimpleTcpCluster - Replication member added:org.apache.catalina.cluster.mcast.
McastMember[tcp://141.202.143.77:4013,catalina,141.202.143.77,4013, alive=0]
```

8. Restart the CA Service Catalog Windows services: CA Service Accounting and CA Service Catalog.

9. If you are using NTLM authentication to enable single sign-on to CA Service Catalog, set up NTLM authentication for each cluster (see page 608).

You have set up clustering for CA Service Catalog.

Remove a Cluster

When necessary, you can remove a horizontal CA Service Catalog cluster. Sample reasons for doing so include the following conditions:

- This computer becomes obsolete.
- You want to install clustering on a different computer.
- This cluster is no longer needed.

Follow these steps:

1. Open the server.xml file of the horizontal cluster node that you want to remove.
2. Comment the cluster tag.
3. Restart the CA Service Catalog Windows service.

You have removed the cluster node. Next, verify that the load balancer setup no longer references this cluster.

Step 3 - (Optional) Set Up NTLM Authentication for Each Cluster

If you are clustering CA Service Catalog and you are using NTLM authentication to enable Single Sign-On to CA Service Catalog, then set up the cluster for Single Sign-On.

Follow these steps:

1. Perform *one* of the following actions on each cluster:
   - If you are using Apache Load Balancer, perform the following steps on each cluster to set up NTLM Authentication.
     a. Download the mod_auth_sspi module from the sourceforge web site, sourceforge.net.
     b. Copy the mod_auth_sspi.so module to the <APACHE_Home>\modules directory of the Apache web server that you use for CA Service Catalog.
     c. Append the following configuration section to the <APACHE_Home>\conf\httpd.conf file.

```
LoadModule sspi_auth_module modules/mod_auth_sspi.so

<Location ~ "/usm/(wpf|documents|FileStore)">

AuthName "domain_name"

AuthType SSPI

SSPIAuth On

SSPIOfferBasic On

SSPIAuthoritative On

SSPIDomain "domain_name"

SSPIofferSSPI off

require valid-user

</Location>
```

d. Replace *domain_name* with the name of your network domain or Windows domain in the file.

e. Verify that the tomcatAuthentication="false" attribute is set for the Tomcat connectors that this Apache load balancer uses.

2. If you *are* using a load balancer *other than* Apache Load Balancer, configure NTLM authentication for your load balancer first. Then configure Tomcat to use NTLM authentication for CA Service Catalog for each catalog cluster node, if both of the following conditions exist:

   - Your load balancer is not configured to perform NTLM authentication.
   - Your load balancer uses the HTTP Port (default 8080) to connect to Tomcat instances of CA Service Catalog. For more information about how to set up NTLM authentication, see your load balancer documentation.

3. Log in to any CA Service Catalog computer in the cluster.

4. Click Administration, Configuration, Single Sign On Authentication.

   Note: Perform this step and the remaining steps *once* in your implementation. You do not need to repeat these steps for individual clusters, because performing them once affects all clusters.

5. a. Locate the property that is named **Single Sign On Type** and click the Modify icon.

   b. Select the option that is named **Artifact Based Single Sign On** and click Update Configuration.
   The dialog closes, and you return to the Sign On Authentication page.

   c. Locate the property that is named **Artifact Type** and click the Modify icon.

   d. Set **Artifact Type** to the appropriate option for your load balancer, and click Update Configuration. For Apache Load Balancer, select Request.

6. Restart the CA Service Catalog Windows services to ensure that you have set up NTLM Authentication for the clusters.

Step 4 - Set Up Load Balancing

To load balance the existing nodes using Apache HTTP Server, follow these instructions. Perform this process *after* you have set up all cluster nodes.

Note: If you are implementing horizontal clustering on multiple computers, use the computers that have the same default gateway. To obtain the default gateway, enter the ipconfig command at the DOS prompt.

1. Install Apache Web Server load balancer for Windows version 2.2.25. You can download it from the Apache web site, apache.org.
   The default installation folder is C:\Program Files\Apache Software Foundation\Apache2.2.
2. Configure Apache HTTP Server. (see page 610)
3. (Optional) Disable Web Server Features. (see page 610)
4. Create and Configure the workers.properties File. (see page 611)
5. Create the uriworkermap.properties file. (see page 613)
6. Update the httpd.conf file. (see page 614)
7. Verify load balancing. (see page 616)

Configure Apache HTTP Server

Configuring Apache HTTP Server is a required task when you set up load balancing.

Follow these steps:

1. Access the Apache website, www.apache.org.
2. Find and download the file that is named mod_jk-1.2.30-httpd-2.2.3.so. CA Service Catalog supports mod_jk 1.2.30.
3. Rename the mod_jk-1.2.30-httpd-2.2.3.so file to *mod_jk.so*.
4. Copy the mod_jk.so file to the modules folder in the Apache Server installation.

You have configured Apache HTTP Server.

(Optional) Disable Web Server Features

Disabling the web server features of Apache HTTP Server improves performance and reduces potential security risks.

Follow these steps:

1. Delete the following folders under C:\Program Files\Apache Software Foundation\Apache2.2:
   - \cgi-bin
   - \errror
   - \htdocs
   - \icons
   - \manual

> **Note:** The "C:\Program Files\" portion of the path names reflect the typical location that is specified at installation time. This portion of your path names can vary depending on the installation directory that is specified for the \Apache Software Foundation folder at installation time.

2. Rename httpd.conf to _httpd.conf.bak in the C:\Program Files\Apache Software Foundation\Apache2.2\confdirectory.

3. Find the httpd.minimal.conf file.
   This minimal configuration file is included in the Utilities/Apache Webserver directory of the CA Service Catalog installation media.

4. Copy the httpd.minimal.conf file to C:\Program Files\Apache Software Foundation\Apache2.2\conf.

5. Rename the httpd.minimal.conf file to httpd.conf in that directory.

6. Delete all files in that directory *except* the following files:

   - httpd.conf
   - _httpd.conf.bak

7. Change to the C:\Program Files\Apache Software Foundation\Apache2.2\modules directory.

8. Delete all files in that directory *except* the following files:

   - mod_jk.so
   - mod_log_config.so
   - mod_setenvif.so

You have disabled web server features.

Create and Configure the workers.properties File

Creating and configuring the worker.properties file is a required task when you set up load balancing.

Follow these steps:

1. Create the workers.properties file manually in the \conf directory of the Apache installation folder.

2. Verify that the file lists all the Tomcat instances to include in the clustered environment.

3. Obtain the following information for each cluster node:

   - The host name of the clustered node
   - The ajp port of the clustered node. Obtain it from the connector port in the following line in the server.xml file of each cluster node:

```
<Connector port="8009"  maxThreads="150" tomcatAuthentication="false'
```

- The jvmRoute name of the node. Obtain it from the following line in the server.xml file of each cluster node:

  ```
  <Engine name="Standalone" defaultHost="localhost" debug="0" jvmRoute=
  ```

  For example, for the CA Service Catalog cluster node on the computer that is named XYZ, the jvmRoute name is XYZ_USMView.

  Important! Verify that the jvmRoute name is unique for each CA Service Catalog cluster. This name must be unique, because the load balancer uses it to identify each cluster. This name is case-sensitive.

4. Review the following sample worker.properties file sections for the types of clustering that you can perform. In all cases, the worker.properties file defines a load balancer node named loadbalancerview. This node balances CA Service Catalog requests among the CA Service Catalog cluster nodes. For example, this node load balances the /usm context between the workers defined. The context path /usm is defined in the USM_HOME\view\conf\server.xml file pointing to the CA Service Catalog web application.

5. Review the example (see page 613).

   a. Add a worker to the cluster, as follows:

      i. Create a worker section at the end of the worker.properties file, using the following lines as a model:

      ```
      worker.jvmRouteName.port=ajpport
      worker.jvmRouteName.host=HOSTNAME
      worker.jvmRouteName.type=ajp13
      worker.jvmRouteName.lbfactor=1
      ```

      ii. Verify that its jvmRouteName is unique.

      iii. Add the new cluster at the end of the list of balance workers for a loadbalancer node.
      For example, suppose that the jvmRoute name of the new worker is COMPUTER3_caff and its ajpport is 8019. In that case, enter the following new worker section to add the new cluster to the selected loadbalancer node:

      ```
      worker.COMPUTER3_caff.port=8019
      worker.COMPUTER3_caff.host= COMPUTER3
      worker.COMPUTER3_caff.type=ajp13
      worker.COMPUTER3_caff.lbfactor=1
      ```

      iv. Remove an existing cluster from the loadbalancer setup in the worker. properties file, as follows:

      1. Delete the section for the worker.

      2. Remove any references to the deleted worker from the list of balance workers.

The list of balance workers begins with the following line:

```
worker.<loadbalancernode>.balance_workers
```

You have created and configured the worker.properties file.

Horizontal Clustering Example for CA Service Catalog

This example illustrates how to use clustering to load balance the /usm context of CA Service Catalog between two workers. The cluster specifications are as follows:

Worker1:

- Hostname: Computer1
- JVMroutename: Computer1_USMView
- AJP port: 8009

Worker 2:

- Hostname: Computer2
- JVMroutename: Computer2_USMView
- AJP port: 8009

In these examples, Computer1 and Computer2 are the host names (computer names) of the workers.

Use the loadbalancerview node to load balance between the workers Computer1 and Computer2 as horizontal clusters for CA Service Catalog. To do so, define the loadbalancerview node sections of the worker.properties as follows.

```
worker.list=loadbalancerview
worker.status.type=status
worker.loadbalancerview.method=Busyness
worker.loadbalancerview.type=lb
worker.loadbalancerview.balance_workers=COMPUTER1_USMView,COMPUTER2_USMView
worker.loadbalancerview.sticky_session=1
worker.COMPUTER1_USMView.port=8009
worker.COMPUTER1_USMView.host=COMPUTER1
worker.COMPUTER1_USMView.type=ajp13
worker.COMPUTER1_USMView.lbfactor=10
worker.COMPUTER2_USMView.port=8009
worker.COMPUTER2_USMView.host=COMPUTER2
worker.COMPUTER2_USMView.type=ajp13
worker.COMPUTER2_USMView.lbfactor=10
```

Create the uriworkermap.properties File

Creating and configuring the uriworkermap.properties file is a required task when you set up load balancing. This file specifies which context the load balancer node selects and forwards to its cluster nodes.

Note: If the file exists already, update it to match the text in the following steps.

Follow these steps:

1. Manually create the uriworkermap.properties file in the \conf directory of the Apache installation folder.
2. Enter the following lines in the file:

   ```
   /usm|/*=loadbalancerview
   ```

3. Save the file.

You have created the uriworkermap.properties file.

Update the httpd.conf File

Updating the httpd.conf file is a required task when you set up load balancing.

Follow these steps:

1. Open the conf/httpd.conf file in the Apache HTTP Server installation directory and update it to include the following specifications:

   ```
   Listen 89
   LoadModule jk_module modules/mod_jk.so
   JkWorkersFile conf/workers.properties
   <VirtualHost *:89>
    ServerName load balancer host name
    JkMountFile conf/uriworkermap.properties
    JkLogFile logs/mod_jk.log
    JkLogLevel debug
   </VirtualHost>
   ```

2. Find the following lines:

   ```
   JkLogFile logs/mod_jk.log
   JkLogLevel debug
   ```

3. (Optional) Replace the lines in the previous step with the following lines:

   ```
   JkLogFile "|bin/rotatelogs.exe logs/mod_jk.log.%Y-%m-%d-%H_%M_%S 10M"
   JkLogLevel emerg
   ```

   This action modifies the mod_jk.log file on your production server to record only critical errors. The action also enables automatic rollover when the log file size reaches 10 MB.

4. Add a Listen directive with the port number for every VirtualHost port in the file.
   For example, suppose that you have defined a virtual host at port 89, as follows:

   ```
   <VirtualHost *:89>
   ```

   In that case, add the Listen directive for this port in the httpd.conf file, for example:

   ```
   Listen 89
   ```

   Note: The commonly used port is 89.

This specification enables the Apache HTTP Server to listen on this port and accept incoming requests.

5. Change the Default Type from text/plain to text/html.

   Note: This setting works well on most browsers. If you experience any difficulty with performance or display quality after changing this option, return it to its original value.

6. Save and close the conf/httpd.conf file.

7. Adjust related settings (see page 615) in other locations.

8. Disable the HTTP ports of the cluster computers (see page 615).

9. Configure the server information for the cluster computers (see page 616).

Adjust Related Settings

Adjusting related settings is a required task when you update the httpd.conf file.

Follow these steps:

1. Open your web browser. Set the proper values for the ServerAdmin and ServerName options.

2. Restart the Apache service, as follows:

   a. Open the Apache Service Monitor.

   b. Highlight the service to restart.

   c. Click Restart.

3. Test by accessing the link http://*hostname*:89/usm.
   Here, *hostname* specifies the load balancer computer, the computer on which the Apache HTTP Server is configured for load balancing.

4. Review the mod_jk.log file under the logs folder in the Apache directory to determine which jvmRoute node was called. An example follows:

   ```
   found worker HOST1__USMView (HOST1__USMView) for route COMPUTER1__USMVi
   ```

(Optional) Disable HTTP Ports

To enhance security, disable the HTTP ports of the cluster computers when you update the httpd.conf file. Doing so routes users directly to the load balancer computer rather than directly to a cluster.

Follow these steps:

1. Comment the connector tag that includes HTTP port information, in the server.xml files of each cluster computer. This port is the startup node that is provided during installation, typically 8080.

2. Recycle the CA Service Catalog Windows services of the clusters whose server.xml files were changed. The Windows services are named CA Service Accounting and CA Service Catalog.

Configure Server Information

Configuring the server information of the cluster computers is a required task when you update the httpd.conf file.

Follow these steps:

1. Click **Administration**, **Configuration**, **Server Information**, in the CA Service Catalog GUI.

2. Replace the server host name and port number with the load balancer host name and port number.

3. Recycle the CA Service Catalog Windows services of the clusters whose Server Information options were changed.

You have configured the server information of the cluster computers.

Note: If you do not perform this task, the following error occurs for users who request CA Service Catalog services using Internet Explorer 8.0: Forms that include a lookup field that calls a report object do not populate correctly when the user clicks the Search icon.

Verify Load Balancing

To test load balancing, verify that the load is distributed to other nodes when one of the nodes in the same cluster becomes busy. To test failover functionality, verify that the load is distributed to other nodes when one of the nodes in the same cluster shuts down.

Verify that *all* clustered nodes communicate efficiently with *all* load balancer computers using the telnet utility. If the clusters do not run efficiently, verify that this communication exists and check for any network configuration problems. For example, suppose that your load balancer host name is abc and the port is 89. Verify that you can successfully connect from all your clustered nodes using the following command from each node:

```
telnet abc 89
```

We recommend that you cluster your load balancer computers to help avoid single-point-of-failure problems with an individual load balancer computer. For more information, see the Apache website and other resources about how to cluster load balancer computers.

You can also record cluster-related logging information in the tomcat_view.log file.

Follow these steps:

1. Add the following section to the log4j.xml file for each CA Service Catalog computer:

```
<logger name="org.apache.catalina.cluster" additivity="false">
  <level value="TRACE" />
  <appender-ref ref="tomcat_view" />
</logger>
```

2. Set the log level for each log4j.xml file appropriately. For example, use a high log level while you are troubleshooting. Conversely, use a low log level, or comment out the previous lines, at other times.

Step 7 - (Optional) Enable Secured Sockets Layer (SSL) Authentication

Configuring the SSL authentication provides enhanced login security while allowing users to access a higher performance connection.

Perform the following steps to enable SSL authentication in CA Service Management.

1. Configure SSL Authentication in the Products of the Solution (see page 617).
2. Run the SSL Authentication Batch File (see page 617).
3. Enable SSL Integration (see page 618).

Configure SSL Authentication in the Products of the Solution

You must first configure SSL authentication in each product you installed as part of the solution.

For information on how to configure SSL authentication in the products of the solution see the following information:

- Configure SSL Authentication in CA SDM (see page 935)
- Configure SSL Authentication in CA Service Catalog (see page 1432)
- Configure SSL Authentication in CA APM (see page 318)

Run the SSL Authentication Batch File

After you installed CA Service Management and configured SSL authentication, you must the run the SSL authentication batch file.

Follow these steps:

1. Navigate to [ISO_ROOT]\\DBCleanupUtility.
2. Run the UpdateScriptUSS.bat batch file.

Enable SSL Integration

After you configured SSL authentication in each of the products, you must enable SSL integration through the common administration user interface.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.

2. In the Home page, click Request a Service.
   The Request Page Appears.

3. Under Categories, click Service Management Administration.

4. Click Product Integrations.

5. Under each product tab, check the **HTTPS** check box and specify the SSL port numbers.

6. Click Submit.

Upgrade to the Supported JRE Version for Unified Self Service

You must upgrade to the supported JRE version to successfully implement Unified Self Service.

Follow these steps:

For Windows

1. Download the supported JRE version.

2. Shut down the following services:

   - CA Unified Self-Service jetty server

   - CA Unified Self-Service server

3. Take a backup of wrapper.conf, located at <drive>:\Program Files\CA\Self Service\OSOP\tomcat-7.0.40\bin.

4. Edit wrapper.conf using the text editor and modify **set.JAVA_HOME=** with the JRE Installed location. **Example:** \Program Files\Java\jre1.8.0_45\bin

5. Save the file.

6. Start the following services:

   - CA Unified Self-Service jetty server

- CA Unified Self-Service server

For Linux

1. Download the supported JRE version.
2. Shut down all the services for Unified Self Service.
3. Take a backup of startup.sh, located at opt/CA/Self Service/bin.
4. Open startup.sh.
5. Look for **Export JAVA_HOME=** and update with the JRE installed location.
6. Look for **Export PATH= /bin:** and update with the JRE installed location.
7. Start all the services for Unified Self Service.

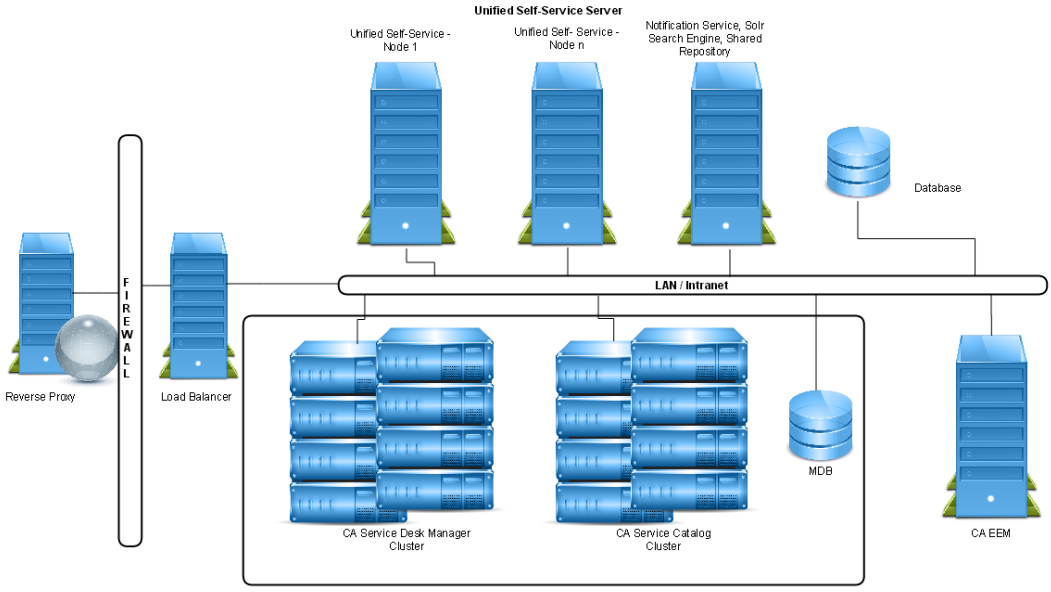
How to Set up the Cluster Environment for Unified Self-Service

For the optimal performance, set up Unified Self-Service on a cluster environment. In an ideal cluster environment, multiple server instances with identical configuration span across multiple nodes. All instances in a cluster work together to provide high availability, reliability, and scalability.

You need the following minimum requirements for the cluster environment:

- Two machines to set up the Unified Self-Service nodes
- One machine to set up Solr 1.4.1, Notification Server, and Shared Repository
- One Database server
- One machine for Load Balancer

The following diagram shows an ideal cluster environment for Unified Self-Service:



Follow these steps:

1. Set up and Configure Node 1 (see page 620)
2. Set up and Configure Node 2 (see page 623)
3. Configure the Load Balancer (see page 624)

Set up and Configure Node 1

Set up Unified Self-Service on node 1 and configure it for the cluster environment.

Follow these steps:

1. Install Unified Self-Service on a machine or node 1. Ensure that you give the Database Host as the machine name.
2. Onboard a tenant and configure the CA SDM data source. For more information, see Onboard Tenants (see page 1679).
3. Shutdown Unified Self-Service in services.msc.
4. Open the portal-ext.properties file located in the OSOP folder of the Unified Self-Service installation directory.
5. Append the file with the following lines:

```
#cluster
cluster.link.enabled=true
ehcache.cluster.link.replication.enabled=true
lucene.replicate.write=false
net.sf.ehcache.configurationResourceName=/custom-ehcache/hibernate-clustered.xml
```

```
ehcache.multi.vm.config.location=/custom-ehcache/liferay-multi-vm-clustered.xml
```

6. Extract the custom-ehcache.zip file from the OSOP\tools folder to the OSOP\tomcat-7.0.40 \webapps\ROOT\WEB-INF\classes\ folder.

   Important! Ensure that after the extraction, the custom-ehcache folder is created in the same path as the **hibernate-clustered.xml** and **liferay-multi-vm-clustered.xml** files.

7. Open the server.xml file from the OSOP\tomcat-7.0.40\conf\ folder.

8. Replace <Engine name="Catalina" defaultHost="localhost"> with <Engine name="Catalina" defaultHost="localhost" jvmRoute="node1">.

9. Restart Unified Self-Service services.

10. Install and Configure Apache Solr (see page 621) and Configure Liferay to use Solr for Searching (see page 622).

11. Configure the common repository for attachments on the Unified Self-Service common server. For more information, see the Liferay documentation.

12. Copy the OSOP\jetty-7.2.2.v20101205 folder to the Unified Self-Service common server to configure the notification server on the common Unified Self-Service server.

13. Configure the notification server on the Unified Self-Service node:

    a. Open portal-ext.properties file and search for *cometd*.

    b. Replace localhost with the hostname or IP address of Unified Self-Service common server and port with the port number on which Jetty is running. For example,

    ```
    #cometd configurations begin
    cometd.enable=true
    cometd.contextPath=/notification-server
    #internal properties are used by java client
    cometd.internal.host=localhost
    cometd.internal.port=18686
    cometd.internal.protocol=http
    #external properties are used by jquery clients
    cometd.external.host=localhost
    cometd.external.port=18686
    cometd.external.protocol=http
    #cometd configurations end
    ```

    c. Stop Unified Self-Service Jetty server from service.msc.

Unified Self-Service node 1 is configured.

Install and Configure Apache Solr

Install Apache Solr on the Unified Self-Service common server.

Follow these steps:

1. Download Solr 1.4.1 on the Unified Self-Service common server. For more information, see any Solr website, example, http://archive.apache.org/dist/lucene/solr/1.4.1.

2. From the Solr distribution, copy example folder so that Unified Self-Service is also at the same level.

3. Define the environment variable as the location for Solr to store the search index.
   Example: $SOLR_HOME=/openspace/solr

   > **Note:** This environment variable can be defined on the start up sequence of the operating system, in the environment for the user who is logged in, or in the start-up script for your application server. If you are using Tomcat to host Solr, modify setenv.sh or setenv.bat and add the environment variable there.

4. Use this environment variable as a parameter for JVM during the start up configuration of the application server.

   > **Note:** If you are using Tomcat, edit catalina.sh or catalina.bat and add the -Dsolr.solr.home=$SOLR_HOME to the $JAVA_OPTS variable.

5. Install Solr on the Unified Self-Service common server. For more information, see http://lucene.apache.org/solr.

   > **Note:** Install the Solr search engine on a separate machine from Liferay. To integrate Solr search engine with Liferay, restart the application server.

6. Shut down Solr.

7. From the Solr distribution, copy **solr.war** to the webapps directory of your servlet container.

8. Start Solr on the Jetty server:

   a. Go to $SOLR_HOME on the command prompt.

   b. Run java -Dsolr.solr.home=/openspace/solr -jar start.jar to set the java system property solr.solr.home.

Configure Liferay to use Solr for Searching

Do not run Liferay and Solr search engine on the same machine.

Follow these steps:

1. Install the Solr Liferay plugin on Unified Self-Service node 1.
2. Copy solr-web.war file from OSOP\tools to the OSOP\deploy folder of the Unified Self-Service installation directory.
3. Open solr-spring.xml from the WEB-INF/classes/META-INF folder.
4. Modify the following value to point to the server where Solr is up and running:

   ```
   <constructor-arg type="java.lang.String" value="http://localhost:8080/solr" />
   ```

5. Save the solr-spring.xml file and place it back in the plugin archive.
6. Copy the schema.xml file from the extracted solr-web folder (docroot/WEB-INF/conf) to $SOLR_HOME/conf folder of the Unified Self-Service common server.
7. Restart Solr on the Unified Self-Service common server.
   Liferay server search is now upgraded to use Solr.
8. From Unified Self-Service, select Control Panel, Server, Server Administration.
9. Click Execute button next to reindex all search indexes at the bottom of the page.
   Liferay will begin sending indexing requests to Solr for execution. Once Solr has indexed the data, a search server runs independently of all the Unified Self-Service nodes.The Unified Self-Service search now uses the Solr as the search index. This is ideal for a clustered environment, as it allows all the Unified Self-Service nodes to share one search server and one search index, and this search server operates independently of all the nodes.

Set up and Configure Node 2

Set up and configure Unified Self-Service on node 2 for the cluster environment.

Follow these steps:

1. Stop the Unified Self-Service services on node 1.
2. Create backup of node 1:
   - (Windows) Run TakeBackup.bat from the bin folder of the Unified Self-Service installation directory.
   - (Linux) Run TakeBackup.sh

   Backup is created in Unified Self-Service_installation\CAOpenSpaceBackup.car file of the Unified Self-Service installation directory.

3. On node 2, install the similar configuration Unified Self-Service as set up in node 1:

    a. Select Use existing database option.

    b. Ensure that you use the same database host name as used during the Unified Self-Service node1 setup.

    c. Select node1 backup CAOpenSpaceBackup.car.**Note:** Ensure user has all the privileges according to the basic installation.

    d. Ensure that you extracted the custom-ehcache.zip file in the OSOP\tomcat-7.0.40\webapps\ROOT\WEB-INF\classes\ folder of the Unified Self-Service installation directory.

    > **Important!** Ensure that after the extraction, the custom-ehcache folder is created in the same path as the **hibernate-clustered.xml** and **liferay-multi-vm-clustered.xml** files.

    e. Open the server.xml file from the OSOP\tomcat-7.0.40\conf\ folder and replace <Engine name="Catalina" defaultHost="localhost"> with <Engine name="Catalina" defaultHost="localhost" jvmRoute="node2">.

After the successful configuration, two Unified Self-Service nodes run with the same database in a cluster.

Configure the Load Balancer

Configure the load balancer to increase scalability and to maintain performance.

Follow these steps:

1. Download and install Apache HTTP server 2.2.
2. Download mod_jk.so (http://mod_jk.so) and copy it to APACHE_HOME\modules\ directory.
3. Modify the APACHE_HOME\conf\httpd.conf file:
    - Append the file with the following lines:

```
JkWorkersFile conf/workers.properties

JkLogFile logs/mod_jk.log

JkLogLevel info

JkLogStampFormat "[%a %b %d %H:%M:%S %Y]"

JkMount /* loadbalancer
```

    - Add the following entry in the httpd.conf file (if not added):

```
# Load the mod_jk connector

LoadModule jk_module modules/mod_jk.so
```

4. Define the IP addresses of node1 and node 2 in the APACHE_HOME\conf\workers.properties file:

   ```
   worker.node1.host = <IP ADDRESS OF NODE1>
   worker.node2.host = <IP ADDRESS OF NODE2>
   ```

5. Start load balancer.

6. On the client machine (from where you are accessing Unified Self-Service) modify C:\Windows\System32\drivers\etc\host file to point to the IP address of the Load Balancer. For example, if you on boarded a tenant with virtual host as test.openspace.com (http://test.openspace.com) and the IP address of the Apache server is 10.11.12.13, then you have to add 10.11.12.13 test.openspace.com (http://test.openspace.com) line in the host file. This allows access to the virtual host from the client machine.
   Load balancer is configured.

7. Stop the Unified Self-Service services on node 1 and verify that requests are getting mapped to node 2 even if node 1 is down.

Uninstall CA Service Management 14.1

This article contains the following topics:

After you have uninstalled CA Service Management product or products from a system, you must remove the database details from that system. To remove the database details, see Run the Database Cleanup Utility (see page 627)topic

Uninstall CA Asset Portfolio Management

You can uninstall the CA Asset Portfolio Management 14.1 components except CA MDB. CA MDB cannot be uninstalled.

Follow these steps:

1. From the Start menu on a CA Service Management Release 14.1 server, navigate to **Control Panel**, **Programs**.

2. Select **Programs and Features**. Locate and double-click CA Asset Portfolio Management.

3. Select Uninstall and follow the on-screen wizard instructions.
   CA APM 14.1 is uninstalled.
   If you have installed CA APM on multiple servers, uninstall these installations in a similar way.

Uninstall CA Service Catalog

You can uninstall CA Service Catalog and CA EEM from one or more computers.

Follow these steps:

1. Stop all CA Service Catalog Windows services on all computers.

2. Open the Windows Control Panel, select CA Service Catalog, and click Uninstall.

   Note: The CA Service Catalog data in the MDB is saved for any future CA Service Catalog installations in your enterprise. If you delete the MDB data, you cannot recover it.

3. If no other CA Technologies products in your enterprise use CA EEM, use the Windows Control Panel to uninstall it.

   Important! Before you uninstall CA EEM, unregister all registered applications. For more information, see your CA EEM documentation.

4. (Optional) Review the uninstallation log files in the Windows Temp directory:

   - CA_Service_Catalog_view.log
   - CA_Service_Catalog_Uninstall.log

Note: Tomcat and the JRE are installed automatically during the CA Service Catalog installation. They are also uninstalled automatically during the CA Service Catalog uninstallation.

After Uninstalling Service Catalog, you must uninstall CA Service Management Administration.

Uninstall CA Service Desk Manager

To uninstall CA Service Desk Manager,

1. Depending upon the operating system,
   - (Windows) From the Start menu, select All Programs, CA, Service Desk Manager, Uninstall.
   - (Linux/ UNIX) Go to the directory where you installed CA SDM (NX_ROOT/SDUninstall) and use ./SDUninstall.

   A message window appears.
2. Click Next.
3. Choose the option to keep all the files or to remove them during the uninstallation, and click Next.
4. Choose the services that you want to shutdown and click Next.
5. After the services are stopped, click Uninstall.
   The uninstallation process starts.
6. Select the option to restart the system (recommended for Windows) after the uninstallation and click Done.

At the end of the topic, you have successfully uninstalled CA SDM. Proceed to run the UninstallCleanup utility (see page 627).

Uninstall Unified Self-Service

Uninstall Unified Self-Service, if you no longer need it. Before uninstalling, ensure that you install JRE 1.7.51 or later and set JAVA_HOME to the JRE path. Make sure to add JAVA_HOME in the Environment PATH variable.

Follow these steps:

- (Windows) Click Start, All Programs, CA, Unified Self-Service, Change Unified Self-Service Installation, and select Uninstall Product. You are prompted to take the backup. Click OK.
  A CAOpenSpaceBackup.car backup file is created under the path C:\CA_Open_Space_Backup.
- (Linux) Navigate to the install directory, run Change Unified Self-Service Installation, and select Uninstall Product. You are prompted to take the backup. Click OK.
  A CAOpenSpaceBackup.car backup file is created under the path \CA_Open_Space_Backup.
  The installed directories and files are deleted from the system but the database is not deleted.

Run the Database Cleanup Utility

During the installation of CA Service Management 14.1 products, each of the installed product is registered in a common mdb table that is reflected in the deployment summary of the selected environment. These entries must be cleared in the following cases:

- Uninstallation of any CA Service Management products

- Moving Database or migration from one server to another

Run the CA Service Management database cleanup utility on a Windows or a Non-Windows environment. The database cleanup utility removes the entries and adds these to the following tables:

Table Name from where the entries are removed	Table Name to which the removed entries are added
al_cdb_componentinstallstate	al_cdb_comp_installstate_bkup
al_cdb_configurationparameters	al_cdb_config_params_backup

Note: On a Non-Windows Platform, before running the **DBCleanup.sh** Utility, you must export the Oracle Environment variables on the terminal.

Follow these steps:

1. Navigate to *DVD1\DBCleanupUtility* directory.
2. For Windows, double-click the **DBCleanupUtility.bat** to launch the DBCleanup utility.
   On a Non-Windows platform, you must run the **DBCleanupUtility.sh** file.
3. Enter the following details:
   a. **Database Server Type**: Specify the type of server, MS SQL or Oracle.
   b. **Database Host Name:** Enter the host name of the server where the database resides.
   c. **Database User Name**:
      - **SQL Server**: Enter the privileged user detail that has permission to create and modify schema.
      - **Oracle**: Provide the mdbadmin user name.
   d. **Database Password**:
      - **MS SQL**: Enter the database password used by the database admin user.
      - **Oracle**: Enter the password for the Oracle database user.
   e. **Database Port Number:** Provide the database port number.
   f. **Enter Database Name:** Enter the database name. For example, mdb.
   g. **System Name**: Provide the host name of the system from where you want to uninstall the CA Service Management product or products.
4. Select any of the following products that you want to uninstall:

- **SDM -** CA Service Desk Manager.
- **SLCM-** CA Service Catalog.
- **ITAM -** CA IT Asset Manager.
- **USS -** Unified Self-Service.
  The utility cleans up the database and removes the entries of the selected product installed on the server.

Implementing CA Service Management Release 14.1.01

This topic contains the following information:

CA Service Management 14.1.01 is a cumulative patch that has several enhancements and bug fixes (see page 91) on top of CA Service Management 14.1. All the necessary files that are required for the patch installation are packaged as a .CAZ or .tar.Z files available at CA Support Online.

Installation on Windows Operating System

- Navigate to the folder where you downloaded the cumulative patch .tar.Z file and run the following command run the following command: CA Service Desk Manager
- CA Asset Portfolio Management
- CA Service Catalog
- Unified Self-Service

Note: CA Service Desk Manager (Windows) users need to apply the mandatory patch RO80745 after applying the cumulative patch.

Follow these steps:

1. Download the Cumulative Patch (.caz) file from http://ca.com/support.

2. Download the cazipxp.exe (available inside the APPLYPTF) utility from http://supportconnectw.ca.com/public/ca_common_docs/latest_applyptf.asp.
   Copy the cazipxp.exe file to the same folder as the downloaded cumulative .CAZ file. Ignore this step if you already have cazipxp.exe file.

3. In the Windows command prompt, navigate to the folder where you downloaded the cumulative patch .caz file and run the following command:

   ```
   cazipxp.exe –u <Cumulative Patch.caz>
   ```

4. After the command is executed, the following files are available in the same folder:
   RO80231.caz
   Contains the necessary patch installation files for CA SDM.
   RO80262.caz
   Contains the necessary patch installation files for CA APM.
   RO80252.caz
   Contains the necessary patch installation files for CA Service Catalog.
   RO80300.caz
   Contains the necessary patch installation files Unified Self-Service.
   Product Readme Files
   The readme files contain information about the new features in the patch, the installation instructions, and other important information about the patch.

   Note: CA SDM users can also use APPLYPTF for applying the patch. The respective patches are copied to :

   - $NX_ROOT\patches\SDM_CUM1
   - $NX_ROOT\patches\APM_CUM1
   - $NX_ROOT\patches\CATALOG_CUM1
   - $NX_ROOT\patches\USS_CUM1

   Depending on the product patch you want to install, you must extract the corresponding .caz file. For example, for CA SDM, extract RO80231.caz file.

5. To extract the patch installation files, in the Windows command prompt, run the following command:

   ```
   cazipxp.exe –u <.caz file of the product>
   ```

   For example, for CA Service Catalog, run the following command:

   ```
   cazipxp.exe –u RO80252.caz
   ```

6. The patch installation procedure depends on the product you want to install. The extracted files contain a readme file that has all the necessary installation instructions. Follow the steps and complete the patch installation.

Installation on Linux Operating System

On a Linux operating systems, you can apply the patch for the following products:

- CA Service Desk Manager
- Unified Self-Service

Note: CA Service Desk Manager(Linux) users need to apply the mandatory patch RO80746 after applying the cumulative patch.

Follow these steps:

1. Download the Cumulative Patch (.tar.Z) file from http://ca.com/support.
   Copy the files for the cumilative patch in the $NX_ROOT/Patches directory. The $NX_ROOT /Patches directory may not exist if this is the first patch you are applying on your environment. You must manually create the folder and copy the files.

2. Navigate to the folder where you downloaded the .tar.Z file and run the following command:

   ```
   tar -xvzf <Cumulative_Patch.tar.Z>
   ```

3. After the command is executed, the following files are available in the same folder:
   RO80302.tar.Z
   Contains the necessary patch installation files for CA SDM.
   RO80301.tar.Z
   Contains the necessary patch installation files Unified Self-Service.
   CA_SDM_14_1_01_Readme.pdf
   The readme file contains information about the new features in the patch, the installation instructions, and other important information about the patch.

   Depending on the product patch you want to install, you must extract the corresponding .tar. Z file. For example, for CA SDM, extract the RO80302.tar.Z file.

4. The patch installation procedure depends on the product you want to install. The extracted files contain a readme file that has all the necessary installation instructions. Follow the steps and complete the patch installation.

5. To apply the patch run the following command:

   ```
   applyptf.<OS type> -r $NX_ROOT/Patches/RO80302.jcl -e $NX_ROOT
   ```

Installation on AIX or Solaris Operating System

On AIX and Solaris operating systems, you can apply the patch for CA Service Desk Manager.

Note: CA Service Desk Manager users need to apply the mandatory patch RO80747(For Solaris) and RO80748 (For AIX) after applying the cumulative patch.

Follow these steps:

1. Download the Cumulative Patch (.tar.Z) file from http://ca.com/support.

2. Copy the files for the cumulative patch in the $NX_ROOT/Patches directory. The $NX_ROOT /Patches directory may not exist if this is the first patch you are applying on your environment. You must manually create the folder and copy the files.

3. Navigate to the folder where you downloaded the cumulative patch .tar.Z file and run the following command:

   ```
   uncompress $NX_ROOT/Patches/<Cumulative_Patch.tar.Z>
   tar -xvf $NX_ROOT/Patches/<Cumulative_Patch.tar.Z>
   ```

4. After the command is executed, the following files are available in the same folder:

   For Solaris: **RO80304.tar.Z**

   For AIX: **RO80305.tar.z**

   CA_SDM_14_1_01_Readme.pdf
   The readme file contains information about the new features in the patch, the installation instructions, and other important information about the patch.

   Depending on the product patch you want to install, you must extract the corresponding .tar. Z file. For example, for CA SDM, extract the RO80304.tar.Z file.

5. The patch installation procedure depends on the product you want to install. The extracted files contain a readme file that has all the necessary instructions. Follow the steps and complete the patch installation.

6. To apply the patch run the following command:
   For AIX:

   ```
   applyptf.<OS type> -r $NX_ROOT/Patches/RO80305 .jcl -e $NX_ROOT
   ```

   For Solaris:

   ```
   applyptf.<OS type> -r $NX_ROOT/Patches/RO80304 .jcl -e$NX_ROOT
   ```

Install CA Service Desk Manager Release 14.1.01

Important! All components of the cumulative patch are supplied and implemented in English and all supported languages. However, the updates from the patch to the UI elements, utilities, messages, and so on appear in their respective language based on the product installation. Please go through the readme before applying the patch and ensure that you perform the post installation steps.

To help you plan for a successful implementation of Cumulative Patch, you must meet the following prerequisites:

- To install and use the cumulative patch, ensure that CA Service Desk Manager 14.1 is already installed. For information, visit CA Technical Support (http://ca.com/support). (http://ca.com/support.)
- Ensure that you read the enhancements and new features (see page 109) available for CA SDM, after applying this patch.
- Back up your system and database before installing the cumulative patch. This is necessary in case any problems are encountered during the cumulative patch installation.

Complete the following steps to apply the cumulative patch to CA Service Desk Manager 14.1:

For Windows:

1. Apply RO80231.caz which is extracted from CASM 14.1.01 cumulative patch.
2. If you do not have the ApplyPTF utility, download it from CA Technical Support (http://ca.com/support).
3. Shutdown the CA SDM services in all the servers.
4. Depending on the CA SDM configuration, complete one of the following steps:
   - (Advanced availability configuration) Log in into the standby server, which you are planning to promote as the new background server.
   - (Conventional configuration) Log in to the primary server.
5. Run the APPLYPTF command.
6. Select the ApplyPTF to local or remote nodes option and click Next.
7. Click Browse and select RO80231.caz file from $NX_ROOT\Patches\SDM_CUM1\ or from the location where the caz file has been extracted.
8. Leave all other options unchanged unless the node name is incorrect.

9. Click Next to install the patch.
   Once this patch is installed successfully, find the following files under the $NX_ROOT\Patches folder:

   - Language independent patch: RO80230
   - Language dependent patch: RO802229
   - Language independent patch readme: RO80230.TXT
   - Language dependent patch readme: RO80229.TXT

10. Apply the language independent patch first and then apply the language dependent patch (follow the instructions provided in the respective readmes).

For Non-Windows:

1. Apply the following patch (which is extracted from CASM 14.1.01 cumulative patch), depending on your non- windows environment:

   - (Linux) RO80302.tar.Z
   - (AIX) RO80305.tar.Z
   - (Solaris) RO80304.tar.Z

2. If you do not have the ApplyPTF utility, download it from CA Technical Support (http://ca.com/support). (http://ca.com/support.)

3. Depending on your non-windows environment, extract the patch file in the $NX_ROOT/Patches/SDM_CUM1/ directory:

   Note: The $NX_ROOT/Patches/SDM_CUM1/ directory may not exist, if you are applying the fix for the first time. In such a case, you must create it manually.

   - For Linux, unzip the patch file using tar -xvzf RO80302.tar.Z
   - For AIX, uncompress and untar the patch file as follows:

     a. i. uncompress $NX_ROOT/Patches/RO80305.tar.Z

        ii. tar -xvf $NX_ROOT/Patches/RO80305.tar

   - For Solaris, uncompress and untar the patch file as follows:

     a. i. uncompress $NX_ROOT/Patches/RO80304.tar.Z

        ii. tar -xvf $NX_ROOT/Patches/RO80304.tar

4. To apply the patch, run the following command, depending on your non-windows environment:
   - (Linux) applyptf.<OS type> -r $NX_ROOT/Patches/RO80302 .jcl -e $NX_ROOT
   - (AIX) applyptf.<OS type> -r $NX_ROOT/Patches/RO80305 .jcl -e $NX_ROOT
   - (Solaris) applyptf.<OS type> -r $NX_ROOT/Patches/RO80304 .jcl -e $NX_ROOT
5. When this patch is installed successfully, find the following files under the $NX_ROOT/Patches folder:
   a. For Linux:
      - Language independent patch: RO80249
      - Language dependent patch: RO80248
      - Language independent readme: RO80249.TXT
      - Language dependent readme: RO80249.TXT
   b. For AIX:
      - Language independent patch: RO80271
      - English language patch: RO80272
      - Language independent readme: RO80271.TXT
      - English readme: RO80272.TXT
   c. For Solaris:
      - Language independent patch: RO80258
      - Language dependent patch: RO80278
      - Language independent readme: RO80258.TXT
      - Language dependent readme: RO80278.TXT
6. Apply the language independent patch first and then apply the language dependent patch (follow the instructions provided in the respective Readmes).

Note: When the patch is successfully applied, before uploading any attachments, check ALL repositories and re-select the correct Servlet Server if needed. If the files that are replaced during the patch application process are not available in the expected locations then the patch was not applied properly. Review the Applyptf log file for additional information or contact CA Technical Support (http://ca.com/support) for assistance.

See the respective Post_Installation_and_Backout_Steps located in $NX_ROOT/doc folder to complete the patch installation process.

You may find the following known issues associated with this patch:

- Unable to Batch Import Knowledge Documents Using the keit_daemon Command (see page 152)
- Auto Refresh does not work when an existing attachment or URL is deleted or detached from a Configuration Item (see page 178)

Implementing CA IT Asset Manager Release 14.1.01

Complete the following steps to apply the cumulative patch to CA IT Asset Manager 14.1:

Verify the Prerequisites

- To apply cumulative patch 14.1.01, you must have already installed CA APM 14.1 GA.
- If you have installed CA APM 12.9, you must first upgrade to CA APM 14.1 and then apply the cumulative patch.

Install the Patch

Follow these steps:

1. Download the CA APM 14.1.01 cumulative patch from CA Support Online to the CA APM application server in the APM_14_1_01 folder.
2. Run the cazipxp.exe –u RO80262.caz command to unzip the CA APM 14.1.01 cumulative patch (caz file) in the same folder:
3. Verify that the following files are available:

- MDB.exe
- Setup.bat
- Patch.msp

4. Double click and extract ‘MDB.exe’ to get MDB folder.
5. Complete the following steps to u pdate the web server, application server components and database.

> **Note:** Please apply the Database patch first and then apply the patch in the application and webserver components.

- Log in to the application server where you downloaded and extracted the patch. From the command prompt, go to the APM_14_1_01 folder. To apply the database patch, use the following command.

> **Important!** We recommend that you back up your MDB database before you perform the MDB update. If your MDB update fails, restore the backup and start the installation again. We do not recommend that you reinstall the MDB update in the same environment where the MDB update failed.

For **SQL Server**, execute the following command:

```
setup.bat -SERVERTYPE=DB -DBVENDOR=mssql -DBNAME=<mdb_name> -DBHOST=<database_hostname> -
DBUSER=<database_username> -DBPASSWORD=<database_password> -MANIFEST=Unicenter_Asset_Portfolio_Management -
WORKSPACE=UAPM
```

SERVERTYPE
SERVERTYPE is DB, for database patch application.

DBVENDOR
Specifies the database vendor name. Enter mssql for SQL Server.

DBNAME
Specifies the existing CA APM Release 14.1 MDB database name.

DBHOST
Specifies the database server system host name.

DBUSER
Specifies the existing CA APM Release 14.1 MDB database user name.

DBPASSWORD
Specifies the existing CA APM Release 14.1 MDB database password.

Important! The -DBUSER and -DBPASSWORD parameter values must match your existing CA APM Release 14.1 database user name and password.

MANIFEST
Specifies the name of the manifest file. Do not change the default value for this parameter.

WORKSPACE
Specifies the name of the workspace. Do not change the default value for this parameter.

For **Oracle Server**, execute the following command:

```
setup.bat -SERVERTYPE=DB -DBVENDOR=oracle -DBNAME=<oracle_service_name> -DBHOST=<database_hostname> -
DBUSER=<database_username> -ORA_TBLSPACE_PATH=<tablespace_path> -DBPASSWORD=<database_password> -
MDB_ADMIN_PSWD=<mdb_administrator_password> -MANIFEST=Unicenter_Asset_Portfolio_Management -WORKSPACE=UAPM
```

SERVERTYPE
SERVERTYPE is DB, for database patch application.

DBVENDOR
Specifies the database vendor name. Enter oracle for Oracle.

DBNAME
Specifies the existing Oracle Service name.

DBHOST
Specifies the database server system host name.

DBUSER
Specifies the existing Oracle database user name.

ORA_TBLSPACE_PATH
Specifies the path to the Oracle tablespace.

DBPASSWORD
Specifies the existing Oracle database password

Important! The -DBUSER and -DBPASSWORD parameter values must match your existing CA APM Release 14.1 database user name and password.

MDB_ADMIN_PSWD
Specifies the existing MDB administrator password.

MANIFEST
Specifies the name of the manifest file. Do not change the default value for this parameter.

WORKSPACE
Specifies the name of the workspace. Do not change the default value for this parameter.

6. To update the application server, copy the folder APM_14_1_01 to the Application server. In the command prompt, go to the APM_14_1_01 folder and run the following command.

   ```
   Setup.bat -SERVERTYPE=APP
   ```

   Note: If the Application server and the Web server components reside on the same Machine, you can ignore step 7.

7. To update the web server, copy the folder APM_14_1_01 to the Web server. In the command prompt, go to the APM_14_1_01 folder and run the following command.

   ```
   Setup.bat -SERVERTYPE=WEB
   ```

Verify the Cumulative Patch Installation

After you have completed all installation procedures, you can verify that CA APM 14.1.01 and the database upgrade were performed successfully.

Database upgrade verification

1. Login to the server where you downloaded and extracted the CA APM 14.1.01 cumulative patch.
2. Navigate to the folder where you downloaded and extracted the CA APM 14.1.01 cumulative patch (APM_14_1_01).
3. Navigate to the MDB\mdb1.5 folder.
4. Open the install_<databasename>.log file with a text editor.

   Note: In the log file name, database name is replaced with the name of the database. For example, if the database name is test, the log file name is install_test.log.

5. Verify that a message similar to the following message appears at the end of the log file:

   'MDB setup completed successfully'.

Cumulative Patch verification

1. Login to APM application.

2. After a successful login click on ‘About’ link (top-right).
   The display should be:
   Release: 14.1.1.28

3. Verify the ITAMMSP.log file in the system drive.

4. In the Add/Remove Programs, click View Installed Updates and verify the entry **CA ITAM 14.1.01.**

Install Localization Update on the Cumulative Patch

After you verify the cumulative patch installation, you must install the localization update for languages other than English.

Follow these steps:

1. Log in to the Application Server.

2. In the Windows command prompt, navigate to <ITAM installation folder>\L10N\language_pack.

3. Run the following command:

   ```
   SetSeeddata.exe <language code-country code>
   ```

   For example, SetSeeddata.exe de_DE. The language codes are same as the folder names present at this location.

4. Verify the LOGSetSeeddata.log file.

Uninstall CA APM 14.1.01

You can decide to uninstall CA APM from a computer for various reasons. For example, you can uninstall CA APM because you decided to use the computer for a different purpose or to move the components to another computer.

Note: The MDB upgrade cannot be reverted. To revert the MDB changes, restore the previous database backup.

Follow these steps:

1. Login to the servers (Application & Web) where you installed CA APM 14.1.01.

2. Go to Control Panel > Programs and Features and click View installed updates.

3. Right-click on CA ITAM 14.1.01 and select Uninstall to uninstall this cumulative patch.

Enhancements

Ensure that you read the enhancements and new features (see page 91) available for CA APM, after applying this patch.

Maintenances

Cumulative#	Testfix#	Title	Description
APM 14.1.01	T5E2402	NON ADMIN USERS FAILS TO LOG IN	Issue with non admin users logging into APM.
	T5M7130	CAN'T UPDATE COST RECORD	Unable to update cost record extensions.
	T5E2402	METADATA DOESN'T FRESH ON ALL SERVERS IN LOAD BALANCING ENVIRONMENT.	In NLB environment, extensions created from one server are not available from other server without resetting IIS.
	NA	INTERNET EXPLORER RENDERING.	Internet explorer rendering issues.
	NA	PATCH OVERRIDING IIS SETTINGS AND ENABLING WINDOWS AUTHENTICATION.	Patch overriding IIS settings and enabling windows authentication.
	NA	IP ADDRESSES NOT SHARED	IP no synced with SAM and APM.
	T5E2404	UNABLE TO UPDATE ASSET SECONDARY LOOKUP	Unable to update Location and Contact as secondary lookup of an asset.
	NA	MAC ADDRESS FIELD SMALL	MAC address coming from SAM update.
	T5E2402	INACTIVATE ROLE	Unable to save set role to inactive.
	T5GJ134	CLEAR EXCEPTION MESSAGE NOT DISPLAYED	Import job errors out with inappropriate Exception message.
	T5E2408	ITAM-12.9-INVALID CA_ASSET ROWS	Data importer job fails to create an asset.
	T5XU059	DATA IMPORT LOG FILES LINE NUMBER ISSUE	Issue with data importer log files.
	T5E2404	UNABLE TO UPDATE ASSET SECONDARY LOOKUP	Unable to update Location and Contact as secondary lookup of an asset.
	T5GJ138	[CONFIGURATION] CANNOT REMOVE FOREIGNGROUP LEVEL 2 OR MORE REQUIRED FIELDS.	Unable to remove from the configuration the additional fields associated to related objects.
	T5E2402	ITAM - 12.9 - ERROR WHEN CREATING FILTER	Date filter saving issues.

Cumulative#	Testfix#	Title	Description
	T5GJ133	DATA IMPORTER - IMPROPER LOG RESULTS	Data importer doesn't show log results correctly as processed.
	T5M7120	UNABLE TO CLEAR DATE FIELD	Try to import by giving null values for any date field. Get the exception in the log.
	T5M7120	ERROR CREATING SEARCHES	The search does not give the Save successful message and also throws an exception when the search is brought up.
	T5UM103	LIFECYCLE STATUS DATE CHANGE	The life cycle status date is not changing when the life cycle status is updated.
	T5UM103	UNHANDLE SQL EXCEPTION	Infrequent error when using APM.
	T5GJ140	UNABLE TO SAVE ANY EXISTING CONTACT RECORDS	The application encountered an error while saving an object that references other objects. Contact ID contains invalid reference key.
	T5M712	EXTENDED FIELD NOT SHAREABLE	The extended field should be available for selection.
	T5GJ137	HARDWARE RECONCILIATION THROWING ERROR LAST_UPDATE_DATE=NULL	A reconciled computer deleted from ITCM interface and the ITAM Hardware Engine is executed last_update_date to NULL.
	T5EM232	CANNOT DELETE FIELD ON ASSET	Can not delete field from GUI.
	T5E2406	ITAM - 12.9 -EVENT SERVICE LIFECYCLE STATUS	NA
	NA	[WCF] USER SHOULD BE ABLE TO UPDATE LAST UPDATE OR CREATION DATES AS NEEDED.	Last update user set up.
	T5M7125	UNABLE TO ADD FIELD IN CONF	In Asset Configuration ON mode, we are unable to add Legal Status History Fields to Legal Documents for Assets.
	T5GJ135	HIDE INTERNAL ATTRIBUTES FROM 'ADD EXISTING FIELDS' POPUP - CONFIGURATION	ITAMService.log shows that the code is attempting to add data into the arg_allocation_summary_view table, even though these fields are hidden on the configuration.
	NA	IMPORT JOB ERROR	Import job errors out with inappropriate Exception message.
	T5XU050	READ-ONLY PERMISSIONS ISSUE FOR NON-ADMIN USERS	Read-Only permissions issue for Non-Admin users.
	T5GJ134	NULL EXCEPTION MESSAGE IN WEB SERVICE	Exception Message: Web Service threw exception in data importer.
	T5M7120	UNABLE TO CLEAR DATE FIELD	When importing by giving null values for any date field. Get the exception in the log.

Cumulative#	Testfix#	Title	Description
	T5JH194	SORTING IMPORTER JOBS ON JOB ID IN ASCENDING ORDER	Unable to sort Import Jobs on Job Id in Ascending direction.
	T5EM232	ERROR ON DEAUTHORIZE	Unable to de authorise user from user management.
	T5EM232	AUTHORIZE USERS SEARCH	When searching for authorise users are performing an Or as opposed to an And.
	T5EM232	ERROR ON CHANGE MODEL WIZARD	APM fails to run change model wizard, tried to execute a model change from/to the same asset family.
	T5GJ138	CANNOT FIND CONTACT /ROLE	Unable to search for the user already existing.
	NA	HW RECON-LIFECYCLE STATUS ERR	updates are failing and ITAMHWEngine.log is throwing numerous errors.
	T5UM105	ISSUE WITH ASSET AUDITS	NA
	T5UM104	ISSUE WITH CONFIGURATION: ASSET ENTITLEMENTS	All links in Asset Entitlements do not show in configuration ON mode in software asset.
	T5UM092	FILTER VALUES CASE SENSITIVE	Organisation save throws error"The User is not authorized to modify the asset due to the filter".
	T5EM227	IMPORT JOB ERROR	Data Importer fails to import assets when main destination object is set to 'Asset (All Families)'
	T5EM226	AUTOCOMPLETE NOT WORKING	The autocomplete function is not working on lookup fields in the 'additional information' section of the asset details page.

Upgrade to CA Service Catalog Release 14.1.01

This Readme contains instructions on how to download and install the CA Service Catalog 14.1.01 patch updates.

Note: All components of the CA Service Catalog 14.1.01 patch are supplied and implemented in English only. For example, the installation program for the patch runs in English only. However, the updates from the patch to the CA Service Catalog UI elements, utilities, messages, and so forth appear in the chosen product installation language. These updates function the same way in both English and non-English environments. Therefore, you can install the patch in both environments to obtain the latest updates to the product.

We strongly recommend that in addition to applying the patch, you must also configure the Secure Socket Layer (SSL). Instructions for enabling SSL can be found in the CA Service Catalog documentation wiki (https://wiki.ca.com/display/CASM1401/Configure+CA+Service+Catalog+to+Use+Secure+Socket+Layer)along with other general security considerations. In addition, administrators must disable login using the HTTP GET method. To disable, set the Allow Login with GET configuration in CA Service Catalog Administration, Configuration, Single Sign On Authentication to No.

For information on Poodle Vulnerability and remediation steps to secure the Apache Tomcat server used by CA Service Catalog SSL (HTTPs), refer to technical document posted on CA Support: http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec1155961.aspx

Prerequisites

To help you plan for a successful implementation of the CA Service Catalog 14.1.01 patch, ensure that your environment meets the following prerequisites:

- To install and use the patch, ensure that you have installed CA Service Catalog 14.1. For information on this, visit http://ca.com/support.

- Back up your system and database before installing the patch. This is necessary in case any problems are encountered during the installation of the patch.
  For instructions, see Technical Document TEC472303, “Backup and Restore Procedures for CA Service Catalog Products” which is posted on http://ca.com/support.

How to Install the Patch

Follow these instructions to apply the patch on top of the CA Service Catalog 14.1 base version.

1. If you do not have the cazipxp.exe utility, download it from the CA Technical Support at http://ca.com/support.

2. Extract the patch setup file CA_SLCM_r14_1_01_Setup.exe from <Rxxxx.caz> by running the following command:

   ```
   cazipxp.exe –u < Patch cazip file>
   ```

3. Run the *CA_SLCM_r14_1_01_Setup.exe* on all the systems where you have installed the base version of CA Service Catalog 14.1. Follow the installation wizard to install the patch.

How to Uninstall the Patch

Follow these instructions to uninstall the patch:

1. Click **Control Panel**, **Programs and Features**.

2. Double click the CA Service Catalog r14.1.01 and follow the uninstallation wizard instructions to uninstall the patch.

CA Service Catalog Patch Enhancements

Note: For more information related to Patch enhancements, new features, new certifications, fixes, and other updates provided with the CA Service Catalog 14.1.01 patch, see CA Service Management Release 14.1.01 Enhancements (see page 91).

Files Affected

This section lists the files that are affected with the application of CA Service Catalog 14.1.01 Patch. Some of the files listed may not be present in your system depending on the CA Service Management products and components that you have installed.

Note: USM_HOME refers to the CA Service Catalog product install path.

If you have customized CA Service Catalog using the Customization Framework, note the following two locations where the files may get affected by this patch application:

- As a best practice, the customization of files must be implemented under USM_HOME\filestore\custom folder (and its sub folders). As such, after applying the patch, you may be required to merge the files from this folder (and its sub folders) with the new files delivered by the Patch. A list of the files being updated by the patch is documented in this section.
- Customizations outside the USM_HOME\filestore\custom folder (and its sub folders) must be backed up before applying the CA Service Catalog 14.1.01 patch. After applying the patch, you must re-implement the customizations on the new files delivered with the patch. The following files are updated with the patch application.

List of Files Affected

Following are the list of files that are replaced:

- USM_HOME\version.properties
- USM_HOME\accounting\scripts\MDB\SQL\seeddata_de_DE.properties
- USM_HOME\accounting\scripts\MDB\SQL\seeddata_fr_FR.properties
- USM_HOME\accounting\scripts\MDB\SQL\seeddata_it_IT.properties
- USM_HOME\accounting\scripts\MDB\SQL\seeddata_zh_CN.properties

- USM_HOME\catalog\content\ApplicationServices.xml
- USM_HOME\catalog\content\ApplicationServices_da_DK.properties
- USM_HOME\catalog\content\ApplicationServices_da_DK.xml
- USM_HOME\catalog\content\ApplicationServices_de_DE.properties
- USM_HOME\catalog\content\ApplicationServices_de_DE.xml
- USM_HOME\catalog\content\ApplicationServices_es_ES.properties
- USM_HOME\catalog\content\ApplicationServices_es_ES.xml
- USM_HOME\catalog\content\ApplicationServices_fi_FI.xml
- USM_HOME\catalog\content\ApplicationServices_fr_FR.properties
- USM_HOME\catalog\content\ApplicationServices_fr_FR.xml
- USM_HOME\catalog\content\ApplicationServices_it_IT.properties
- USM_HOME\catalog\content\ApplicationServices_it_IT.xml
- USM_HOME\catalog\content\ApplicationServices_ja_JP.properties
- USM_HOME\catalog\content\ApplicationServices_ja_JP.xml
- USM_HOME\catalog\content\ApplicationServices_nl_NL.xml
- USM_HOME\catalog\content\ApplicationServices_pt_BR.xml
- USM_HOME\catalog\content\ApplicationServices_sv_SE.xml
- USM_HOME\catalog\content\ApplicationServices_zh_CN.xml
- USM_HOME\catalog\content\CorporateServices.xml
- USM_HOME\catalog\content\CorporateServices_da_DK.xml
- USM_HOME\catalog\content\CorporateServices_de_DE.xml
- USM_HOME\catalog\content\CorporateServices_es_ES.xml
- USM_HOME\catalog\content\CorporateServices_fi_FI.xml
- USM_HOME\catalog\content\CorporateServices_fr_FR.xml
- USM_HOME\catalog\content\CorporateServices_it_IT.properties
- USM_HOME\catalog\content\CorporateServices_it_IT.xml
- USM_HOME\catalog\content\CorporateServices_ja_JP.xml

- USM_HOME\catalog\content\CorporateServices_nl_NL.xml
- USM_HOME\catalog\content\CorporateServices_pt_BR.xml
- USM_HOME\catalog\content\CorporateServices_sv_SE.xml
- USM_HOME\catalog\content\CorporateServices_zh_CN.xml
- USM_HOME\catalog\content\FacilitiesServices.xml
- USM_HOME\catalog\content\FacilitiesServices_da_DK.xml
- USM_HOME\catalog\content\FacilitiesServices_de_DE.xml
- USM_HOME\catalog\content\FacilitiesServices_es_ES.xml
- USM_HOME\catalog\content\FacilitiesServices_fi_FI.xml
- USM_HOME\catalog\content\FacilitiesServices_fr_FR.xml
- USM_HOME\catalog\content\FacilitiesServices_it_IT.properties
- USM_HOME\catalog\content\FacilitiesServices_it_IT.xml
- USM_HOME\catalog\content\FacilitiesServices_ja_JP.xml
- USM_HOME\catalog\content\FacilitiesServices_nl_NL.xml
- USM_HOME\catalog\content\FacilitiesServices_pt_BR.xml
- USM_HOME\catalog\content\FacilitiesServices_sv_SE.xml
- USM_HOME\catalog\content\FacilitiesServices_zh_CN.xml
- USM_HOME\catalog\content\ITServices.xml
- USM_HOME\catalog\content\ITServices_da_DK.xml
- USM_HOME\catalog\content\ITServices_de_DE.xml
- USM_HOME\catalog\content\ITServices_es_ES.properties
- USM_HOME\catalog\content\ITServices_es_ES.xml
- USM_HOME\catalog\content\ITServices_fi_FI.xml
- USM_HOME\catalog\content\ITServices_fr_FR.properties
- USM_HOME\catalog\content\ITServices_fr_FR.xml
- USM_HOME\catalog\content\ITServices_it_IT.properties
- USM_HOME\catalog\content\ITServices_it_IT.xml

- USM_HOME\catalog\content\ITServices_ja_JP.xml
- USM_HOME\catalog\content\ITServices_nl_NL.xml
- USM_HOME\catalog\content\ITServices_pt_BR.xml
- USM_HOME\catalog\content\ITServices_sv_SE.xml
- USM_HOME\catalog\content\ITServices_zh_CN.xml
- USM_HOME\catalog\content\NetworkServices.xml
- USM_HOME\catalog\content\NetworkServices_da_DK.xml
- USM_HOME\catalog\content\NetworkServices_de_DE.xml
- USM_HOME\catalog\content\NetworkServices_es_ES.xml
- USM_HOME\catalog\content\NetworkServices_fi_FI.xml
- USM_HOME\catalog\content\NetworkServices_fr_FR.xml
- USM_HOME\catalog\content\NetworkServices_it_IT.properties
- USM_HOME\catalog\content\NetworkServices_it_IT.xml
- USM_HOME\catalog\content\NetworkServices_ja_JP.xml
- USM_HOME\catalog\content\NetworkServices_nl_NL.xml
- USM_HOME\catalog\content\NetworkServices_pt_BR.xml
- USM_HOME\catalog\content\NetworkServices_sv_SE.xml
- USM_HOME\catalog\content\NetworkServices_zh_CN.xml
- USM_HOME\catalog\content\PersonnelServices.xml
- USM_HOME\catalog\content\PersonnelServices_da_DK.xml
- USM_HOME\catalog\content\PersonnelServices_de_DE.xml
- USM_HOME\catalog\content\PersonnelServices_es_ES.xml
- USM_HOME\catalog\content\PersonnelServices_fi_FI.xml
- USM_HOME\catalog\content\PersonnelServices_fr_FR.xml
- USM_HOME\catalog\content\PersonnelServices_it_IT.properties
- USM_HOME\catalog\content\PersonnelServices_it_IT.xml
- USM_HOME\catalog\content\PersonnelServices_ja_JP.xml

- USM_HOME\catalog\content\PersonnelServices_nl_NL.xml
- USM_HOME\catalog\content\PersonnelServices_pt_BR.xml
- USM_HOME\catalog\content\PersonnelServices_sv_SE.properties
- USM_HOME\catalog\content\PersonnelServices_sv_SE.xml
- USM_HOME\catalog\content\PersonnelServices_zh_CN.xml
- USM_HOME\catalog\content\ProjectServices.xml
- USM_HOME\catalog\content\ProjectServices_da_DK.xml
- USM_HOME\catalog\content\ProjectServices_de_DE.xml
- USM_HOME\catalog\content\ProjectServices_es_ES.xml
- USM_HOME\catalog\content\ProjectServices_fi_FI.xml
- USM_HOME\catalog\content\ProjectServices_fr_FR.properties
- USM_HOME\catalog\content\ProjectServices_fr_FR.xml
- USM_HOME\catalog\content\ProjectServices_it_IT.properties
- USM_HOME\catalog\content\ProjectServices_it_IT.xml
- USM_HOME\catalog\content\ProjectServices_ja_JP.xml
- USM_HOME\catalog\content\ProjectServices_nl_NL.xml
- USM_HOME\catalog\content\ProjectServices_pt_BR.xml
- USM_HOME\catalog\content\ProjectServices_sv_SE.xml
- USM_HOME\catalog\content\ProjectServices_zh_CN.xml
- USM_HOME\catalog\content\ReservationServices.xml
- USM_HOME\catalog\content\ReservationServices_da_DK.xml
- USM_HOME\catalog\content\ReservationServices_de_DE.xml
- USM_HOME\catalog\content\ReservationServices_es_ES.xml
- USM_HOME\catalog\content\ReservationServices_fi_FI.xml
- USM_HOME\catalog\content\ReservationServices_fr_FR.xml
- USM_HOME\catalog\content\ReservationServices_it_IT.xml
- USM_HOME\catalog\content\ReservationServices_ja_JP.xml

- USM_HOME\catalog\content\ReservationServices_nl_NL.xml
- USM_HOME\catalog\content\ReservationServices_pt_BR.xml
- USM_HOME\catalog\content\ReservationServices_sv_SE.xml
- USM_HOME\catalog\content\ReservationServices_zh_CN.xml
- USM_HOME\catalog\content\TelcomServices.xml
- USM_HOME\catalog\content\TelcomServices_da_DK.xml
- USM_HOME\catalog\content\TelcomServices_de_DE.xml
- USM_HOME\catalog\content\TelcomServices_es_ES.xml
- USM_HOME\catalog\content\TelcomServices_fi_FI.xml
- USM_HOME\catalog\content\TelcomServices_fr_FR.properties
- USM_HOME\catalog\content\TelcomServices_fr_FR.xml
- USM_HOME\catalog\content\TelcomServices_it_IT.properties
- USM_HOME\catalog\content\TelcomServices_it_IT.xml
- USM_HOME\catalog\content\TelcomServices_ja_JP.xml
- USM_HOME\catalog\content\TelcomServices_nl_NL.xml
- USM_HOME\catalog\content\TelcomServices_pt_BR.xml
- USM_HOME\catalog\content\TelcomServices_sv_SE.xml
- USM_HOME\catalog\content\TelcomServices_zh_CN.xml
- USM_HOME\catalog\content\itpam\contentpack\processes\Custom Operators\CA SLCM\EscalationProcess.xml
- USM_HOME\catalog\content\itpam\contentpack\scripts\seeddata_it_IT.properties
- USM_HOME\catalog\content\itpam\contentpack\scripts\seeddata_sv_SE.properties
- USM_HOME\catalog\scripts\MDB\SQL\seeddata_it_IT.properties
- USM_HOME\catalog\scripts\MDB\SQL\usm_rule_condition.xml
- USM_HOME\catalog\scripts\MDB_SantaFe\SQL\usm_rule_condition.xml
- USM_HOME\filestore\contentpacks\CA Service Management Content Pack 2.0.zip
- USM_HOME\filestore\contentpacks\CA_Service_Catalog_Demo_Content_10212013.zip

- USM_HOME\filestore\contentpacks\Localized Service Management Admin Content Pack for Oracle.zip
- USM_HOME\filestore\contentpacks\Localized Service Management Admin Content Pack for SQL.zip
- USM_HOME\filestore\contentpacks\Service Management Admin Content Pack for Oracle.zip
- USM_HOME\filestore\contentpacks\Service Management Admin Content Pack for SQL.zip
- USM_HOME\filestore\contentpacks\Service_Management_Content_Pack.zip
- USM_HOME\filestore\forms\AccessToServer_ja_JP.xml
- USM_HOME\filestore\forms\AppStarGroupAdd_ja_JP.xml
- USM_HOME\filestore\forms\emailOptions_ja_JP.xml
- USM_HOME\filestore\forms\EmployeeTermination_ja_JP.xml
- USM_HOME\filestore\forms\fileShareAccess_ja_JP.xml
- USM_HOME\filestore\forms\NameChange_it_IT.xml
- USM_HOME\filestore\forms\NameChange_ja_JP.xml
- USM_HOME\filestore\forms\NewEmployee_ja_JP.xml
- USM_HOME\filestore\forms\productInfo_ja_JP.xml
- USM_HOME\filestore\forms\serverNTAccess_ja_JP.xml
- USM_HOME\filestore\images\offerings\OotbOfferings\access security.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\access_existing_file_share.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\access_to_emailform.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\add_LDAP_Server.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\add_memory.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\add_user.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\application_env_setup.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\automatic_call_distributor.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\auto_integration.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\backup_pcdata.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\backup_serverdata.svg

- USM_HOME\filestore\images\offerings\OotbOfferings\business_card.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\business_continuity_planning.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\common_configuration.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\conference_bridge.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\contract_negotiation_request.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\corporate_callingcard.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\corporate_card.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\create_mailaccount.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\create_publicfolder.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\create_role.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\DatabaseManagement.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\delete_emailform.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\department_contract_sla.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\desk_phone.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\desk_phone_accessories.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\distribution_list_new.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\distribution_list_remove.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\distribution_list_subscribe.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\distribution_list_unsubscribe.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\employee_recognition.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\extent_reservation.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\fax.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\faxline.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\file_share.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\grantaccess_Finance.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\grantaccess_HR.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\grantaccess_salesmarketing.svg

- USM_HOME\filestore\images\offerings\OotbOfferings\handheld_device.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\host.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\import_users_from_ldap.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\increase_mailboxsize.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\install_upgrade_remove.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\jack_activation.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\knowledge_engineering.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\lan_sla.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\manage_LDAP_servers.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\manage_tenants.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\manage_user.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\map_roles.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\map_tenants.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\mobilephone_accessories.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\mobile_phone.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\multi_tenancy_setting.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\network.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\network_education.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\network_performance_testing.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\network_vulnarability_analysis.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\newfile_share.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\new_hire_onboard.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\new_project_request.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\new_service_offering.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\nonstandard_service_offering.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\pager.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\pc_loaner.svg

- USM_HOME\filestore\images\offerings\OotbOfferings\pre_production_scan.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_accessories.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_desktop.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_desktop_db_software.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_desktop_development_software.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_desktop_management_software.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_desktop_miscellaneous_software.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_desktop_office_software.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_desktop_projectmanagement_sof svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_desktop_reporting_software.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_desktop_software.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_HR_app.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_HR_inhouseapp.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_laptop.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_miscellaneoust_inhouseapp.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_miscellaneous_server_software.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_network_printer.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_operations_app.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_printer.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_procurement_app.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_salesmarketing_app.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_server.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_server_db_software.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\procure_server_software.svg

- USM_HOME\filestore\images\offerings\OotbOfferings\project_change_request.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\project_management_request.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\proxy_access.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\recover_mailbox.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\replace_monitor.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\reports_financial.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\reports_HR.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\reports_ITservice.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\reports_procurement.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\reports_salesmarketing.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\request_access.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\reserve_physical_machine.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\reserve_using_template.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\reserve_virtual_machine.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\restore_pcdata.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\restore_serverdata.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\return_reservation.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\service_decommission.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\service_quality_review.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\static_ip_request.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\sync_contact.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\tenant_onboard.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\vendor_management_request.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\vendor_product_evaluation.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\Video_conference.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\virus_protection.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\voice_mail.svg

- USM_HOME\filestore\images\offerings\OotbOfferings\vpn_access.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\wan_sla.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\webcast.svg
- USM_HOME\filestore\images\offerings\OotbOfferings\wirelessnetwork_sla.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\calendar_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\compass_data_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\data_certificate_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\Data_copy_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\data_ok_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\date_time_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\desktop_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\goblet_bronze_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\goblet_gold_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\goblet_silver_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\headset_data_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\laptop_2_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\laptop_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\office_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\software_data_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\spy_data_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\webcam_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\web_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\windows2003_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\windowsXP_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\windows_time_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\workstation_2_40.svg
- USM_HOME\filestore\images\rateplans\OotbOfferings\workstation_40.svg

- USM_HOME\filestore\plugins\ca.catalog.reservations-select-plugin\plugin.jar
- USM_HOME\filestore\plugins\ca.catalog.resources-select-plugin\plugin.jar
- USM_HOME\filestore\plugins\ca.catalog.samples.policy-plugin\plugin.jar
- USM_HOME\filestore\plugins\ca.catalog.samples.policy-plugin\policy.sample-src.zip
- USM_HOME\filestore\plugins\ca.catalog.samples.select-plugin\plugin.jar
- USM_HOME\filestore\plugins\ca.catalog.samples.select-plugin\select.sample-src.zip
- USM_HOME\filestore\plugins\ca.catalog.samples.table-plugin\plugin.jar
- USM_HOME\filestore\plugins\ca.catalog.samples.table-plugin\table.sample-src.zip
- USM_HOME\filestore\plugins\ca.catalog.servicedesk-select-plugin\plugin.jar
- USM_HOME\filestore\plugins\ca.catalog.servicedesk-select-plugin\plugin_it.properties
- USM_HOME\filestore\portlets\browse.war
- USM_HOME\filestore\portlets\request-edit.war
- USM_HOME\filestore\portlets\request-list.war
- USM_HOME\filestore\portlets\request.war
- USM_HOME\filestore\portlets\status.war
- USM_HOME\filestore\themes\common\css\request.widget.css
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USD_EX_CreateRequest_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_CreateITUSDChangeOrder_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_CreateUSDRequest_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_EX_addProcessInstanceToRec xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_EX_addProcessInstanceToRec xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_EX_addRequestItemPendingA xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_EX_getAssetUUIDByRequestI xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_EX_getAssetUUIDByRequestIt xml

- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_EX_getRequestHeader_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_EX_getRequestItemNotes_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_EX_getRequestItemStatus_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_EX_getRequestItems_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_EX_getRequestItem_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_EX_getRequestsByUserID_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_EX_updateRequestItemStatus.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_EX_updateRequestOfferingSt.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_FulfillmentUSDRequest_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_HW_Fulfillment_USD_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_Notify_Fulfillment_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_Notify_Procurement_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_Set_Fulfilled_it.xml
- USM_HOME\fulfillment\bin\processdefinitions\updateversion\USM_SW_Fulfillment_USD_it.xml
- USM_HOME\fulfillment\scripts\MDB\SQL\seeddata_it_IT.properties
- USM_HOME\fulfillment\WEK\CAFlow\client\sd_wf.jar
- USM_HOME\fulfillment\WEK\CAFlow\client\usm_idews.war
- USM_HOME\reporting\CABI\biar\SLCM_universe.biar
- USM_HOME\scripts\importContent.bat
- USM_HOME\scripts\mergetenants\utility.mergetenants.jar
- USM_HOME\view\conf\ESAPI.properties
- USM_HOME\view\scripts\EIAM\Safex\usm_create_application.xml
- USM_HOME\view\scripts\EIAM\Safex\usm_create_application_data.xml

- USM_HOME\view\scripts\MDB\mdb_usm_Windows.jar
- USM_HOME\view\scripts\MDB\SQL\seeddata_da_DK.properties
- USM_HOME\view\scripts\MDB\SQL\seeddata_de_DE.properties
- USM_HOME\view\scripts\MDB\SQL\seeddata_en_US.properties
- USM_HOME\view\scripts\MDB\SQL\seeddata_es_ES.properties
- USM_HOME\view\scripts\MDB\SQL\seeddata_fi_FI.properties
- USM_HOME\view\scripts\MDB\SQL\seeddata_fr_FR.properties
- USM_HOME\view\scripts\MDB\SQL\seeddata_it_IT.properties
- USM_HOME\view\scripts\MDB\SQL\seeddata_ja_JP.properties
- USM_HOME\view\scripts\MDB\SQL\seeddata_nl_NL.properties
- USM_HOME\view\scripts\MDB\SQL\seeddata_pt_BR.properties
- USM_HOME\view\scripts\MDB\SQL\seeddata_sv_SE.properties
- USM_HOME\view\scripts\MDB\SQL\seeddata_zh_CN.properties
- USM_HOME\view\scripts\MDB\SQL\usm_configuration.xml
- USM_HOME\view\scripts\MDB\SQL\usm_form_attributes_schema.xml
- USM_HOME\view\scripts\MDB\SQL\usm_guinode.xml
- USM_HOME\view\scripts\MDB\SQL\usm_guinode_content.xml
- USM_HOME\view\scripts\MDB\SQL\usm_rule.xml
- USM_HOME\view\scripts\MDB\SQL\usm_rule_action.xml
- USM_HOME\view\scripts\MDB\SQL\usm_rule_event_param.xml
- USM_HOME\view\scripts\MDB\SQL\usm_rule_event_type.xml
- USM_HOME\view\scripts\MDB_SantaFe\SQL\usm_configuration.xml
- USM_HOME\view\scripts\MDB_SantaFe\SQL\usm_form_attributes_schema.xml
- USM_HOME\view\scripts\MDB_SantaFe\SQL\usm_guinode.xml
- USM_HOME\view\scripts\MDB_SantaFe\SQL\usm_guinode_content.xml
- USM_HOME\view\scripts\MDB_SantaFe\SQL\usm_rule.xml
- USM_HOME\view\scripts\MDB_SantaFe\SQL\usm_rule_action.xml

- USM_HOME\view\scripts\MDB_SantaFe\SQL\usm_rule_event_param.xml
- USM_HOME\view\scripts\MDB_SantaFe\SQL\usm_rule_event_type.xml
- USM_HOME\view\webapps\usm\gwt_to_be_extracted.zip
- USM_HOME\view\webapps\usm\admin\deploy_Account.wsdd
- USM_HOME\view\webapps\usm\API\Plugins\allclasses-frame.html
- USM_HOME\view\webapps\usm\API\Plugins\allclasses-noframe.html
- USM_HOME\view\webapps\usm\API\Plugins\constant-values.html
- USM_HOME\view\webapps\usm\API\Plugins\deprecated-list.html
- USM_HOME\view\webapps\usm\API\Plugins\help-doc.html
- USM_HOME\view\webapps\usm\API\Plugins\index-all.html
- USM_HOME\view\webapps\usm\API\Plugins\index.html
- USM_HOME\view\webapps\usm\API\Plugins\overview-frame.html
- USM_HOME\view\webapps\usm\API\Plugins\overview-summary.html
- USM_HOME\view\webapps\usm\API\Plugins\overview-tree.html
- USM_HOME\view\webapps\usm\API\Plugins\serialized-form.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\CacheService.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\CatalogPlugin.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\package-frame.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\package-summary.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\package-tree.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\package-use.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\PluginContext.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\PluginDataException.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\class-use\CacheService.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\class-use\CatalogPlugin.html

- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\class-use\PluginContext.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\class-use\PluginDataException.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\forms\FDOption.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\forms\FDSelectDataProvi html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\forms\FDTableDataProvid html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\forms\FDTableRow.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\forms\package-frame.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\forms\package-summary.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\forms\package-tree.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\forms\package-use.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\forms\class-use\FDOption.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\forms\class-use\FDSelectDataProvider.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\forms\class-use\FDTableDataProvider.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\forms\class-use\FDTableRow.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\ApprovalLevel.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\Approver.ApproverType.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\Approver.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\ApproverGroup.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\ApproverGroup.Operation.html

- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\ApproverGroup.Requirement.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\AssignmentPolicy.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\GroupApprover.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\ManagerApprove.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\package-frame.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\package-summary.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\package-tree.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\package-use.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\UserApprover.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\class-use\ApprovalLevel.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\class-use\Approver.ApproverType.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\class-use\Approver.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\class-use\ApproverGroup.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\class-use\ApproverGroup.Operation.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\class-use\ApproverGroup.Requirement.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\class-use\AssignmentPolicyPlugin.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\class-use\GroupApprover.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\class-use\ManagerApprover.html

- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\policies\class-use\UserApprover.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\user\EemGroup.GroupType.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\user\EemGroup.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\user\package-frame.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\user\package-summary.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\user\package-tree.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\user\package-use.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\user\class-use\EemGroup.GroupType.html
- USM_HOME\view\webapps\usm\API\Plugins\com\ca\usm\plugins\apis\user\class-use\EemGroup.html
- USM_HOME\view\webapps\usm\API\SOAP\com.ca (http://com.ca).usm.soap.axisInterfaces.Offering.xml
- USM_HOME\view\webapps\usm\API\SOAP\com.ca (http://com.ca).usm.soap.axisInterfaces.User.xml
- USM_HOME\view\webapps\usm\API\SOAP\com.ca (http://com.ca).usm.soap.services.RequestServiceImplUtil.xml
- USM_HOME\view\webapps\usm\API\SOAP\com.ca (http://com.ca).usm.soap.services.WebServiceSession.xml
- USM_HOME\view\webapps\usm\explorer\addregaccount.xsl
- USM_HOME\view\webapps\usm\explorer\editprofile.xsl
- USM_HOME\view\webapps\usm\explorer\editregaccount.xsl
- USM_HOME\view\webapps\usm\explorer\images.xsl
- USM_HOME\view\webapps\usm\explorer\ruleactionedit.xsl
- USM_HOME\view\webapps\usm\explorer\billing\acctinfobillingadd.xsl
- USM_HOME\view\webapps\usm\explorer\billing\acctinfobillingedit.xsl
- USM_HOME\view\webapps\usm\explorer\billing\billrateitemimages.xsl
- USM_HOME\view\webapps\usm\explorer\billing\billrpbuilddefmodal.xsl

- USM_HOME\view\webapps\usm\explorer\billing\contentpacks.xsl
- USM_HOME\view\webapps\usm\explorer\request\catalogbrowse.xsl
- USM_HOME\view\webapps\usm\explorer\request\catalogitemdetails.xsl
- USM_HOME\view\webapps\usm\explorer\request\catalogrequestgetforms.xsl
- USM_HOME\view\webapps\usm\explorer\request\launchsdmclient.xsl
- USM_HOME\view\webapps\usm\explorer\request\requestemailprofile.xsl
- USM_HOME\view\webapps\usm\explorer\request\requestgetform.xsl
- USM_HOME\view\webapps\usm\explorer\request\requestprofile.xsl
- USM_HOME\view\webapps\usm\explorer\request\requestshared.xsl
- USM_HOME\view\webapps\usm\explorer\request\requesttracking.xsl
- USM_HOME\view\webapps\usm\explorer\request\request_cart.xsl
- USM_HOME\view\webapps\usm\explorer\request\request_create.xsl
- USM_HOME\view\webapps\usm\explorer\request\request_edit.xsl
- USM_HOME\view\webapps\usm\explorer\request\resetpassword.xsl
- USM_HOME\view\webapps\usm\explorer\request\common\request_attachments.xsl
- USM_HOME\view\webapps\usm\explorer\request\common\request_cartless_attachments.xsl
- USM_HOME\view\webapps\usm\explorer\request\common\request_notes.xsl
- USM_HOME\view\webapps\usm\explorer\request\functions\catalogitemdetailsfunctions.xsl
- USM_HOME\view\webapps\usm\explorer\scripts\billrpbuild-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\billrpbuild.js
- USM_HOME\view\webapps\usm\explorer\scripts\billrpbuilddefmodal-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\billrpbuilddefmodal.js
- USM_HOME\view\webapps\usm\explorer\scripts\billrpbuilddef_so-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\billrpbuilddef_so.js
- USM_HOME\view\webapps\usm\explorer\scripts\browse.widget.js
- USM_HOME\view\webapps\usm\explorer\scripts\common.core.fragments.chart.jar
- USM_HOME\view\webapps\usm\explorer\scripts\dashboard.cab

- USM_HOME\view\webapps\usm\explorer\scripts\formspreview-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\formspreview.js
- USM_HOME\view\webapps\usm\explorer\scripts\icansortfunctions-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\icansortfunctions.js
- USM_HOME\view\webapps\usm\explorer\scripts\jimi.jar
- USM_HOME\view\webapps\usm\explorer\scripts\openviz.jar
- USM_HOME\view\webapps\usm\explorer\scripts\print.cab
- USM_HOME\view\webapps\usm\explorer\scripts\request-list.widget.js
- USM_HOME\view\webapps\usm\explorer\scripts\richtext-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\richtext.js
- USM_HOME\view\webapps\usm\explorer\scripts\servicedetails-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\servicedetails.js
- USM_HOME\view\webapps\usm\explorer\scripts\serviceoption-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\serviceoption.js
- USM_HOME\view\webapps\usm\explorer\scripts\serviceoptionpreview-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\serviceoptionpreview.js
- USM_HOME\view\webapps\usm\explorer\scripts\toolsconfig-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\toolsconfig.js
- USM_HOME\view\webapps\usm\explorer\scripts\wait-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\wait.js
- USM_HOME\view\webapps\usm\explorer\scripts\widgets\browse.widget-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\widgets\browse.widget.js
- USM_HOME\view\webapps\usm\explorer\scripts\widgets\request-attachments-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\widgets\request-attachments.js
- USM_HOME\view\webapps\usm\explorer\scripts\widgets\request-common-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\widgets\request-common.js
- USM_HOME\view\webapps\usm\explorer\scripts\widgets\request-conversation-expanded.js

- USM_HOME\view\webapps\usm\explorer\scripts\widgets\request-conversation.js
- USM_HOME\view\webapps\usm\explorer\scripts\widgets\request-list.widget-expanded.js
- USM_HOME\view\webapps\usm\explorer\scripts\widgets\request-list.widget.js
- USM_HOME\view\webapps\usm\explorer\service\formspreview.xsl
- USM_HOME\view\webapps\usm\explorer\service\servicedefinition.xsl
- USM_HOME\view\webapps\usm\explorer\service\servicedesigner.xsl
- USM_HOME\view\webapps\usm\explorer\service\servicedetails.xsl
- USM_HOME\view\webapps\usm\explorer\service\serviceoptionpreview.xsl
- USM_HOME\view\webapps\usm\explorer\service\serviceoption_details_row.xsl
- USM_HOME\view\webapps\usm\explorer\service\sogpreview.xsl
- USM_HOME\view\webapps\usm\explorer\service\sogspreview.xsl
- USM_HOME\view\webapps\usm\explorer\templates\form.xsl
- USM_HOME\view\webapps\usm\explorer\templates\panel.xsl
- USM_HOME\view\webapps\usm\explorer\templates\sections.xsl
- USM_HOME\view\webapps\usm\locale\about_info.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\richtext_shared.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\ruleactionedit.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\ruleshared.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\toolsconfig.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\billing\billconfig.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\billing\billrpbuilddefmodal.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\formdesigner\gwt.ide.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\formdesigner\gwt.renderer.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\formdesigner\gwt.validator.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\help\reports\reportinghelp.htm
- USM_HOME\view\webapps\usm\locale\icbrpt\request\cataloggetchildren.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\request\countinfo.xml

- USM_HOME\view\webapps\usm\locale\icbrpt\request\requestinfo.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\request\requestshared.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\request\requesttracking.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\request\request_cart.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\request\request_create.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\request\request_edit.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\request\common\request_notes.xml
- USM_HOME\view\webapps\usm\locale\icbrpt\service\servicedetails.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\richtext_shared.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\ruleactionedit.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\ruleshared.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\toolsconfig.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\billing\acctinfobilling.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\billing\acctinfobillingadd.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\billing\acctinfobillingedit.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\billing\billconfig.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\billing\billrpbuilddefmodal.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\formdesigner\gwt.ide.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\formdesigner\gwt.renderer.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\formdesigner\gwt.validator.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\help\reports\reportinghelp.htm
- USM_HOME\view\webapps\usm\locale\iccnzh\request\cataloggetchildren.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\request\requestinfo.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\request\requestshared.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\request\requesttracking.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\request\request_cart.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\request\request_create.xml

- USM_HOME\view\webapps\usm\locale\iccnzh\request\request_edit.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\request\common\request_notes.xml
- USM_HOME\view\webapps\usm\locale\iccnzh\service\servicedetails.xml
- USM_HOME\view\webapps\usm\locale\icdede\acctinfotenantprofile.xml
- USM_HOME\view\webapps\usm\locale\icdede\acctinfotenantprofileedit.xml
- USM_HOME\view\webapps\usm\locale\icdede\addnewtenant.xml
- USM_HOME\view\webapps\usm\locale\icdede\agpopupsearchaccountincludes.xml
- USM_HOME\view\webapps\usm\locale\icdede\popupsearchaccount.xml
- USM_HOME\view\webapps\usm\locale\icdede\richtext_shared.xml
- USM_HOME\view\webapps\usm\locale\icdede\ruleactionedit.xml
- USM_HOME\view\webapps\usm\locale\icdede\ruleshared.xml
- USM_HOME\view\webapps\usm\locale\icdede\searchtenant.xml
- USM_HOME\view\webapps\usm\locale\icdede\searchtenantpopup.xml
- USM_HOME\view\webapps\usm\locale\icdede\showdomains.xml
- USM_HOME\view\webapps\usm\locale\icdede\termsandconditions.xml
- USM_HOME\view\webapps\usm\locale\icdede\toolsconfig.xml
- USM_HOME\view\webapps\usm\locale\icdede\billing\billconfig.xml
- USM_HOME\view\webapps\usm\locale\icdede\billing\billingpaymentsadd.xml
- USM_HOME\view\webapps\usm\locale\icdede\billing\billrpbuilddefmodal.xml
- USM_HOME\view\webapps\usm\locale\icdede\billing\invoicehistory.xml
- USM_HOME\view\webapps\usm\locale\icdede\cmdb\cibudetails.xml
- USM_HOME\view\webapps\usm\locale\icdede\formdesigner\gwt.ide.xml
- USM_HOME\view\webapps\usm\locale\icdede\formdesigner\gwt.renderer.xml
- USM_HOME\view\webapps\usm\locale\icdede\formdesigner\gwt.validator.xml
- USM_HOME\view\webapps\usm\locale\icdede\gwt\gwt.expression.xml
- USM_HOME\view\webapps\usm\locale\icdede\help\reports\reportinghelp.htm
- USM_HOME\view\webapps\usm\locale\icdede\request\cataloggetchildren.xml

- USM_HOME\view\webapps\usm\locale\icdede\request\catalogrequestsearch.xml
- USM_HOME\view\webapps\usm\locale\icdede\request\gwt.requestlist.xml
- USM_HOME\view\webapps\usm\locale\icdede\request\requestinfo.xml
- USM_HOME\view\webapps\usm\locale\icdede\request\requestshared.xml
- USM_HOME\view\webapps\usm\locale\icdede\request\requesttracking.xml
- USM_HOME\view\webapps\usm\locale\icdede\request\request_cart.xml
- USM_HOME\view\webapps\usm\locale\icdede\request\request_create.xml
- USM_HOME\view\webapps\usm\locale\icdede\request\request_edit.xml
- USM_HOME\view\webapps\usm\locale\icdede\request\common\request_notes.xml
- USM_HOME\view\webapps\usm\locale\icdede\service\servicedetails.xml
- USM_HOME\view\webapps\usm\locale\icdkda\richtext_shared.xml
- USM_HOME\view\webapps\usm\locale\icdkda\ruleactionedit.xml
- USM_HOME\view\webapps\usm\locale\icdkda\ruleshared.xml
- USM_HOME\view\webapps\usm\locale\icdkda\toolsconfig.xml
- USM_HOME\view\webapps\usm\locale\icdkda\billing\billconfig.xml
- USM_HOME\view\webapps\usm\locale\icdkda\billing\billrpbuilddefmodal.xml
- USM_HOME\view\webapps\usm\locale\icdkda\configurator\configurator.xml
- USM_HOME\view\webapps\usm\locale\icdkda\configurator\setup-warnning.html
- USM_HOME\view\webapps\usm\locale\icdkda\formdesigner\gwt.ide.xml
- USM_HOME\view\webapps\usm\locale\icdkda\formdesigner\gwt.renderer.xml
- USM_HOME\view\webapps\usm\locale\icdkda\formdesigner\gwt.validator.xml
- USM_HOME\view\webapps\usm\locale\icdkda\help\reports\reportinghelp.htm
- USM_HOME\view\webapps\usm\locale\icdkda\request\cataloggetchildren.xml
- USM_HOME\view\webapps\usm\locale\icdkda\request\requestinfo.xml
- USM_HOME\view\webapps\usm\locale\icdkda\request\requestshared.xml
- USM_HOME\view\webapps\usm\locale\icdkda\request\requesttracking.xml
- USM_HOME\view\webapps\usm\locale\icdkda\request\request_cart.xml

- USM_HOME\view\webapps\usm\locale\icdkda\request\request_create.xml
- USM_HOME\view\webapps\usm\locale\icdkda\request\request_edit.xml
- USM_HOME\view\webapps\usm\locale\icdkda\request\common\request_notes.xml
- USM_HOME\view\webapps\usm\locale\icdkda\service\servicedetails.xml
- USM_HOME\view\webapps\usm\locale\iceses\acctinfotenantprofileedit.xml
- USM_HOME\view\webapps\usm\locale\iceses\addnewtenant.xml
- USM_HOME\view\webapps\usm\locale\iceses\addregaccount.xml
- USM_HOME\view\webapps\usm\locale\iceses\adduser.xml
- USM_HOME\view\webapps\usm\locale\iceses\editprofile.xml
- USM_HOME\view\webapps\usm\locale\iceses\editregaccount.xml
- USM_HOME\view\webapps\usm\locale\iceses\editusersettings.xml
- USM_HOME\view\webapps\usm\locale\iceses\fulfillmentconfig.xml
- USM_HOME\view\webapps\usm\locale\iceses\includes_shared.xml
- USM_HOME\view\webapps\usm\locale\iceses\nodeframe.xml
- USM_HOME\view\webapps\usm\locale\iceses\popupsearchaccount.xml
- USM_HOME\view\webapps\usm\locale\iceses\popupsearchuser.xml
- USM_HOME\view\webapps\usm\locale\iceses\portalitempart.xml
- USM_HOME\view\webapps\usm\locale\iceses\printjobdetails.xml
- USM_HOME\view\webapps\usm\locale\iceses\richtext_shared.xml
- USM_HOME\view\webapps\usm\locale\iceses\ruleactionedit.xml
- USM_HOME\view\webapps\usm\locale\iceses\ruleedit.xml
- USM_HOME\view\webapps\usm\locale\iceses\ruleshared.xml
- USM_HOME\view\webapps\usm\locale\iceses\ruletypeedit.xml
- USM_HOME\view\webapps\usm\locale\iceses\searchaccount.xml
- USM_HOME\view\webapps\usm\locale\iceses\searchaccountpopup.xml
- USM_HOME\view\webapps\usm\locale\iceses\searchenduser.xml
- USM_HOME\view\webapps\usm\locale\iceses\searchlocationpopup.xml

- USM_HOME\view\webapps\usm\locale\iceses\searchtenant.xml
- USM_HOME\view\webapps\usm\locale\iceses\searchtenantpopup.xml
- USM_HOME\view\webapps\usm\locale\iceses\showdomains.xml
- USM_HOME\view\webapps\usm\locale\iceses\toolsconfig.xml
- USM_HOME\view\webapps\usm\locale\iceses\userdetails.xml
- USM_HOME\view\webapps\usm\locale\iceses\usermgmt.xml
- USM_HOME\view\webapps\usm\locale\iceses\userprofile.xml
- USM_HOME\view\webapps\usm\locale\iceses\billing\assignedmodels.xml
- USM_HOME\view\webapps\usm\locale\iceses\billing\billconfig.xml
- USM_HOME\view\webapps\usm\locale\iceses\billing\billexportrun.xml
- USM_HOME\view\webapps\usm\locale\iceses\billing\billexporttypes.xml
- USM_HOME\view\webapps\usm\locale\iceses\billing\billingpaymentsadd.xml
- USM_HOME\view\webapps\usm\locale\iceses\billing\billplansearch.xml
- USM_HOME\view\webapps\usm\locale\iceses\billing\billrpbuilddefmodal.xml
- USM_HOME\view\webapps\usm\locale\iceses\billing\category.xml
- USM_HOME\view\webapps\usm\locale\iceses\cmdb\ciofferingclick.xml
- USM_HOME\view\webapps\usm\locale\iceses\cmdb\cisubscriptiondetails.xml
- USM_HOME\view\webapps\usm\locale\iceses\cmdb\cmdbcilist.xml
- USM_HOME\view\webapps\usm\locale\iceses\dataprocessor\dpdbadvdefine.xml
- USM_HOME\view\webapps\usm\locale\iceses\dataprocessor\dpdbdefine.xml
- USM_HOME\view\webapps\usm\locale\iceses\dataprocessor\dpfieldadd.xml
- USM_HOME\view\webapps\usm\locale\iceses\dataprocessor\dpicdbadd.xml
- USM_HOME\view\webapps\usm\locale\iceses\dataprocessor\dpprofileadd.xml
- USM_HOME\view\webapps\usm\locale\iceses\dataprocessor\dpshowdomains.xml
- USM_HOME\view\webapps\usm\locale\iceses\formdesigner\gwt.ide.xml
- USM_HOME\view\webapps\usm\locale\iceses\formdesigner\gwt.renderer.xml
- USM_HOME\view\webapps\usm\locale\iceses\formdesigner\gwt.validator.xml

- USM_HOME\view\webapps\usm\locale\iceses\help\portal\portalhelp.htm
- USM_HOME\view\webapps\usm\locale\iceses\help\reports\reportinghelp.htm
- USM_HOME\view\webapps\usm\locale\iceses\metering\app_shared.xml
- USM_HOME\view\webapps\usm\locale\iceses\planning\billbudgetlayout.xml
- USM_HOME\view\webapps\usm\locale\iceses\policy\policybuilder.xml
- USM_HOME\view\webapps\usm\locale\iceses\provision\provisioncfgfront.xml
- USM_HOME\view\webapps\usm\locale\iceses\provision\provisioncfgnetdev.xml
- USM_HOME\view\webapps\usm\locale\iceses\provision\provisionexchange.xml
- USM_HOME\view\webapps\usm\locale\iceses\provision\provisionhttprequest.xml
- USM_HOME\view\webapps\usm\locale\iceses\provision\provisionlotusnotes.xml
- USM_HOME\view\webapps\usm\locale\iceses\provision\provisionnetflow.xml
- USM_HOME\view\webapps\usm\locale\iceses\provision\provisionsbandwidth.xml
- USM_HOME\view\webapps\usm\locale\iceses\provision\provisionservcfglist.xml
- USM_HOME\view\webapps\usm\locale\iceses\provision\provisionsflow.xml
- USM_HOME\view\webapps\usm\locale\iceses\reports\reportsgenericdataedit.xml
- USM_HOME\view\webapps\usm\locale\iceses\reports\reportsgenericdatagetpivotfields.xml
- USM_HOME\view\webapps\usm\locale\iceses\reports\reportsgenericdataviewedit.xml
- USM_HOME\view\webapps\usm\locale\iceses\reports\reportslist.xml
- USM_HOME\view\webapps\usm\locale\iceses\reports\reportviewforselect.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\catalogcheckout.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\cataloggetchildren.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\catalogitemdetails.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\catalogitemrequests.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\catalogpastitems.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\catalogpendingaction.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\catalogpendingitems.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\catalogpopularitems.xml

- USM_HOME\view\webapps\usm\locale\iceses\request\catalogrequesteditems.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\catalogrequestsearch.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\catalogsearch.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\requestaddedit.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\requestinfo.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\requestmessagealerts.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\requestprofile.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\requestpushthrough.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\requestsaudit.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\requestsemail.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\requestshared.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\requesttracking.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\request_cart.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\request_create.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\request_edit.xml
- USM_HOME\view\webapps\usm\locale\iceses\request\common\request_notes.xml
- USM_HOME\view\webapps\usm\locale\iceses\scheduler\schedulertaskedit.xml
- USM_HOME\view\webapps\usm\locale\iceses\service\selectedsogdetails.xml
- USM_HOME\view\webapps\usm\locale\iceses\service\servicedetails.xml
- USM_HOME\view\webapps\usm\locale\icfifi\richtext_shared.xml
- USM_HOME\view\webapps\usm\locale\icfifi\ruleactionedit.xml
- USM_HOME\view\webapps\usm\locale\icfifi\ruleshared.xml
- USM_HOME\view\webapps\usm\locale\icfifi\toolsconfig.xml
- USM_HOME\view\webapps\usm\locale\icfifi\billing\billconfig.xml
- USM_HOME\view\webapps\usm\locale\icfifi\billing\billrpbuilddefmodal.xml
- USM_HOME\view\webapps\usm\locale\icfifi\formdesigner\gwt.ide.xml
- USM_HOME\view\webapps\usm\locale\icfifi\formdesigner\gwt.renderer.xml

- USM_HOME\view\webapps\usm\locale\icfifi\formdesigner\gwt.validator.xml
- USM_HOME\view\webapps\usm\locale\icfifi\help\reports\reportinghelp.htm
- USM_HOME\view\webapps\usm\locale\icfifi\request\cataloggetchildren.xml
- USM_HOME\view\webapps\usm\locale\icfifi\request\requestinfo.xml
- USM_HOME\view\webapps\usm\locale\icfifi\request\requestshared.xml
- USM_HOME\view\webapps\usm\locale\icfifi\request\requesttracking.xml
- USM_HOME\view\webapps\usm\locale\icfifi\request\request_cart.xml
- USM_HOME\view\webapps\usm\locale\icfifi\request\request_create.xml
- USM_HOME\view\webapps\usm\locale\icfifi\request\request_edit.xml
- USM_HOME\view\webapps\usm\locale\icfifi\request\common\request_notes.xml
- USM_HOME\view\webapps\usm\locale\icfifi\service\servicedetails.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\agpopupsearchaccountincludes.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\docman.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\docmanadddocmodal.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\fulfillmentconfig.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\includes_shared.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\logon.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\nodeleft.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\popupsearchaccountincludes.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\portaladdtemplatemodal.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\portalmanagement.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\richtext_shared.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\ruleactionedit.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\ruleshared.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\searchincludes.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\searchtenant.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\toolsconfig.xml

- USM_HOME\view\webapps\usm\locale\icfrfr\billing\billconfig.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\billing\billingaccountsubscriptiontreepresubscribe.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\billing\billplan.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\billing\billrateitemtext.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\billing\billrpbuilddefmodal.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\billing\contentpacksimport.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\cmdb\cisubscriptiondetails.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\dataprocessor\dpprofileadd.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\dataprocessor\dpsystem.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\formdesigner\gwt.ide.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\formdesigner\gwt.renderer.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\formdesigner\gwt.validator.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\help\portal\portalhelp.htm
- USM_HOME\view\webapps\usm\locale\icfrfr\help\reports\reportinghelp.htm
- USM_HOME\view\webapps\usm\locale\icfrfr\ix\exportimport.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\planning\billbudgetlayout.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\provision\provisionhttprequest.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\provision\provisionnetflow.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\provision\provisionsbandwidth.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\provision\provisionsflow.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\reports\reportsadd.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\reports\reportsedit.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\reports\reportsgenericfolderlistmodal.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\reports\reportsgenericofflinecreate.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\reports\reportsgenericprintoptions.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\reports\reportsprofile.xml

- USM_HOME\view\webapps\usm\locale\icfrfr\request\catalogcheckout.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\cataloggetchildren.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\catalogitemrequests.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\catalogpastitems.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\catalogpendingaction.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\catalogpendingitems.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\catalogpopularitems.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\catalogrequesteditems.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\catalogrequestsearch.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\gwt.requestlist.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\requestaddedit.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\requestinfo.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\requestlistpendingactiondescription.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\requestmessagealerts.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\requestpendingactiondescription.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\requestprofile.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\requestpushthrough.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\requestsaudit.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\requestsemail.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\requestshared.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\requesttracking.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\request_cart.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\request_create.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\request_edit.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\request\common\request_notes.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\service\servicedesigner.xml
- USM_HOME\view\webapps\usm\locale\icfrfr\service\servicedetails.xml

- USM_HOME\view\webapps\usm\locale\icfrfr\service\serviceselection.xml
- USM_HOME\view\webapps\usm\locale\icitit\aboutproduct.xml
- USM_HOME\view\webapps\usm\locale\icitit\adduser.xml
- USM_HOME\view\webapps\usm\locale\icitit\agpopupsearchaccount.xml
- USM_HOME\view\webapps\usm\locale\icitit\editprofile.xml
- USM_HOME\view\webapps\usm\locale\icitit\editusersettings.xml
- USM_HOME\view\webapps\usm\locale\icitit\error.xml
- USM_HOME\view\webapps\usm\locale\icitit\includes_shared.xml
- USM_HOME\view\webapps\usm\locale\icitit\messagealerts.xml
- USM_HOME\view\webapps\usm\locale\icitit\messagechangeevents.xml
- USM_HOME\view\webapps\usm\locale\icitit\messagechangeeventsdetails.xml
- USM_HOME\view\webapps\usm\locale\icitit\messagenews.xml
- USM_HOME\view\webapps\usm\locale\icitit\passwordpolicyaddedit.xml
- USM_HOME\view\webapps\usm\locale\icitit\passwordpolicylist.xml
- USM_HOME\view\webapps\usm\locale\icitit\popupsearchaccount.xml
- USM_HOME\view\webapps\usm\locale\icitit\portalauthenticate.xml
- USM_HOME\view\webapps\usm\locale\icitit\printjobdetails.xml
- USM_HOME\view\webapps\usm\locale\icitit\printmanagement.xml
- USM_HOME\view\webapps\usm\locale\icitit\richtext_shared.xml
- USM_HOME\view\webapps\usm\locale\icitit\ruleactionedit.xml
- USM_HOME\view\webapps\usm\locale\icitit\ruleshared.xml
- USM_HOME\view\webapps\usm\locale\icitit\runtimeapp.xml
- USM_HOME\view\webapps\usm\locale\icitit\runtimeappadd.xml
- USM_HOME\view\webapps\usm\locale\icitit\runtimeappall.xml
- USM_HOME\view\webapps\usm\locale\icitit\runtimeappedit.xml
- USM_HOME\view\webapps\usm\locale\icitit\searchaccountresults.xml
- USM_HOME\view\webapps\usm\locale\icitit\searchlocationpopup.xml

- USM_HOME\view\webapps\usm\locale\icitit\toolsconfig.xml
- USM_HOME\view\webapps\usm\locale\icitit\userdetails.xml
- USM_HOME\view\webapps\usm\locale\icitit\usermgmt.xml
- USM_HOME\view\webapps\usm\locale\icitit\userprofile.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\acctinfobilling.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\acctinfobillingadd.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\acctinfobillingedit.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\acctinfobillingpaymentadd.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\acctinfobillingpaymentedit.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billconfig.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billconfigeditmodal.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billgroupadd.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billgroupedit.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billgroupshowall.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billingaddadjustment.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billingaddadjustmentsla.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billingadjustmentdetails.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billingadjustments.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billingadjustmentsearch.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billingadjustmentslasearch.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billingeditadjustmentdetails.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billingeditadjustmentdetailssla.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billrpbuilddefdepend.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billrpbuilddefmodal.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billrpbuilddefmodaleffective.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billsettledefadd.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billsettledefdetails.xml

- USM_HOME\view\webapps\usm\locale\icitit\billing\billsettledefedit.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\billsettledefsearch.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\category.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\contentpacks.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\expandinvoicerun.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\expandinvoicerunprint.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\searchpayment.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\searchstatement.xml
- USM_HOME\view\webapps\usm\locale\icitit\billing\substates.xml
- USM_HOME\view\webapps\usm\locale\icitit\cmdb\ciofferingdetails.xml
- USM_HOME\view\webapps\usm\locale\icitit\cmdb\cirequestdetails.xml
- USM_HOME\view\webapps\usm\locale\icitit\cmdb\cisubscriptiondetails.xml
- USM_HOME\view\webapps\usm\locale\icitit\cmdb\cmdbcilist.xml
- USM_HOME\view\webapps\usm\locale\icitit\cmdb\offeringcatalog.xml
- USM_HOME\view\webapps\usm\locale\icitit\cmdb\offeringcatalogsearch.xml
- USM_HOME\view\webapps\usm\locale\icitit\dataprocessor\dpdbviewhistory.xml
- USM_HOME\view\webapps\usm\locale\icitit\dataprocessor\dpfileupload.xml
- USM_HOME\view\webapps\usm\locale\icitit\dataprocessor\dpfileuploadcomplete.xml
- USM_HOME\view\webapps\usm\locale\icitit\dataprocessor\dpprofilelist.xml
- USM_HOME\view\webapps\usm\locale\icitit\dataprocessor\dpsystem.xml
- USM_HOME\view\webapps\usm\locale\icitit\formdesigner\gwt.ide.xml
- USM_HOME\view\webapps\usm\locale\icitit\formdesigner\gwt.renderer.xml
- USM_HOME\view\webapps\usm\locale\icitit\formdesigner\gwt.validator.xml
- USM_HOME\view\webapps\usm\locale\icitit\help\catalog_contents\Desktop-Deluxe.html
- USM_HOME\view\webapps\usm\locale\icitit\help\catalog_contents\Desktop-Standard.html
- USM_HOME\view\webapps\usm\locale\icitit\help\catalog_contents\Laptop-Deluxe.html
- USM_HOME\view\webapps\usm\locale\icitit\help\catalog_contents\Laptop-Standard.html

- USM_HOME\view\webapps\usm\locale\icitit\help\reports\reportinghelp.htm
- USM_HOME\view\webapps\usm\locale\icitit\ix\ixobjectattributemapping.xml
- USM_HOME\view\webapps\usm\locale\icitit\metering\defineappmetric.xml
- USM_HOME\view\webapps\usm\locale\icitit\planning\billbudgetlayout.xml
- USM_HOME\view\webapps\usm\locale\icitit\policy\policybuilder.xml
- USM_HOME\view\webapps\usm\locale\icitit\provision\provisionhttprequest.xml
- USM_HOME\view\webapps\usm\locale\icitit\reports\reports.xml
- USM_HOME\view\webapps\usm\locale\icitit\reports\reportscustomlayoutlist.xml
- USM_HOME\view\webapps\usm\locale\icitit\reports\reportsgenericdataviewedit.xml
- USM_HOME\view\webapps\usm\locale\icitit\reports\reportsgenericofflinecreate.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\catalogbrowse.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\catalogcheckout.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\cataloggetchildren.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\catalogitemdetails.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\catalogitemrequests.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\catalogpastitems.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\catalogpendingaction.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\catalogpendingitems.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\catalogrequesteditems.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\catalogrequestgetforms.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\catalogrequestprofile.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\catalogrequestsearch.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\checkout.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\gwt.requestlist.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\recentrequestlist.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestaddcatalog.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestaddedit.xml

- USM_HOME\view\webapps\usm\locale\icitit\request\requestapproveconfirmmessage.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestcatalogsearch.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestdocuments.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestemailprofile.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestinfo.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestinfoshared.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestlistpendingactiondescription.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestmessagealerts.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestpdashared.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestprofile.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestpushthrough.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestsaudit.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestsearch.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestsemail.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestshared.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requestslistapproval.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requesttracking.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requesttrackinghistory.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\requesttrackingpolicyaction.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\request_cart.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\request_create.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\request_edit.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\webstoreitemdetails.xml
- USM_HOME\view\webapps\usm\locale\icitit\request\common\request_notes.xml
- USM_HOME\view\webapps\usm\locale\icitit\service\gwt.ide.xml
- USM_HOME\view\webapps\usm\locale\icitit\service\servicedetails.xml
- USM_HOME\view\webapps\usm\locale\icitit\service\serviceoption_details_row.xml

- USM_HOME\view\webapps\usm\locale\icitit\service\serviceoption_policyprocess.xml
- USM_HOME\view\webapps\usm\locale\icitit\service\serviceselection.xml
- USM_HOME\view\webapps\usm\locale\icitit\service\sogdetails.xml
- USM_HOME\view\webapps\usm\locale\icitit\slacalendar\cat_calendar_shared.xml
- USM_HOME\view\webapps\usm\locale\icitit\workflow\wfcreateprocess.xml
- USM_HOME\view\webapps\usm\locale\icitit\workflow\wfdetails.xml
- USM_HOME\view\webapps\usm\locale\icitit\workflow\wfmonitorprocess.xml
- USM_HOME\view\webapps\usm\locale\icitit\workflow\wftasksbyprocessid.xml
- USM_HOME\view\webapps\usm\locale\icjpja\richtext_shared.xml
- USM_HOME\view\webapps\usm\locale\icjpja\ruleactionedit.xml
- USM_HOME\view\webapps\usm\locale\icjpja\ruleshared.xml
- USM_HOME\view\webapps\usm\locale\icjpja\toolsconfig.xml
- USM_HOME\view\webapps\usm\locale\icjpja\billing\billconfig.xml
- USM_HOME\view\webapps\usm\locale\icjpja\billing\billplanmodal.xml
- USM_HOME\view\webapps\usm\locale\icjpja\billing\billrpbuilddefmodal.xml
- USM_HOME\view\webapps\usm\locale\icjpja\cmdb\ciofferingclick.xml
- USM_HOME\view\webapps\usm\locale\icjpja\dataprocessor\dpfieldadd.xml
- USM_HOME\view\webapps\usm\locale\icjpja\formdesigner\gwt.ide.xml
- USM_HOME\view\webapps\usm\locale\icjpja\formdesigner\gwt.validator.xml
- USM_HOME\view\webapps\usm\locale\icjpja\help\reports\reportinghelp.htm
- USM_HOME\view\webapps\usm\locale\icjpja\provision\provisioncfgfront.xml
- USM_HOME\view\webapps\usm\locale\icjpja\provision\provisioneventmgmt.xml
- USM_HOME\view\webapps\usm\locale\icjpja\provision\provisionhttprequest.xml
- USM_HOME\view\webapps\usm\locale\icjpja\provision\provisionlotusnotes.xml
- USM_HOME\view\webapps\usm\locale\icjpja\provision\provisionnetflow.xml
- USM_HOME\view\webapps\usm\locale\icjpja\provision\provisionsbandwidth.xml
- USM_HOME\view\webapps\usm\locale\icjpja\provision\provisionsflow.xml

- USM_HOME\view\webapps\usm\locale\icjpja\request\cataloggetchildren.xml
- USM_HOME\view\webapps\usm\locale\icjpja\request\catalogitemdetails.xml
- USM_HOME\view\webapps\usm\locale\icjpja\request\catalogrequestgetforms.xml
- USM_HOME\view\webapps\usm\locale\icjpja\request\requestinfo.xml
- USM_HOME\view\webapps\usm\locale\icjpja\request\requestprofile.xml
- USM_HOME\view\webapps\usm\locale\icjpja\request\requestshared.xml
- USM_HOME\view\webapps\usm\locale\icjpja\request\requesttracking.xml
- USM_HOME\view\webapps\usm\locale\icjpja\request\request_cart.xml
- USM_HOME\view\webapps\usm\locale\icjpja\request\request_create.xml
- USM_HOME\view\webapps\usm\locale\icjpja\request\request_edit.xml
- USM_HOME\view\webapps\usm\locale\icjpja\request\common\request_notes.xml
- USM_HOME\view\webapps\usm\locale\icjpja\service\servicedetails.xml
- USM_HOME\view\webapps\usm\locale\icjpja\service\sogdetails.xml
- USM_HOME\view\webapps\usm\locale\icjpja\workflow\wforgpost.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\richtext_shared.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\ruleactionedit.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\ruleshared.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\toolsconfig.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\billing\billconfig.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\billing\billrpbuilddefmodal.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\formdesigner\gwt.ide.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\formdesigner\gwt.renderer.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\formdesigner\gwt.validator.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\help\reports\reportinghelp.htm
- USM_HOME\view\webapps\usm\locale\icnlnl\request\cataloggetchildren.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\request\requestinfo.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\request\requestshared.xml

- USM_HOME\view\webapps\usm\locale\icnlnl\request\requesttracking.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\request\request_cart.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\request\request_create.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\request\request_edit.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\request\common\request_notes.xml
- USM_HOME\view\webapps\usm\locale\icnlnl\service\servicedetails.xml
- USM_HOME\view\webapps\usm\locale\icsesv\adduser.xml
- USM_HOME\view\webapps\usm\locale\icsesv\editprofile.xml
- USM_HOME\view\webapps\usm\locale\icsesv\editusersettings.xml
- USM_HOME\view\webapps\usm\locale\icsesv\richtext_shared.xml
- USM_HOME\view\webapps\usm\locale\icsesv\ruleactionedit.xml
- USM_HOME\view\webapps\usm\locale\icsesv\ruleshared.xml
- USM_HOME\view\webapps\usm\locale\icsesv\toolsconfig.xml
- USM_HOME\view\webapps\usm\locale\icsesv\userdetails.xml
- USM_HOME\view\webapps\usm\locale\icsesv\userprofile.xml
- USM_HOME\view\webapps\usm\locale\icsesv\billing\acctinfosubscriptionlistshared.xml
- USM_HOME\view\webapps\usm\locale\icsesv\billing\billconfig.xml
- USM_HOME\view\webapps\usm\locale\icsesv\billing\billrateitemtext.xml
- USM_HOME\view\webapps\usm\locale\icsesv\billing\billrpbuilddefmodal.xml
- USM_HOME\view\webapps\usm\locale\icsesv\formdesigner\gwt.ide.xml
- USM_HOME\view\webapps\usm\locale\icsesv\formdesigner\gwt.renderer.xml
- USM_HOME\view\webapps\usm\locale\icsesv\formdesigner\gwt.validator.xml
- USM_HOME\view\webapps\usm\locale\icsesv\help\reports\reportinghelp.htm
- USM_HOME\view\webapps\usm\locale\icsesv\request\cataloggetchildren.xml
- USM_HOME\view\webapps\usm\locale\icsesv\request\requestinfo.xml
- USM_HOME\view\webapps\usm\locale\icsesv\request\requestshared.xml
- USM_HOME\view\webapps\usm\locale\icsesv\request\requesttracking.xml

- USM_HOME\view\webapps\usm\locale\icsesv\request\request_cart.xml
- USM_HOME\view\webapps\usm\locale\icsesv\request\request_create.xml
- USM_HOME\view\webapps\usm\locale\icsesv\request\request_edit.xml
- USM_HOME\view\webapps\usm\locale\icsesv\request\common\request_notes.xml
- USM_HOME\view\webapps\usm\locale\icsesv\service\servicedetails.xml
- USM_HOME\view\webapps\usm\locale\icusen\ruleactionedit.xml
- USM_HOME\view\webapps\usm\locale\icusen\ruleshared.xml
- USM_HOME\view\webapps\usm\locale\icusen\toolsconfig.xml
- USM_HOME\view\webapps\usm\locale\icusen\billing\billconfig.xml
- USM_HOME\view\webapps\usm\locale\icusen\billing\billrpbuilddefmodal.xml
- USM_HOME\view\webapps\usm\locale\icusen\formdesigner\gwt.ide.xml
- USM_HOME\view\webapps\usm\locale\icusen\formdesigner\gwt.validator.xml
- USM_HOME\view\webapps\usm\locale\icusen\request\requestshared.xml
- USM_HOME\view\webapps\usm\locale\icusen\request\requesttracking.xml
- USM_HOME\view\webapps\usm\locale\icusen\service\servicedetails.xml
- USM_HOME\view\webapps\usm\WEB-INF\lib\common.base.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\common.core.fragments.xalan.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\common.core.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\common.crypto.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\common.ui.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\eclipselink.base.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\formsdesigner.base.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\formsdesigner.ide.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\formsdesigner.renderer.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\gxt-gwt22.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\gxt.base.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\gxt.common.jar

- USM_HOME\view\webapps\usm\WEB-INF\lib\infrastructure.installanywhere.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\modules.Common.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\plugins.apis.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\plugins.manager.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\policy.base.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\policy.designer.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\portlets.browse.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\portlets.common.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\portlets.request-edit.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\portlets.request-list.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\portlets.request.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\portlets.status.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\servicebuilder.ide.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\share.fomsdesigner.base.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\spring.gwt.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\spring.jpa.jar
- USM_HOME\view\webapps\usm\WEB-INF\lib\utility.configurator.jar

Implementing CA Service Management 14.1.02

CA Service Management 14.1.02 is a cumulative patch for CA Service Management 14.1 and 14.1.01, which provides new features, enhancements, and bug fixes.

The following patches are available for Windows and Non-Windows environment to download from CA Support (https://support.ca.com/irj/portal/newhome):

- RO86281 (Windows)
- RO86285 (Linux)
- RO86282 (Solaris)
- RO86295 (AIX)

Note: To install CA Service Management 14.1.02, it is mandatory to have CA Service Management 14.1 or 14.1.01 installed in the system.

Prerequisites for CA Service Management 14.1.02 Installation

Verify and complete the following prerequisites before proceeding with CA Service Management 14.1.02 installation :

- To install and use cumulative patch, ensure that CA Service Management 14.1 or 14.1.01 is installed in your environment. For more information, visit CA Technical Support (http://ca.com/support).
- Back up your system database (MDB) before installing the cumulative patch. This is mandatory and ensures safe data recovery if any problems are encountered during the installation process.
- Before installing the patch, ensure that you have read the CA Service Management 14.1.02 Release notes for *What's New in this Release*, fixes, and known issues. For more information, see CA Service Management Release 14.1.02 Enhancements . (see page 69)

Prerequisites for CA Service Desk Manager and Unified Self-Service Installation

Do not invoke ApplyPTF manually in your system while running the CA Service Management 14.1.02 patch installer. If ApplyPTF is invoked, an alert message may appear that you can run only one ApplyPTF at a time, and the task of applying CA SDM or USS patch gets completed without applying the patch.

Prerequisites for CA Asset Portfolio Management Installation

Complete the following prerequisites before proceeding with CA APM 14.1.02 installation:

- Install .NET 4.5.2 framework on Windows Server 2008 (see page)
- Add ASP.NET in IIS on Windows Server 2012 (see page 686)

Install .NET 4.5.2 framework on Windows Server 2008:

To install .NET 4.5.2 framework on Windows Server 2008, complete the following steps:

1. Navigate to .NET 4.5.2 framework *Root folder/filestore/*Prerequisite.
2. Execute **NDP452-KB2901907-x86-x64-AllOS-ENU.exe.**
3. Follow on-screen instructions. Click **Next**.

4. Review the summary screen.

5. Click **Finish** to exit the installer.
   .NET 4.5.2 framework is now installed.

Add ASP.NET in IIS on Windows Server 2012

To add ASP.NET in IIS on Windows Server 2012, perform the following steps:

1. Open Server Manager.

2. Navigate to **Manage**, **Add Roles and Features**.

3. Follow on-screen instructions. Select installation type and destination server.

4. Select **Roles** from the select server roles pane, expand **Web Server (IIS)**, **Application Development (IIS)**.

5. Select **ASP.NET 3.5** and **ASP.NET 4.5**.

6. Click **Next**.

7. Follow on-screen instructions and complete the installation.
   ASP.Net is now added in IIS.

For more information on supported operating system, databases, web browsers, and so on, see Supportability Matrix. (see page 119)

Additionally, if you want to identify and list the CA Service Management product patches installed in your system, you can run SMPatchReport utility. For more information, see Run SMPatchReport Utility to Get Installed Patches List. (see page 742)

Install CA Service Management 14.1.02

To install CA Service Management 14.1.02. perform the following based on the operating system installed in your system (Windows/Non-Windows):

- Install CA Service Management 14.1.02 (Windows) (see page 688)
- Install CA Service Management 14.1.02 (Non-Windows) (see page 692)

Install CA Service Management 14.1.02 (Windows)

This article describes how to install the CA Service Management 14.1.02 patch for Windows. Ensure that you have completed installation prerequisites (see page 686)before proceeding with patch installation.

Important: If you have applied test fixes on CA Service Management 14.1.02, you must not reapply the CA Service Management 14.1.02 patch as it may override the test fix changes.

Note: If you are installing the patch on CA SDM 14.1 or 14.1.01, consider the following based on your server configuration:

- Advanced Availability: log on to the standby server, which you plan to promote as the new background server and install the patch.
- Conventional: log on to the primary server.

Note: In a CA APM distributed environment, the CA Service Management 14.1.02 patch must be applied on all servers. However, the database screen is shown only on the component server and you must install the MDB patch from the component server.

Perform the following steps:

1. Download **RO86281. CAZ** from CA Support (http://www.ca.com/in/support.aspx).
2. Extract the file using following command:

   ```
   cazipxp.exe -u <Patch cazip file>
   ```

   Note: If you do not have the cazipxp.exe utility, download it from CA Support (http://www.ca.com/in/support.aspx).

3. Extract **CASM_14.1.02_CommonPatchInstaller_Win.zip**.
4. Perform the following steps if CA Service Catalog is installed in your environment:
   a. Download **RO86617.CAZ** from CA Support (http://www.ca.com/in/support.aspx).
   b. Copy and paste the **RO86617.CAZ** in the *CASM_14.1.02 _CommonPatchInstaller_Win\Patches\SLCM\Binaries* folder.
5. Navigate to *CASM_14.1.02_CommonPatchInstaller_Win* folder *and* double-click **Setup.exe**.
6. Review and accept the license agreement terms.
7. In Database Configuration, select Microsoft SQL Server or Oracle as the database type. Ensure that you have installed Microsoft SQL Server or Oracle database client in the system.

Note: In case of CA SDM, the installer detects and identifies if there is a primary or standby server (Conventional or Advanced Availability) and displays the MDB database screen.

Provide the database configuration details as per the selected database (Oracle or Microsoft SQL Server):

a. **Microsoft SQL Server**: Complete the following if you have installed Microsoft SQL Server database:

- **Database Server**: The host name of the database server. If the target instance is part of a clustered instance, the virtual host name of the cluster must be used.
- **Database Name**: Specifies the Database name (mdb), the name of the target DBMS. The default value is mdb.
- **Database Port**: Specifies the port identifier for the target DBMS.
- **Database Server Instance**: The database instance name. Leave this field blank if you are using the default instance.
- **Database Admin User**: For SQL Server, **sa** is the default value. Provides permission to create users and schema.
- **Database Admin Password**: Specifies the database password of users specified by the database admin user.
- **mdbadmin Password**: Specify the password for the mdbadmin user.
- **Confirm mdbadmin Password**: Confirm the mdbadmin user password.

b. **Oracle**: Complete the following if you have installed Oracle database:

- **Database Server**: Specifies the host name of Oracle database server.
  If the target instance is part of a clustered instance, the virtual host name of the cluster must be used.
- **Oracle Service Name**: Specifies the Oracle Service name.
- **Listener Port**: Specifies the listener port for database.
- **Net Service Name**: Identifies the Net Service Name of Oracle database where the database resides.
  If database is remote, use the Net Service Name that is defined in Oracle client on the local computer. CA SDM accesses the database through a local installation of the Oracle client.
- **DBA User Name**: Authenticates the name of the user with DBA access. The default value for DBA user is **SYS.**
- **DBA User Password**: Authenticates the password for DBA user.

- **mdbadmin Password**: Specify password for mdbadmin user.
- **Confirm mdbadmin Password**: Confirm mdbadmin user password.
- **Tablespace Path (on DB Server)**: Specifies the tablespace directory on the database server.
- **Oracle Home Path**: Specifies the Oracle client 32-bit path.
- **Data Tablespace Name**: Specifies tablespace name. The default value is **MDB_DATA**.
- **Index Tablespace Name**: Specifies index tablespace name: Default value is **MDB_INDEX**.

8. Click **Next.**
9. On the product selection page, the patch installer identifies the CA Service Management products installed in the system.

   Note: On the product selection page, deselect the products for which the patch is already updated.

   Verify and click **Next.**
10. If CA Service Catalog is installed in your environment, provide the CA Embedded Entitlements Manager (CA EEM) details:
    a. **CA EEM Server Name**: Specifies the CA EEM server name which is configured with CA Service Catalog.
    b. **CA EEM Admin User Name**: Authenticates the name of the user with Admin access. The default value for Admin user is **EiamAdmin.**
    c. **CA EEM Admin Password**: Specify password for CA EEM admin user.
11. Perform the following step if CA Service Catalog is installed in your environment and you are installing this patch on CA Service Management 14.1:
    a. Select one or both the options available on the CA Service Catalog Import Content page to import the content pack.
12. Review the Patch Information Summary page and click **Next**.
13. Review Installation progress. Click **Install** to install the selected product/products on your local system.
14. Review the installation task review progress bar. Once it reaches 100%, click **Next**.

15. Review patch Installation summary screen for the following:
    - Click the log folder URL link to view log information.
    - To view post-installation tasks based on your server configuration, see Post-Install Tasks (see page 700).
16. Click **Finish** to exit the installer.

> **Note:** If patch installation fails on a server where you have installed more than one CA Service Management product, retry the installation. Deselect the failed product from the installer screen and proceed with the installation.

> **Note:** If patch installation fails for a product, retry the installation by using the **Retry** option in the wizard where it fails. If retry does not work, exit the installer and relaunch it. If problem persists, contact CA Support (http://www.ca.com/in/support.aspx).

If you are installing CA Service Management 14.1.02 (CA SDM and USS) on Non-Windows, refer to the following topics:

- Install CA Service Management 14.1.02 Patch on Linux (CA SDM and USS) (see page 693)
- Install CA Service Desk Manager 14.1.02 Patch on Solaris (see page 698)
- Install CA Service Desk Manager 14.1.02 Patch on AIX (see page 695)

Install CA Service Management 14.1.02 (Non-Windows)

To install CA Service Management 14.1.02 on Non-Windows, perform the following:

> **Important:** If you have applied Test Fixes on CA Service Management 14.1.02, you must not reapply the CA Service Management 14.1.02 patch as it may override the Test Fix changes.

> **Note:** On Non-Windows, if you try to reapply CA Service Management 14.1.02 patch (CA SDM and USS) on a system, an error message is displayed that the patch is already applied. Reapplying the patch does not work.

- Install CA Service Management 14.1.02 Patch on Linux (CA SDM and USS) (see page 693)

- Install CA Service Desk Manager 14.1.02 Patch on AIX (see page 695)
- Install CA Service Desk Manager 14.1.02 Patch on Solaris (see page 698)

Install CA Service Management 14.1.02 Patch on Linux (CA SDM and USS)

Note: On Non-Windows,reapplying the CA Service Management 14.1.02 for CA SDM and USS is not allowed. To reapply, first uninstall the patch and reinstall. For more information on how to uninstall the patch, see Uninstall CA Service Management 14.1.02 . (see page 727)

Ensure that you have verified and completed the installation prerequisites (see page 398) before proceeding with patch installation. Perform the following steps for installing the patch (CA SDM and USS) on Linux:

Note: If you are installing the patch on CA SDM 14.1 or 14.1.01, consider the following based on your server configuration:

- Advanced Availability: log on to the standby server, which you plan to promote as the new background server and install the patch.
- Conventional: log on to the primary server.

1. Download **RO86285.tar.Z** file from CA Support (http://www.ca.com/in/support.aspx).
2. Untar the tar.Z by executing the following command:

   ```
   tar -xvzf
   RO86285
   .tar.Z
   ```

3. Untar **CASM_14.1.02_CommonPatchInstaller_Linux.tar.gz** using the following command:

   ```
   tar -xvzf CASM_14.1.02_CommonPatchInstaller_Linux.tar.gz
   ```

4. Set the CA SDM bin and LIB environment variables.
   For example:

   ```
   export PATH=/opt/CA/ServiceDeskManager/bin:$PATH

   export LD_LIBRARY_PATH=/opt/CA/ServiceDeskManager/lib:$LD_LIBRARY_PATH
   ```

5. Run setup file to install CA Service Management 14.1.02 using the following command:

   ```
   ./setup.sh
   ```

6. Review and accept the license agreement terms.

7. In Database Configuration, select **Oracle** as the database type. Ensure that you have installed Oracle database client in your system.

   Note: In case of CA SDM, the installer detects and identifies if there is a primary or standby server (Conventional or Advanced Availability) and displays the MDB database screen.

   Provide the following Oracle database configuration details:

   - **Database Server**: Specifies the host name of Oracle database server.
     If the target instance is part of a clustered instance, the virtual host name of the cluster must be used.
   - **Oracle Service Name**: Specifies the Oracle Service name.
   - **Listener Port**: Specifies the listener port for database.
   - **Net Service Name**: Identifies the Net Service Name of Oracle database where the database resides.
     If database is remote, use the Net Service Name that is defined in Oracle client on the local computer. CA SDM accesses the database through a local installation of the Oracle client.
   - **DBA User Name**: Authenticates the name of the user with DBA access. The default value for DBA user is **SYS.**
   - **DBA User Password**: Authenticates the password for DBA user.
   - **mdbadmin Password**: Specify password for mdbadmin user.
   - **Confirm mdbadmin Password**: Confirm mdbadmin user password.
   - **Tablespace Path (on DB Server)**: Specifies the tablespace directory on the database server.
   - **Oracle Home Path**: Specifies the Oracle client 32-bit path.
   - **Data Tablespace Name**: Specifies tablespace name. The default value is **MDB_DATA**.
   - **Index Tablespace Name**: Specifies index tablespace name: Default value is **MDB_INDEX**.

8. Click **Next.**
9. On the product selection page, the patch installer identifies the CA Service Management products installed in the system. Verify and click **Next.**
10. Review the Patch Information Summary page and click **Next**.

11. Review the Installation progress. Click **Install** to install the selected items on your local system.

12. Review the installation task review progress bar. Once it reaches 100%, click **Next**.

13. Review the patch Installation summary screen for the following:

    - For log information, copy the log folder path to a browser.
    - Copy the URL link for post-Installation tasks to see Post Installation Steps for CA SDM Conventional Configuration (see page 700) or Post Installation Steps for Advanced Availability Configuration (see page 704).

14. Click **Finish** to exit the installer.

Note: If patch installation fails on a server where you have installed more than one CA Service Management product, retry the installation. Deselect the failed product from the installer screen and proceed with the installation.

Note: If patch installation fails for a product, retry the installation by using the **Retry** option in the wizard where it fails. If retry does not work, exit the installer and relaunch it. If problem persists, contact CA Support (http://www.ca.com/in/support.aspx).

Install CA Service Desk Manager 14.1.02 Patch on AIX

Note: On Non-Windows,reapplying the CA Service Management 14.1.02 for CA SDM and USS is not allowed. To reapply, first uninstall the patch and reinstall. For more information on how to uninstall the patch, see Uninstall CA Service Management 14.1.02 . (see page 727)

Ensure that you have verified and completed CA SDM installation prerequisites (see page 398)before proceeding with patch installation. Perform the following to install CA SDM patch on AIX:

Note: If you are installing the patch on CA SDM 14.1 or 14.1.01, consider the following based on your server configuration:

- Advanced Availability: log on to the standby server, which you plan to promote as the new background server and install the patch.
- Conventional: log on to the primary server.

1. Download **RO86295.tar.Z** file from CA Support (http://www.ca.com/in/support.aspx).
2. Untar the **RO86295.tar.Z** file by executing the following command:

   ```
   Bash# gtar -xvzf RO86295.tar.z
   ```

3. Untar the CASM_14.1.02_CommonPatchInstaller_Aix.tar.gz by executing the following command:

   ```
   Bash# gtar -xvzf
   CASM_14.1.02_CommonPatchInstaller_Aix.tar.gz
   ```

4. Set CA SDM bin and LIB environment variables.
   For example:

   ```
   export PATH=/opt/CA/ServiceDeskManager/bin:$PATH
   ```

   ```
   export LIBPATH=/opt/CA/ServiceDeskManager/lib:$LIBPATH
   ```

5. Run setup file to install CA Service Management 14.1.02 using the following command:

   ```
   ./setup.sh
   ```

6. Review and accept the license agreement terms.
7. In Database Configuration, select Oracle as the database type. Ensure that you have installed Oracle database client in your system.

   Note: In case of CA SDM, the installer detects and identifies if there is a primary or standby server (Conventional or Advanced Availability) and displays the MDB database screen.

   Provide the following Oracle configuration details:

   - **Database Server**: Specifies the host name of Oracle database server.
     If the target instance is part of a clustered instance, the virtual host name of the cluster must be used.
   - **Oracle Service Name**: Specifies the Oracle Service name.
   - **Listener Port**: Specifies the listener port for database.
   - **Net Service Name**: Identifies the Net Service Name of Oracle database where the database resides.
     If database is remote, use the Net Service Name that is defined in Oracle client on the local computer. CA SDM accesses the database through a local installation of the Oracle client.

- **DBA User Name**: Authenticates the name of the user with DBA access. The default value for DBA user is **SYS.**
- **DBA User Password**: Authenticates the password for DBA user.
- **mdbadmin Password**: Specify password for mdbadmin user.
- **Confirm mdbadmin Password**: Confirm mdbadmin user password.
- **Tablespace Path (on DB Server)**: Specifies the tablespace directory on the database server.
- **Oracle Home Path**: Specifies the Oracle client 32-bit path.
- **Data Tablespace Name**: Specifies tablespace name. The default value is **MDB_DATA**.
- **Index Tablespace Name**: Specifies index tablespace name: Default value is **MDB_INDEX**.

8. Click **Next.**
9. On the product selection page, the patch installer identifies the CA Service Management products installed in the system. Verify and click **Next.**
10. Review the Patch Information Summary page and click **Next**.
11. Review Installation progress. Click **Install** to install the selected product/products on your local system.
12. Review installation task review progress bar. Once it reaches 100%, click **Next**.
13. Review the patch Installation summary screen for the following:
    - For log information, copy the log folder path to a browser.
    - Copy the URL link for post-Installation tasks to see Post Installation Steps for CA SDM Conventional Configuration (see page 700) or Post Installation Steps for Advanced Availability Configuration (see page 704).
14. Click **Finish** to exit the installer.

Note: If patch installation fails, retry the installation by using the Retry option in the wizard where it fails. If retry does not work, exit the installer and relaunch it. If problem persists, contact CA Support.

Install CA Service Desk Manager 14.1.02 Patch on Solaris

Note: On Non-Windows,reapplying the CA Service Management 14.1.02 for CA SDM and USS is not allowed. To reapply, first uninstall the patch and reinstall. For more information on how to uninstall the patch, see Uninstall CA Service Management 14.1.02 . (see page 727)

Ensure that you verified and completed the CA SDM installation prerequisites (see page 398)before proceeding with patch installation. Perform the following to install CA SDM patch on AIX:

Note: If you are installing the patch on CA SDM 14.1 or 14.1.01, consider the following based on your server configuration:

- Advanced Availability: Log on to the standby server, which you plan to promote as the new background server and install the patch.
- Conventional: Log on to the primary server.

1. Download **RO86282.tar.Z** file from CA Support (http://www.ca.com/in/support.aspx).
2. Run the following command to untar the RO86282.tar.Z file:

   ```
   $ gtar -xvzf RO86282
   .tar.Z
   ```

3. Run the following command to untar **CASM_14.1.02_CommonPatchInstaller_Solaris.tar.gz**:

   ```
   $ gtar -xvzf CASM_14.1.02_CommonPatchInstaller_Solaris.tar.gz
   ```

4. Set CA SDM bin and LIB environment variables.
   For example:

   ```
   export PATH=/opt/CA/ServiceDeskManager/bin:$PATH

   export LD_LIBRARY_PATH=/opt/CA/ServiceDeskManager/lib:$LD_LIBRARY_PATH
   ```

5. Run setup file to install CA Service Management 14.1.02 using the following command:

   ```
   ./setup.sh
   ```

6. Review and accept the license agreement terms.
7. In Database Configuration, select Oracle as the database type. Ensure that you have installed Oracle database client in your system.

Note: In case of CA SDM, the installer detects and identifies if there is a primary or standby server (Conventional or Advanced Availability) and displays the MDB database screen.

Provide the following Oracle database configuration details:

- **Database Server**: Specifies the host name of Oracle database server.
  If the target instance is part of a clustered instance, the virtual host name of the cluster must be used.
- **Oracle Service Name**: Specifies the Oracle Service name.
- **Listener Port**: Specifies the listener port for database.
- **Net Service Name**: Identifies the Net Service Name of Oracle database where the database resides.
  If database is remote, use the Net Service Name that is defined in Oracle client on the local computer. CA SDM accesses the database through a local installation of the Oracle client.
- **DBA User Name**: Authenticates the name of the user with DBA access. The default value for DBA user is **SYS.**
- **DBA User Password**: Authenticates the password for DBA user.
- **mdbadmin Password**: Specify password for mdbadmin user.
- **Confirm mdbadmin Password**: Confirm mdbadmin user password.
- **Tablespace Path (on DB Server)**: Specifies the tablespace directory on the database server.
- **Oracle Home Path**: Specifies the Oracle client 32-bit path.
- **Data Tablespace Name**: Specifies tablespace name. The default value is **MDB_DATA**.
- **Index Tablespace Name**: Specifies index tablespace name: Default value is **MDB_INDEX**.

8. Click **Next.**
9. On the product selection page, the patch installer identifies the CA Service Management products installed in the system. Verify and click **Next.**
10. Review the Patch Information Summary page and click **Next**.
11. Review the Installation progress. Click **Install** to install the selected items on your local system.
12. Review the installation task review progress bar. Once it reaches 100%, click **Next**.

13. Review the Patch Installation summary screen.
    For log information, copy the log folder path to a browser.
    To view post-installation tasks based on your server configuration and log folder, see, Post Installation Steps for CA SDM Conventional Configuration (see page 700) or Post Installation Steps for Advanced Availability Configuration (see page 704).

14. Click **Finish** to exit the installer.

Note: If patch installation fails, retry the installation by using the **Retry** option in the wizard where it fails. If retry does not work, exit the installer and relaunch it. If problem persists, contact CA Support (http://www.ca.com/in/support.aspx).

Post-Installation Tasks

Complete the following post-installation tasks based on the CA Service Management 14.1.02 product /products installed in your system:

- Post Installation Steps for CA Service Desk Manager (see page 700)
- Post Installation Steps for CA Asset Portfolio Manager (see page 722)
- Post Installation Steps for CA Service Catalog (see page 723)
- Post Installation Steps for Unified Self-Service (see page 724)

Post Installation Steps for CA Service Desk Manager

After installing CA SDM 14.1.02, perform the following post-installation steps based on your server configuration:

- Post Installation Steps for Conventional Configuration (see page 700).
- Post Installation Steps for Advanced Availability Configuration. (see page 704)
- Optional Steps for Specific Issues when Installing CA Service Desk Manager 14.1.02 (see page 711) .

For more information on how to perform post-backout steps, see Post-Backout Steps for CA Service Desk Manager 14.1.02. (see page 733)

Post Installation Steps for CA SDM Conventional Configuration

Complete the following post installation steps for CA SDM Conventional Configuration:

- Install CA Service Management 14.1.02 on CA SDM 14.1 (see page 701)
  - Mandatory Steps (see page 701)
  - Mandatory Steps for CA Business Intelligence (see page 702)
    - Import Service Desk BIARs (see page 702)
    - Use Dashboard Reports (see page 703)
  - Mandatory Steps for CA SDM Mobility (see page 703)

- Install CA Service Management 14.1.02 on CA SDM 14.1.01 (see page 703)

Install CA Service Management 14.1.02 on CA SDM 14.1

Follow these steps:

1. To reconfigure CA SDM on primary server, run the following command:

   ```
   pdm_configure
   ```

   Important! Do not select Load Default Data.

2. Navigate to *NX_ROOT**data* folder.

3. To load data, run the following commands:

   ```
   pdm_load -f santafe_insert.dat
   pdm_load -f santafe_update.dat
   pdm_load -f tucson_insert.dat
   pdm_load -r -f tucson_delete.dat
   ```

4. Alert users to clear browser cache. Run the following command:

   ```
   pdm_webcache -Hpdm_webcache -b
   ```

5. Repeat **Step 1** and **Step 4** on the secondary server.

Mandatory Steps

Follow these steps:

1. Create a backup of *web.xml* from *NX_ROOT**bopcfg**www**CATALINA_BASE**webapps**CAisd**WEB-INF* in your local directory to perform a backout, if required.

2. Open the *web.xml* file from *NX_ROOT**bopcfg**www**CATALINA_BASE**webapps**CAisd**WEB-INF.*

3. Search for the following statement:
   <!-- Add filter here -->

4. Copy and paste the following configuration under the *<!-- Add filter here -->* statement:

   ```
   <!-- Cross-origin support for Attachments Servlet -->
   <filter>
   <filter-name>CORS</filter-name>
   <filter-class>com.thetransactioncompany.cors.CORSFilter</filter-class>
   <init-param>
   <param-name>cors.supportedMethods</param-name>
   <param-value>POST, GET, OPTIONS</param-value>
   </init-param>
   <init-param>
   <param-name>cors.allowOrigin</param-name>
   ```

```
<param-value>*</param-value>
</init-param>
</filter>
```

5. Search for the following statement:
   <!-- Add filter-mapping here -->

6. Copy and paste the following configuration under the *<!-- Add filter-mapping here -->* statement:

```
<!-- Cross-origin support for Attachments Servlet -->
<filter-mapping>
<filter-name>CORS</filter-name>
<servlet-name>UploadServlet</servlet-name>
</filter-mapping>
```

7. Verify that the configurations under the filter and filter-mapping statements are as shown in the following sample:

```
<!-- Add filter here -->
<!-- Cross-origin support for Attachments Servlet -->
<filter>
<filter-name>CORS</filter-name>
<filter-class>com.thetransactioncompany.cors.CORSFilter</filter-class>
<init-param>
<param-name>cors.supportedMethods</param-name>
<param-value>POST, GET, OPTIONS</param-value>
</init-param>
<init-param>
<param-name>cors.allowOrigin</param-name>
<param-value>*</param-value>
</init-param>
</filter>
<!-- Add filter-mapping here -->
<!-- Cross-origin support for Attachments Servlet -->
<filter-mapping>
<filter-name>CORS</filter-name>
<servlet-name>UploadServlet</servlet-name>
</filter-mapping>
```

8. Save and close the *web.xml* file.

9. Repeat the **Steps 1-8** to update *web.xml.tpl* file in the *NX_ROOT\samples\pdmconf\web.xml.tpl* folder to avoid losing these changes when pdm_configure is run.

10. Run the *pdm_configure* command.

11. Start CA SDM services.

Mandatory Steps for CA Business Intelligence

Complete the following steps if you have installed CA Business Intelligence:

- Import Service Desk BIARs (see page 702)
- Use Dashboard Reports (see page 703)

Import Service Desk BIARs

Follow these steps:

- Download the required patch from CA Support and follow the instructions provided in the Test Fix.
  - Windows: RO79125
  - Linux: RO79126
  - Solaris: RO79127
  - AIX: RO79128
    For example, download the Windows patch readme RO79125 and follow the instructions mentioned in the section *Procedure to create a backup .biar file*.

Use Dashboard Reports

Before you use dashboard reports, ensure that both CA SDM and CA Service Catalog use the same CA Business Intelligence server.

- Run the following queries if you have configured MDB with Oracle database:

```
create or replace function MDBADMIN.left(str1 varchar2 :=NULL,num1 NUMBER)
RETURN VARCHAR2
as
ascii_chr varchar2(32767);
begin
ascii_chr:= substr(str1,1, num1);
return ascii_chr;
end;

Update report_labels set language_code ='en' where language_code='en ';
Update report_labels set language_code ='De' where language_code='De ';
```

Mandatory Steps for CA SDM Mobility

Follow these steps:

1. Navigate to *NX_ROOT\bopcfg\www\CATALINA_BASE_REST\webapps*.
2. Create a backup and delete the workflow folder.
3. Verify that the workflow folder is created after the CA SDM server services are recycled.

Note: To resolve specific issues when installing CA SDM 14.1.02, see Optional Steps for Specific Issues when Installing CA Service Desk Manager 14.1.02 (see page 711).

Install CA Service Management 14.1.02 on CA SDM 14.1.01

If you are installing CA SDM 14.1.02 on CA SDM 14.1.01 installation, perform the following steps:

Important: Before you proceed, ensure that you have performed the post-installation steps mentioned in the CA SDM 14.1.01 readme.

Follow these steps:

1. To reconfigure CA SDM on primary server, run the following command:

   ```
   pdm_configure
   ```

   Important! Do not select **Load Default Data**.

2. Navigate to the *NX_ROOT*\data folder.

3. To load data, run the following commands:

   ```
   pdm_load -f tucson_insert.dat
   pdm_load -r -f tucson_delete.dat
   ```

4. To alert users to clear browser cache, run the following commands:

   ```
   pdm_webcache -Hpdm_webcache -b
   ```

5. Repeat **Step 1** and **Step 4** on the secondary server.

   Note: To resolve specific issues when installing CA SDM 14.1.02, see Optional Steps for Specific Issues when Installing CA Service Desk Manager 14.1.02 (see page 711).

Post Installation Steps for Advanced Availability Configuration

The following post-installation options are available for CA SDM Advanced Availability (AA) Configuration:

Install CA Service Management 14.1.02 on CA SDM 14.1

For this procedure, the following host name examples are considered:

- Background server host name is *sdmcahost1*
- Standby server host name is *sdmcahost2*
- Application server host name is *sdmcahost3*

Follow these steps:

1. Stop CA SDM services on all Advanced Availability servers.
2. Log on to the standby server that you want to promote as the new background server.
   For example, promote *sdmcahost2* server as the background server.
3. Run the following command on the standby server to start the CA SDM configuration wizard:

   ```
   pdm_configure
   ```

   Important: On the last configuration screen, before clicking **Finish**, uncheck the **Start service when completed** checkbox.

   For example, execute the *pdm_configure* command on the *sdmcahost2* server.
4. To promote the standby server as the new background server, perform the following steps.

1. a. To suppress version control on the standby (*sdmcahost2)* and background (*sdmcahost1)* servers, run the following command:

      ```
      pdm_server_control -v
      ```

   b. Start the services on standby server (*sdmcahost2)*.

   c. To promote the standby server (*sdmcahost2)* as the new background server, run the following command:

      ```
      pdm_server_control -b
      ```

2. To alert users to clear browser cache, run the following command:

   ```
   pdm_webcache -Hpdm_webcache -b
   ```

3. On the original background server (*sdmcahost1)*, run the CA SDM 14.01.02 patch installer.
   For more information on how to install the patch on a specific operating system, see Install CA Service Management 14.1.02 (see page 688). For example, to install CA SDM 14.1.02 on Windows, see Install CA Service Management 14.1.02 (Windows) (see page 688).
4. Run the following command on the original background server (*sdmcahost1)* to start the CA SDM configuration wizard:

   ```
   pdm_configure
   ```

   Important: On the last configuration screen, before clicking **Finish**, uncheck the **Start service when completed** checkbox.

5. Execute the following commands on the original background server (*sdmcahost1)*:

a. To suppress version control on the original background server (*sdmcahost1)*, run the following command:

```
pdm_server_control -v
```

b. Start the services on the original background server (*sdmcahost1)*.

c. To promote the original background server (*sdmcahost1)* as the background server, run the following command:

```
pdm_server_control -b
```

6. Perform the following steps:

a. Navigate to *NX_ROOT\data.*

b. To load data from CA SDM 14.1.01, run the following commands:

```
pdm_load -f santafe_insert.dat
pdm_load -f santafe_update.dat
pdm_load -f tucson_insert.dat
pdm_load -r -f tucson_delete.dat
```

c. To alert users to clear browser cache, run the following command:

```
pdm_webcache -H
pdm_webcache -b
```

7. Start the services on the original standby server (*sdmcahost2)*.

8. On all application servers (*sdmcahost3)*, run the CA SDM 14.01.02 patch installer.
For more information on how to install the patch on a specific operating system, see Install CA Service Management 14.1.02 (see page 688). For example, to install CA SDM 14.1.02 on Windows, see Install CA Service Management 14.1.02 (Windows) (see page 688).

9. Run the following command on the application server (*sdmcahost3)* to start the CA SDM configuration wizard:

```
pdm_configure
```

10. To alert users to clear browser cache, run the following command:

```
pdm_webcache -H
pdm_webcache -b
```

Mandatory Steps

Follow these steps:

1. Open *web.xml* from *NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF.*

2. Search for the following statement:
<!-- Add filter here -->

3. Copy and paste the following configuration under the *<!-- Add filter here -->* statement:

```
<!-- Cross-origin support for Attachments Servlet -->
<filter>
<filter-name>CORS</filter-name>
```

```
<filter-class>com.thetransactioncompany.cors.CORSFilter</filter-class>
<init-param>
<param-name>cors.supportedMethods</param-name>
<param-value>POST, GET, OPTIONS</param-value>
</init-param>
<init-param>
<param-name>cors.allowOrigin</param-name>
<param-value>*</param-value>
</init-param>
</filter>
```

4. Search for the following statement:
   <!-- Add filter-mapping here -->

5. Copy and paste the following configuration under the *<!-- Add filter-mapping here -->* statement:

```
<!-- Cross-origin support for Attachments Servlet -->
<filter-mapping>
<filter-name>CORS</filter-name>
<servlet-name>UploadServlet</servlet-name>
</filter-mapping>
```

6. Verify that the configurations under the filter and filter-mapping statements are as shown in the following sample:

```
<!-- Add filter here -->
<!-- Cross-origin support for Attachments Servlet -->
<filter>
<filter-name>CORS</filter-name>
<filter-class>com.thetransactioncompany.cors.CORSFilter</filter-class>
<init-param>
<param-name>cors.supportedMethods</param-name>
<param-value>POST, GET, OPTIONS</param-value>
</init-param>
<init-param>
<param-name>cors.allowOrigin</param-name>
<param-value>*</param-value>
</init-param>
</filter>
<!-- Add filter-mapping here -->
<!-- Cross-origin support for Attachments Servlet -->
<filter-mapping>
<filter-name>CORS</filter-name>
<servlet-name>UploadServlet</servlet-name>
</filter-mapping>
```

7. Save the *web.xml* file.

8. Restart tomcat.

9. Repeat the **Steps 1-8** to update the *web.xml.tpl* file located in *NX_ROOT\samples\pdmconf\web.xml.tpl.*

10. Run the *pdm_configure* command.

11. Start CA SDM services.

Mandatory Steps for the CA Business Intelligence

Complete the following steps if you have installed CA Business Intelligence:

- Import Service Desk BIARs (see page 708)
- Use Dashboard Reports (see page 708)

Import Service Desk BIARs

Follow these steps:

- Download the required patch from CA Support and follow the instructions provided in the Test Fix.
  - Windows: RO79125
  - Linux: RO79126
  - Solaris: RO79127
  - AIX: RO79128
    For example, download the Windows patch readme RO79125 and follow the instructions mentioned in the section *Procedure to create a backup .biar file*.

Use Dashboard Reports

Follow these steps:

1. Ensure that both CA SDM and CA Service Catalog use the same CA Business Intelligence server.
2. If you have configured MDB with Oracle database, run the following commands:

```
create or replace function MDBADMIN.left(str1 varchar2 :=NULL,num1 NUMBER)
 RETURN VARCHAR2
 as
 ascii_chr varchar2(32767);
 begin
 ascii_chr:= substr(str1,1, num1);
 return ascii_chr;
 end;

Update report_labels set language_code ='en' where language_code='en ';
Update report_labels set language_code ='De' where language_code='De ';
```

Mandatory Steps for CA SDM Mobility

Follow these steps:

1. Navigate to *NX_ROOT\bopcfg\www\CATALINA_BASE_REST\webapps*.
2. Create a backup and delete the workflow folder.
3. Verify that the workflow folder is created after CA SDM server services are recycled.

Note: To resolve specific issues when installing CA SDM 14.1.02, see Optional Steps for Specific Issues when Installing CA Service Desk Manager 14.1.02 (see page 711).

Install CA Service Management on CA SDM 14.1.01

Perform the following post-installation steps, if you have installed CA SDM 14.1.02 on CA SDM 14.1.0:

Important: Ensure that you have performed the post-installation steps mentioned in patch installation on 14.1 (see page 704).

1. Stop CA SDM services on all Advanced Availability servers.
2. Log on to the standby server to promote it as the new background server.
   For example, promote the *sdmcahost2* server as the background server.
3. Run the following command on the standby server (*sdmcahost2)* to start the CA SDM configuration wizard:

   ```
   pdm_configure
   ```

   Important: On the last configuration screen, before clicking **Finish**, uncheck the **Start service when completed** checkbox.

4. To promote the standby server (*sdmcahost2)* as the new background server, perform the following steps:
   a. To suppress version control on the standby (*sdmcahost2)* and background servers (*sdmcahost1)*, run the following command:

      ```
      pdm_server_control -v
      ```

   b. Start the services on standby server (*sdmcahost2)*.
   c. To promote the standby server (*sdmcahost2)* as the new background server, run the following command:

      ```
      pdm_server_control -b
      ```

5. To alert users to clear browser cache, run the following commands:

   ```
   pdm_webcache -Hpdm_webcache -b
   ```

6. On the original background server (*sdmcahost1)*, run the CA SDM 14.01.02 patch installer. For more information on how to install the patch on a specific operating system, see Install CA Service Management 14.1.02 (see page 688). For example, to install CA SDM 14.1.02 on Windows, see Install CA Service Management 14.1.02 (Windows) (see page 688).
7. Run the following command on the original background server (*sdmcahost1)* to start the CA SDM configuration wizard:

   ```
   pdm_configure
   ```

Important: On the last configuration screen, before clicking **Finish**, uncheck the **Start service when completed** checkbox.

8. Execute the following commands on the original background server (*sdmcahost1)*:

    a. To suppress version control on the original background server (*sdmcahost1)*, run the following command:

    ```
    pdm_server_control -v
    ```

    b. Start the services on the original background server (*sdmcahost1)*.

    c. To promote the original background server (*sdmcahost1)* as the background server, run the following command:

    ```
    pdm_server_control -b
    ```

9. Perform the following steps:

    a. Navigate to the *NX_ROOT**data* folder.

    b. To load data from CA SDM 14.1.01, run the following commands:

    ```
    pdm_load -f tucson_insert.dat
    pdm_load -r -f tucson_delete.dat
    ```

    c. To alert users to clear browser cache, run the following command:

    ```
    pdm_webcache -H
    pdm_webcache -b
    ```

10. Start the services on the original standby server (*sdmcahost2)*.

11. On all application servers (*sdmcahost3)*, run the CA SDM 14.01.02 patch installer.
    For more information on how to install the patch on a specific operating system, see Install CA Service Management 14.1.02 (see page 688). For example, to install CA SDM 14.1.02 on Windows, see Install CA Service Management 14.1.02 (Windows) (see page 688).

12. Run the following command on the application servers (*sdmcahost3)* to start the CA SDM configuration wizard:

    ```
    pdm_configure
    ```

13. To alert users to clear browser cache, run the following command:

    ```
    pdm_webcache -H
    pdm_webcache -b
    ```

Note: To resolve specific issues when installing CA SDM 14.1.02, see Optional Steps for Specific Issues when Installing CA Service Desk Manager 14.1.02 (see page 711).

Optional Steps for Specific Issues when Installing CA Service Desk Manager 14.1.02

This section lists how to resolve specific issues when installing CA Service Desk Manager 14.1.02:

Optional Steps for Specific Issues when Installing CA SDM 14.1.02 on CA SDM 14.1

Prob# USRD 2113

KT_DAEMON MAY TERMINATE WITH STRING TOO BIG ERROR

Resolution:

This fix introduces an NX variable **NX_ALLOW_COMMENT_VIA_UPDATE_STATUS**. Set the value of the variable to **Yes**, to insert comments without changing the status via Update Status window.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s ALLOW_COMMENT_VIA_UPDATE_STATUS -v yes -a pdm_option.inst
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s ALLOW_COMMENT_VIA_UPDATE_STATUS -v yes -a pdm_option.inst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 2971

SORT FAILS IN DETAIL PAGE FOR ASCENTED CHARACTERS IN ORACLE

This fix introduces an NX variable **@NX_ORCL_SORTING**. Set this variable to **BINARY_CI** then the CA Service Desk Manager sorts the values according to BINARY_CI. You can also use JAPANESE_M_CI for sorting the Japanese or kana sensitive values and GENERIC_M_CI for polish or Czech characters.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s ORCL_SORTING -v BINARY_CI -a pdm_option.inst
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s ORCL_SORTING -v BINARY_CI -a pdm_option.inst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 2991

EXPORTING MORE THAN 5000 CONFIGURATION ITEMS FAILS

This fix introduces an NX variable, **@NX_EXPORT_STATUS_TIMEOUT**. Set this variable to a value greater than 300 milliseconds, which is used if there are more than 5000 configuration items.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s EXPORT_STATUS_TIMEOUT –v 1800 –a pdm_option.inst
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s EXPORT_STATUS_TIMEOUT -v 1800 -a pdm_option.inst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 2992

KD EMAIL NOTIFICATION SENT WITH HIGH URGENCY LEVEL

This fix introduces an NX variable **@NX_KT_EMAIL_NOTIFY_LEVEL**. Set this variable to the new notification urgency level as: 1-Low, 2-Normal, 3-High, 4-Emergency

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s KT_EMAIL_NOTIFY_LEVEL -v 1 -a pdm_option.inst

Where, 1 is the Low urgency level
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s KT_EMAIL_NOTIFY_LEVEL -v 1 -a pdm_option.inst -t
 Where, 1 is the Low urgency level
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 3024

HEALTHSERVLET MAKES TOMCAT FILE SIZE HUGE

If HealthServlet webapp is already deployed, perform the following steps:

1. Stop the Apache Tomcat server on which HealthServlet webapp is hosted.
2. Take a backup of the file: */webapps/HealthServlet/WEB-INF/classes/health.xml*
3. Delete the HealthServlet */webapps/HealthServlet* folder.
4. Copy the file *$NX_ROOT/samples/HealthServlet/HealthServlet.war* to *webapps* folder.
5. Restart the Apache Tomcat server.
6. Copy back the *health.xml* file to the folder: */webapps/HealthServlet/WEB-INF/classes*

Prob# USRD 3029

SQL ERROR MAY OCCUR WHEN OPENING KNOWLEDGE DOCUMENT

This fix introduces an NX variable **@NX_KD_TICKET_ACCURACY**. This variable is used to specify the maximum number of tickets for which the CA Service Desk Manager guarantees an accurate count when displaying a Knowledge Document. These are tickets that have either been solved by the Knowledge Document or that were opened based on the Knowledge Document. The count of these tickets is free from canceled tickets up to the number specified in the NX_KD_TICKET_ACCURACY variable. By default, this value is set to 300.

Note: Setting this value too high may impact performance when opening up Knowledge Documents, depending on your environment. This fix requires that the NX variable **@NX_IGNORE_CANCELED** also be installed and set to **Yes**.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s KD_TICKET_ACCURACY -v 300 -a pdm_option.inst
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s KD_TICKET_ACCURACY -v 300 -a pdm_option.inst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 3055

ALLOW STRICT SURVEYS TO BE SENT TO MULTIPLE TICKETS

This fix introduces an NX variable **@NX_ALLOW_STRICT_SURVEY_FOR_MULTIPLE_TICKETS**. Set this variable to **Yes**, to ensure that strict surveys allow one response per ticket per contact.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s ALLOW_STRICT_SURVEY_FOR_MULTIPLE_TICKETS -v Yes -a pdm_option.
inst
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s ALLOW_STRICT_SURVEY_FOR_MULTIPLE_TICKETS -v Yes -a pdm_option.
inst –t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 3067

REPORTED BY FIELD NOT FOCUSABLE

This fix introduces an NX variable **@NX_FOCUS_REPORTED_BY**. Set this variable to **Yes**.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s FOCUS_REPORTED_BY -v <XXX> -a pdm_option.inst
```

Where '<XXX>' is set to **Yes**

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s FOCUS_REPORTED_BY -v <XXX> -a pdm_option.inst -t
 Where '<XXX>' is set to Yes
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 3200

TWO WORKFLOW TASKS STATUS MAY SHOW PENDING

The fix introduces an NX variable **@NX_INSERT_WF_PREVIOUS** to avoid the status of workflow task to become pending.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s INSERT_WF_PREVIOUS -v YES -a pdm_option.inst
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s INSERT_WF_PREVIOUS -v YES -a pdm_option.inst –t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 3148

LDAP SERVER CONTACTED WHILE LOGGING IN SSO

This correction introduces an NX variable **@NX_STRIP_DOMAIN_NAME**. Set this variable to **Yes**, to strip the domain name from the login name of the NTLM authenticated user during login to CA Service Desk Manager.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s STRIP_DOMAIN_NAME -v Yes -a pdm_option.inst
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s STRIP_DOMAIN_NAME -v Yes -a pdm_option.inst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 3124

SLOW PERFORMANCE DUE TO QUEUED TRANSACTIONS ON

This fix introduces an NX variable **@NX_VIRTDB_LOCK_AGENTS**. This variable should be assigned an number equivalent to the number of locking update agents. By default, the value is 1.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s VIRTDB_LOCK_AGENTS -v <XXX> -a pdm_option.inst
 Where, <XXX> is number of locking agent.
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s VIRTDB_LOCK_AGENTS -v <XXX> -a pdm_option.inst -t

Where, <XXX> is number of locking agent.
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 2975

MISSING HTML MESSAGE IN TICKET NOTIFICATION

The fix to this problem introduces an **NX_INSERT_NLH_MSG_HTML** variable that can be tweaked to avoid the problem. Set this variable to **YES**, then the html message body of the notification can be inserted into not_log table. If the *Notification Message Body* is removed from the Default initial message template for request/incident/problem Message Template, the html message will replace the message body of the notification.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s INSERT_NLH_MSG_HTML -v YES -a pdm_option.inst
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s INSERT_NLH_MSG_HTML -v YES -a pdm_option.inst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 3258

UNEXPECTED BEHAVIOUR ON CLICKING CAB CONSOLE B

Follow these steps:

1. Start the CA Service Desk Manager service.
2. From the command prompt, navigate to the *NX_ROOT**data* folder.
3. Backup the *current usp_pdmMacro* and *usp_pdmMacroParam* tables by running the following commands on the command prompt.

   ```
   pdm_extract usp_pdmMacro > USRD_2789_backup_macro.dat
   ```

   ```
   pdm_extract usp_pdmMacroParam > USRD_2789_backup_param.dat
   ```
4. Verify that these files are successfully created.
5. Update the *usp_pdmMacro* and *usp_pdmMacroParam* tables by running the following commands on the command prompt:

   ```
   pdm_load -u -f data_USRD_2789_UPDATE.dat
   ```

   ```
   pdm_load -i -f data_USRD_2789_INSERT_en-US.dat
   ```
6. Then clear the cache of these tables by executing the following commands:

   ```
   pdm_cache_refresh -t usp_pdmMacro
   ```

```
pdm_cache_refresh -t usp_pdmMacroParam
```

Prob# USRD 2976

PDM_ISQL RETURNS ERROR WHEN PDMWEB.EXE IS RENAMED

- This fix introduces an NX variable **@NX_PDMWEB_RENAMED_TO**. Set the variable to the new cgi name of the webengine.
  To install the option, run the following command from the command prompt on the primary server:

  ```
  pdm_options_mgr -c -s PDMWEB_RENAMED_TO -v <XXX> -a pdm_option.inst
  ```

  Where, <XXX> is the input name used instead of *pdmweb*

  To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

  ```
  pdm_options_mgr -c -s PDMWEB_RENAMED_TO -v <XXX> -a pdm_option.inst -t
  ```

  Restart the server.

- This fix introduces an NX variable **@NX_EXE_EXCLUDE**. Set this variable to **Yes**.
  To install the option, run the following command from the command prompt on the primary server:

  ```
  pdm_options_mgr -c -s EXE_EXCLUDE -v <XXX> -a pdm_option.inst
  ```

  Where, <XXX> is set to **Yes**.

  To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

  ```
  pdm_options_mgr -c -s EXE_EXCLUDE -v <XXX> -a pdm_option.inst -t
   Where, <XXX> is set to Yes.
  ```

  Restart the server.

Prob# USRD 3283

PERFORMANCE ISSUES WITH SUPPORT AUTOMATION DOM

This fix introduces an NX variable **@NX_STOP_SA_DOMSRVR_MASS_UPDATES**. This variable is used to specify whether to send mass updates to NX_SA_DOMSRVR process. Set the value to **Yes** to stop sending the mass updates to NX_SA_DOMSRVR process.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s STOP_SA_DOMSRVR_MASS_UPDATES -v Yes -a pdm_option.inst
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s STOP_SA_DOMSRVR_MASS_UPDATES -v Yes -a pdm_option.inst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 3297

KNOWLEDGE REPORT CARD FOR ALL DAYS FAILS

Follow these steps:

1. Copy the contents of *$NX_ROOT\doc\Validation_Patterns_and_Parameters.txt* to the end of *NX_ROOT\bopcfg\www\web.cfg* and *NX_ROOT\bopcfg\www\web.cfg.tpl*, replacing the existing contents of these values in the *web.cfg* and *web.cfg.tpl* files.
   NX_ROOT represents the Service Desk Application Installation folder.

   Note: The contents of *Validation_Patterns_and_Parameters.txt* need to be added to the *web.cfg* file of the desired webengine. For example, if you want to **only** protect the secondary server webengine and the *web.cfg* filename for that webengine is: *secondaryservername-web1.cfg*, then, the contents need to be added to this file and **not** to the default *web.cfg*.

   Important: If the NX_VALIDATE_REQUEST_PARAMETER variable is already installed, you may skip this step.

2. To install the option, run the following command from the command prompt on the primary server:

   ```
   pdm_options_mgr -c -a pdm_option.inst -s VALIDATE_REQUEST_PARAMETER -v 1
   ```

3. To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

   ```
   pdm_options_mgr -c -a pdm_option.inst -s VALIDATE_REQUEST_PARAMETER -v 1 -t
   ```

   For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

4. Restart the CA Service Desk Manager services.

Optional Steps for Specific Issues when Installing CA SDM 14.1.02 on CA SDM 14.1.01

Prob# USRD 2113

KT_DAEMON May Terminate with the STRING TOO BIG Error

Resolution:

The fix introduces a new optional NX variable **NX_ALLOW_COMMENT_VIA_UPDATE_STATUS**. Set the value to **Yes** to insert comments without changing the status through the Update Status window.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s ALLOW_COMMENT_VIA_UPDATE_STATUS -v yes -a pdm_option.inst
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s ALLOW_COMMENT_VIA_UPDATE_STATUS -v yes -a pdm_option.inst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 2971

Sorting of Accented Characters in Oracle Fails

Resolution:

The fix introduces a new optional NX variable **@NX_ORCL_SORTING**. Set the value to **BINARY_CI** to sort the values according to BINARY_CI, **JAPANESE_M_CI** to sort the Japanese or kana sensitive values, or **GENERIC_M_CI** to sort the Polish or Czech characters.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s ORCL_SORTING -v BINARY_CI -a pdm_option.inst
```

To avoid losing the change when you run the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s ORCL_SORTING -v BINARY_CI -a pdm_option.inst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Prob# USRD 2991

Export of 5000 and More Configuration Items Fails

Resolution:

The fix introduces a new optional NX variable **@NX_EXPORT_STATUS_TIMEOUT**. The variable is used if there are more than 5000 configuration items. You can set the varible to a value greater than 300 milliseconds.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s EXPORT_STATUS_TIMEOUT –v 1800 –a pdm_option.inst
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s EXPORT_STATUS_TIMEOUT -v 1800 -a pdm_option.inst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the NX_ROOT directory and restart the server.

Prob# USRD 2992

KD Email Notification is Sent with High Urgency Level

Resolution:

Run the following commands to uninstall the NX variables:

```
pdm_options_mgr -c -s KT_EMAIL_NOTIFY_LEVEL -v 1 -a pdm_option.deinst
where 1 is the Low urgency level.

pdm_options_mgr -c -s KT_EMAIL_NOTIFY_LEVEL -v 1 -a pdm_option.deinst -t
where 1 is the Low urgency level.
```

Note: For each secondary CA SDM server you have configured, manually add or update the NX variable above in each secondary CA SDM server machine within its *NX.env* file located under the NX_ROOT directory. A CA SDM product recycle is normally needed for the new NX variable to take effect.

Prob# USRD 3024

HEALTHSERVLET Increases the Size of the TOMCAT File

Resolution:

If the HealthServlet webapp is already deployed, perform the following steps:

1. Stop the tomcat server where the HealthServlet webapp is hosted.
2. Take a backup of the file */webapps/HealthServlet/WEB-INF/classes/health.xml*
3. Delete the HealthServlet/webapps/HealthServlet folder.
4. Copy the file *NX_ROOT/samples/HealthServlet/HealthServlet.war* to the webapps folder.
5. Restart the tomcat server.
6. Copy the *health.xml* file to the folder */webapps/HealthServlet/WEB-INF/classes.*

Prob# USRD 3029

SQL Error May Occur when Opening the Knowledge Document

Resolution:

This fix introduces a new NX variable @NX_KD_TICKET_ACCURACY. This variable is used to specify the maximum number of tickets to which Service Desk will guarantee an accurate count when displaying a Knowledge Document. These are tickets that have either been solved by the Knowledge Document or that were opened based on the Knowledge Document. The count of these tickets will be guaranteed to be free from canceled tickets up to the number specified in

NX_KD_TICKET_ACCURACY. By default, this value is set to 300. Please note that setting this value too high may impact performance when opening up Knowledge Documents, depending on your environment. As well, please note that this correction requires that the NX variable @NX_IGNORE_CANCELED also be installed and set to “Yes”.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s KD_TICKET_ACCURACY -v 300 -a pdm_option.inst
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s KD_TICKET_ACCURACY -v 300 -a pdm_option.inst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the NX_ROOT directory and restart the server.

Prob# USRD 3055

Allow Strict Surveys to be Sent to Multiple Tickets

Resolution:

The fix introduces a new NX variable **@NX_ALLOW_STRICT_SURVEY_FOR_MULTIPLE_TICKETS**. Set the value to **Yes** to let strict surveys allow one response per ticket per contact.

To install the option, run the following command from the command prompt on the primary server:

```
pdm_options_mgr -c -s ALLOW_STRICT_SURVEY_FOR_MULTIPLE_TICKETS -v Yes -a pdm_option.
inst
```

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s ALLOW_STRICT_SURVEY_FOR_MULTIPLE_TICKETS -v Yes -a pdm_option.
inst –t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the NX_ROOT directory and restart the server.

Prob# USRD 3067

REPORTED BY FIELD NOT FOCUSABLE

Resolution:

The fix introduces a new NX variable **@NX_FOCUS_REPORTED_BY**. You must set the value to **Yes**.

To install the option, run the following command from the command prompt on the primary server::

```
pdm_options_mgr -c -s FOCUS_REPORTED_BY -v <XXX> -a pdm_option.inst
```

where <*XXX*> is set to **Yes**.

To avoid losing changes when you execute the pdm_configure command, run the command with the -t option as follows:

```
pdm_options_mgr -c -s FOCUS_REPORTED_BY -v <XXX> -a pdm_option.inst -t
```

where <*XXX*> is set to **Yes**.

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the NX_ROOT directory and restart the server.

pdm_options_mgr -c -s STOP_SA_DOMSRVR_MASS_UPDATES -v Yes -a pdm_option.inst -t

Post Installation Steps for CA Asset Portfolio Manager

After installing CA Asset Portfolio Management 14.1.02, perform the following post-installation steps:

- Modify the Configurations on Windows Server 2012: (see page 722)
- Modify Event Service (see page 722)
- Modify Import Driver (see page 723)
- Modify Web Server Component (see page 723)

Modify the Configurations on Windows Server 2012:

1. Log in to the CA ITAM web server.
2. Navigate to the *Root/Web Server* folder.
3. Open the *Web.config* file and locate the *system.web* section.
4. Modify the Current Key with the New Key as shown next.
   Current Key:

   ```
   compilation
   ```

   New Key:

   ```
   compilation targetFramework="4.5"
   ```
5. Execute the following command to stop and restart IIS services on the web servers:

   ```
   iisreset
   ```

Modify Event Service

1. Log in to the CA ITAM application server.
2. Navigate to the *Root/Event Service* folder.
3. Open the *CA.Applications.EventService.exe.config* file.
4. Modify the Current Key with the New Key as shown next.
   Current Key:

   ```
   maxNameTableCharCount="16384"
   ```

New Key:

```
maxNameTableCharCount="2147483647"
```

5. Save the file.

Modify Import Driver

1. Log in to the CA ITAM application server.
2. Navigate to the *Root/Import Driver* folder.
3. Open the *ImportDriver.exe.config* file.
4. Modify the Current Key with the New Key as shown next.
   Current Key:

   ```
   maxNameTableCharCount="16384"
   ```

   New Key:

   ```
   maxNameTableCharCount="2147483647"
   ```

5. Save the file.

Modify Web Server Component

1. Log in to the CA ITAM web server.
2. Navigate to the *Root/Web Server* folder.
3. Open the *Web.config* file.
4. Modify the Current Key with the New Key as shown next.

   Current Key:

   ```
   <binding name="st_importBinding"/>
   ```

   New Key:

   ```
   <!--<binding name="st_importBinding" />-->
   <binding name="st_importBinding" maxBufferSize="2147483647"
   maxReceivedMessageSize="2147483647" maxBufferPoolSize="524288" transferMode="
   Buffered">
   <readerQuotas maxDepth="32" maxStringContentLength="2147483647" maxArrayLength="
   2147483647"
   maxBytesPerRead="4096" maxNameTableCharCount="2147483647" />
   </binding>
   >
   ```

5. Save the file.

Post Installation Steps for CA Service Catalog

After installing CA Service Catalog 14.1.02, perform the following post-installation steps:

Enable CORS filter

Perform the following steps to enable CORS filter:

1. Open the *USMHOME/view/webapps/usm/WEB-INF/web.xml* file.
2. Modify the Current Key with the New Key as shown next.
   Current Key:

   ```
   <param-name>cors.allowed.origins</param-name>
   <param-value>*</param-value>
   ```

   New Key:

   ```
   <param-name>cors.allowed.origins</param-name>
   <param-value><http/https>://<Catalog Host Name>:<Catalog Port No>,
   <http/https>://<USS Host Name>:<USS Port No></param-value>
   ```

3. Save the file.
4. Restart the CA Service Catalog Windows Service.

(Optional) Form Cache

Form definitions are cached for better response time with use case like submitting a request and viewing a request. This configuration is ideal for production deployments as form definitions seldom change. However for deployments on development or test environments the form definitions change frequently, it becomes imperative to read the form definition every time instead of using the cache.

Perform the following steps to disable form definition cache:

1. Open the *USMHOME/view/conf/ehcache.xml* file.
2. Modify the Current Key with the New Key as shown next.
   Current Key:

   ```
    <cache name="system.form.cache" maxBytesLocalHeap="100M" eternal="false"
   overflowToDisk="false" timeToIdleSeconds="86400" timeToLiveSeconds="120000"/>
   ```

   New Key:

   ```
    <cache name="system.form.cache" maxBytesLocalHeap="100M" eternal="false"
   overflowToDisk="false" timeToIdleSeconds="2" timeToLiveSeconds="2"/>
   ```

3. Save the file.
4. Restart the CA Service Catalog Windows Service.

Post Installation Steps for Unified Self-Service

Perform the following optional post-installation steps for USS 14.1.02:

Prerequisites

Create a backup of the *US4SM\OSOP\portal-ext.properties* file.

Note: *US4SM* is the default Unified Self-Service installation directory.

Customize CA SDM Data Source Property

Perform the following steps to customize the CA SDM Data Source Property:

1. Open the *US4SM\OSOP\portal-ext.properties* file and copy the following content at the end of the file:

```
# SDM Datasource Config Fields
# Maximum number of the SDM Fields that can be shown in SDM Datasource config
Fields sections
# If no value/invalid value/ value less than 4 is specified, it will default to
10
sdm.configFields.maxFieldsToShowInConfigOptionsPage = 10
# If you want this property to be tenant specific, prefix the Web ID of the
tenant to the property. It is case-sensitive
# (Web Id can be obtained from the http(s)://server-name:<port-no>/group
/control panel > Portal Instances)
# Example Format:
# someCompany.com.sdm.configFields.maxFieldsToShowInConfigOptionsPage = 10
```

2. Save the file and restart (see page 1704) the services.

Enable or Disable the Community

Follow these steps:

1. Open *US4SM\OSOP\portal-ext.properties* and copy the following content at the end of the file:

```
# Community On/Off
# Community/Message board feature can be disabled by the setting property
disable.uss.community to true (case sensitive)
# Example - with Multi tenancy
# For a specific tenant, prefix the property with the tenant webID
# For tenants, if the value is not defined or the property is missing,Community
is enabled, by default.

# someCompany.com.disable.uss.community = true

# Example - All other tenant Community will be disabled if the value for the
property is true (case sensitive).
# If the value is not defined or the property is missing, Community is enabled,
by default.
```

```
# disable.uss.community = true
```

2. Save the file and restart (see page 1704) the services.

Enable Clickjacking Filter

Follow these steps:

1. Open the *US4SM\OSOP\tomcat-7.0.40\conf\web.xml* file.

2. Search for the text: *Built In Filter Definitions*
   The Built In Filter section appears as follows:
   <!-- ================== Built In Filter Definitions ==================== -->

   <filter>
   .
   .
   .
   </filter>

3. Add the following filter at the end of the *Built In Filter Definitions* section:

```
<!-- Filter :Restricts framing of USS application in all domains expect the
current domain in which USS is hosted -->
<filter>
<filter-name>ClickjackFilterSameOrigin</filter-name>
<filter-class>org.owasp.esapi.filters.ClickjackFilter</filter-class>
<init-param>
<param-name>mode</param-name>
<param-value>SAMEORIGIN</param-value>
</init-param>
</filter>
<filter-mapping>
<filter-name> ClickjackFilterSameOrigin </filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>
```

4. Save and close the file and restart (see page 1704) the services.

USS Announcements are Formatted Incorrectly for Windows

1. Navigate to the *US4SM\OSOP\tomcat-7.0.40\bin* folder and edit the file *wrapper.conf:*

   a. Modify the variable *wrapper.java.additional.20* value from *-Duser.timezone=GMT* to *-Duser.timezone=sdm-time-zone*
      For Example: '-Duser.timezone=America/Denver'. (Mountain Time)

   b. Save and close the file.

2. Navigate to *US4SM\OSOP* folder and *a*ppend the following content at the end of the *portal-ext.properties* file.

```
#set this to show the announcement date format in 24/12 hr
#format:
# dd-MMM-yy hh.mm.ss aa for 12 hr format
# dd-MMM-yy HH.mm.ss for 24 hr format
announcement.date.format=dd-MMM-yy hh.mm.ss aa
```

3. Save the file and restart (see page 1704) the services.

USS Announcements are Formatted Incorrectly for Linux

1. Navigate to the *US4SM\OSOP\tomcat-7.0.40\bin* folder and edit the file *setupenv.sh*

   a. Modify the variable *Duser.timezone* value from *-Duser.timezone=GMT* to *-Duser.timezone=sdm-time-zone*
   For Example: '-Duser.timezone=America/Denver'. (Mountain Time)

   b. Save and close the file.

2. Navigate to *US4SM\OSOP* folder and *a*ppend the following content at the end of the *portal-ext.properties* file.

```
#set this to show the announcement date format in 24/12 hr
#format:
# dd-MMM-yy hh.mm.ss aa for 12 hr format
# dd-MMM-yy HH.mm.ss for 24 hr format
announcement.date.format=dd-MMM-yy hh.mm.ss aa
```

3. Save the file and restart (see page 1704) the services.

For more information about USS enhancements, see CA Service Management Release 14.1.02 Enhancements (see page 69).

Uninstall CA Service Management 14.1.02

This article contains the following:

To uninstall CA Service Management 14.1.02, perform the following steps as per the product /products installed in your system:

Uninstall CA Service Desk Manager 14.1.02

To uninstall CA SDM 14.1.02, perform the following based on the type of operating system used by you:

Uninstall CA Service Desk Manager 14.1.02 (Windows)

Perform the following steps to uninstall the patch if you have installed CA SDM on Windows:

1. Log into CA SDM as an Administrator.
2. Shut down CA Service Desk Manager Server.
3. Navigate to the location *where you have extracted the CA Service Management Installer zip package*.
4. Locate *CASM_14.1.02_CommonPatchInstaller _Win\Installer\filestore\utils\ApplyPTF*.
5. Click **APPLYPTF**.
6. Select **Backout PTF** from the local or remote nodes option.
7. Click **Next**.
8. Enter the binary for language-independent patch or the language-dependent patch name. The following binary and language-dependent patches are supported:
   - Binary: **RO86155**
   - Language Master CAZ**: RO86157**
   - English:**RO86158**
   - French: **RO86161**
   - French Canadian: **RO86163**
   - German: **RO86159**
   - Italian:**RO86165**
   - Japanese: **RO86166**
   - Portuguese Brazil: **RO86164**
   - Simplified Chinese: **RO86167**
   - Spanish: **RO86160**
9. Leave all other options intact unless the node is incorrect
10. Click **Next** to uninstall CA SDM 14.1.02. Repeat steps **6-9** to remove the required language-dependent patch.
11. To restore MDB database, revert to database backup that you took before applying the patch. For more information, see Prerequisites (see page 686) .

12. To perform the post-backout steps, see Post-Backout Steps for CA Service Desk Manager 14.1.02 (see page 733).

Uninstall CA Service Desk Manager 14.1.02 (Linux)

Perform the following steps to uninstall the patch, if you have installed CA SDM 14.1.02 on Linux:

1. Log into CA SDM as root user.
2. Shut down the CA Service Desk Manager Server.
3. Navigate to the location where you have extracted the CA Service Management Installer tar.gz package.
4. Navigate to the *CASM_14.1.02_CommonPatchInstaller _Linux\Installer\filestore\utils\ApplyPTF* folder.
5. The following binary and language-dependent patches are supported:
   - Binary name: **RO86202**
   - Language Master: **RO86203**
   - English: **RO86204**
   - French: **RO86206**
   - German: **RO86205**
   - Japanese: **RO86207**
6. Execute the following command to remove the binaries or the language-dependent patches. Replace the <patch_name> with the binary or language-dependent patch name:

   ```
   ./applyptf.<platform> -b <patch_name>  -e <NX_ROOT>
   ```

   Here, <platform> specifies the operating system and <NX_ROOT> specifies the CA SDM installed location.

   For example:

   ```
   ./applyptf.linux -b RO86202 -e /opt/CA/ServiceDeskManager
   ```

7. To restore MDB database, revert to database backup that you took before applying the patch.
8. To perform the post-backout steps, see Post-Backout Steps for CA Service Desk Manager 14.1.02 (see page 733).

Uninstall CA Service Desk Manager 14.1.02 (Solaris)

Perform the following steps to uninstall if you have installed CA SDM 14.1.02 on Solaris:

1. Log into CA SDM as root user.
2. Shut down the CA Service Desk Manager Server.
3. Navigate to the location where you have extracted the CA Service Management Installer tar.gz package.
4. Navigate to the *CASM_14.1.02_CommonPatchInstaller _Solaris\Installer\filestore\utils\ApplyPTF* folder.
5. The following binary and language-dependent patches are supported:
   - Binary name: **RO86196**
   - Language Master: **RO86197**
   - English:**RO86198**
   - French: **RO86200**
   - German: **RO86199**
   - Japanese: **RO86201**
6. Execute the following command to remove the binaries or the language-dependent patches. Replace the <patch_name> with the binary or language-dependent patch name:

   ```
   ./applyptf.<platform> -b <patch_name> -e <NX_ROOT>
   ```

   Here, <platform> specifies the operating sytsem and <NX_ROOT> specifies the CA SDM installed location.
   For example:

   ```
   ./applyptf.sun -b RO86196 -e /opt/CA/ServiceDeskManager
   ```

7. To restore MDB database, revert to database backup that you took before applying the patch.
8. To perform post-backout steps, see Post-Backout Steps for CA Service Desk Manager 14.1.02 (see page 733).

Uninstall CA Service Desk Manager 14.1.02 (AIX)

Perform the following steps to uninstall if you have installed CA SDM 14.1.02 on AIX:

1. Log into CA SDM as root user.
2. Stop the CA Service Desk Manager Server.
3. Navigate to the location where you have extracted the CA Service Management Installer tar.gz package.
4. Navigate to the *CASM_14.1.02_CommonPatchInstaller _AIX\Installer\filestore\utils\ApplyPTF* folder.

5. The following binary and language-dependent patches are supported:

   - Binary name: **RO86216**
   - English: **RO86217**

6. Execute the following command to remove the binaries or the language-dependent patches. Replace the <patch_name> with the binary or language-dependent patch name:

   ```
   ./applyptf.<platform> -b <patch_name> -e <NX_ROOT>
   ```

   Here, <platform> specifies the operating sytsem and <NX_ROOT> specifies the CA SDM installed location.
   For example:

   ```
   ./applyptf.aix -b
   RO86216
    -e /opt/CA/ServiceDeskManager
   ```

7. To restore MDB database, revert to database backup that you took before applying the patch. For more information, see Prerequisites (see page 686).

8. To perform post-backout steps, see Post-Backout Steps for CA Service Desk Manager 14.1.02 (see page 733).

Uninstall CA Asset Portfolio Manager 14.1.02

You can uninstall CA Asset Portfolio Management components except CA MDB. CA MDB cannot be uninstalled. Perform the following steps:

1. From Windows **Start** menu, navigate to **Control Panel**, **Programs, Programs and Features, View Installed Updates** on the left pane.

2. Under CA Asset Portfolio Management, select **CA ITAM 14.1.02** .

3. Follow on-screen wizard instructions to uninstall.
   CA APM 14.1.02 is uninstalled.

4. If you have installed CA APM on multiple servers, follow steps **1-3** to uninstall.

5. To restore MDB database, revert to database backup that you took before applying the patch.

Uninstall Unified Self-Service 14.1.02

To uninstall Unified Self-Service, perform the following steps:

1. Log into USS as an Administrator.

2. Stop the USS Server and Jetty Server.

3. Navigate to the location *where you have extracted the CA Service Management Installer zip package.*

4. Locate *CASM_14.1.02_CommonPatchInstaller _Win\Installer\filestore\utils\ApplyPTF*.

5. Click **APPLYPTF-64bit.exe**.
6. Select the **Backout PTF** on local or remote nodes option.
7. Click **Next**.
8. Enter **RO86148** in the first field.
   Leave all other options intact unless the node is incorrect.
9. Click **Next** to uninstall USS 14.1.02.
10. To restore MDB database, revert to database backup that you took before applying the patch.
11. To perform post-backout steps, see Post-Backout Steps for Unified Self-Service 14.1.02 . (see page 736)

Uninstall Unified Self-Service 14.1.02 (Linux)

Perform the following steps to uninstall the patch, if you have installed USS 14.1.02 on Linux:

1. Log into USS as root.
2. Shut down the Unified Self-Service Server and Jetty Server.
3. Navigate to the location where you have extracted the USS Installer tar.gz package.
4. Navigate to the *CASM_14.1.02_CommonPatchInstaller _Linux\Installer\filestore\utils\ApplyPTF* folder.
5. The following binary and language-dependent patches are supported:
   - Binary name: **RO86149**
6. Execute the following command to remove the binaries or the language-dependent patches. Replace the <patch_name> with the binary or language-dependent patch name:

   ```
   ./applyptf.<platform> -b <patch_name>  -e <NX_ROOT>
   ```

   Here, <platform> specifies the operating system and <NX_Root> specifies the USS installed location.

   For example:

   ```
   ./applyptf.linux -b  RO86149 -e /opt/CA/Self Service
   ```

7. To restore MDB database, revert to database backup that you took before applying the patch.
8. To perform post-backout steps, see Post-Backout Steps for Unified Self-Service 14.1.02 . (see page 736)

Uninstall CA Service Catalog 14.1.02

To uninstall CA Service Catalog, perform the following steps:

1. Click **Control Panel**, **Programs and Features**.
2. Double-click the CA Service Catalog r14.1.02 and follow the uninstallation wizard instructions.

Post-Backout Steps for CA Service Desk Manager 14.1.02

Perform the following post-backout steps based on your server configuration:

Post-Backout Steps for CA SDM (Conventional)

Ensure that you are logged in as Administrator to uninstall CA SDM 14.1.02. Perform the following steps:

1. Navigate to the *NX_ROOT**site* folder from the command prompt window.
2. Run the following commands on primary and secondary servers.

   ```
   pdm_perl -pi.old -e "s/resources.created=1/resources.created=0/g" config.
   properties
   ```

3. To reconfigure the primary and secondary server run the following command:

   ```
   pdm_configure
   ```

Note: Do not select *Load Default Data*.

4. Start CA SDM services.

Post-Backout Steps (Advanced Availability)

For CA SDM Advanced Availability configuration, perform the following post-back steps on standby and application servers:

1. Stop CA SDM Services on all Advanced Availability servers.
2. Log on to the standby server that you will promote as the new background server:
3. Run the following command on the standby server:

   ```
   pdm_configure
   ```

4. Promote the standby server as the new background server by executing the following commands:

   a. To suppress version control on the standby and background servers, run the following command:

   ```
   pdm_server_control -v
   ```

   b. To promote the standby server as the new background server, run the following command:

   ```
   pdm_server_control -b
   ```

5. Run *pdm_configure* command on the new standby server.
6. Run *pdm_configure* command on all application servers.

Optional Steps for Specific Issues when Uninstalling CA Service Desk Manager 14.1.02 on 14.1 or 14.1.01

Optional steps below are required only if you installed them during the patch installation process as shown in Optional Steps for Specific Issues when Installing CA SDM 14.1.02 (see page 711).

This list is common when you uninstall CA SDM 14.1.02 on CA SDM 14.1 or CA SDM 14.1.01.

KT_DAEMON MAY TERMINATE WITH STRING TOO BIG ERROR (Prob# USRD 2113)

Execute the following command to uninstall the NX variable:

```
pdm_options_mgr -c -sALLOW_COMMENT_VIA_UPDATE_STATUS -v yes -a pdm_option.deinst
```

```
pdm_options_mgr -c -s ALLOW_COMMENT_VIA_UPDATE_STATUS -v yes -a pdm_option.deinst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

SORT FAILS IN DETAIL PAGE FOR ASCENTED CHARACTERS IN ORACLE (Prob# USRD 2971)

Execute the following command to uninstall the NX variable:

```
pdm_options_mgr -c -s ORCL_SORTING -v BINARY_CI -a pdm_option.deinst
```

```
pdm_options_mgr -c -s ORCL_SORTING -v BINARY_CI -a pdm_option.deinst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

EXPORTING MORE THAN 5000 CONFIGURATION ITEMS FAILS (Prob# USRD 2991)

Execute the following command to uninstall the NX variable:

```
pdm_options_mgr -c -s EXPORT_STATUS_TIMEOUT –v 1800 –a pdm_option.deinst
```

```
pdm_options_mgr -c -s EXPORT_STATUS_TIMEOUT -v 1800 -a pdm_option.deinst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

KD EMAIL NOTIFICATION SENT WITH HIGH URGENCY LEVEL (Prob# USRD 2992)

Execute the following command to uninstall the NX variable:

```
pdm_options_mgr -c -s KT_EMAIL_NOTIFY_LEVEL -v 1 -a pdm_option.deinst
```

```
pdm_options_mgr -c -s KT_EMAIL_NOTIFY_LEVEL -v 1 -a pdm_option.deinst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

SQL ERROR MAY OCCUR WHEN OPENING KNOWLEDGE DOCUMENT (Prob# USRD 3029)

Execute the following command to uninstall the NX variable:

```
pdm_options_mgr -c -s KD_TICKET_ACCURACY -v 300 -a pdm_option.deinst
```

```
pdm_options_mgr -c -s KD_TICKET_ACCURACY -v 300 -a pdm_option.deinst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

ALLOW STRICT SURVEYS TO BE SENT TO MULTIPLE TICKETS (Prob# USRD 3055)

Execute the following command to uninstall the NX variable:

```
pdm_options_mgr -c -s ALLOW_STRICT_SURVEY_FOR_MULTIPLE_TICKETS -v Yes -a pdm_option.
deinst
```

```
pdm_options_mgr -c -s ALLOW_STRICT_SURVEY_FOR_MULTIPLE_TICKETS -v Yes -a pdm_option.
deinst –t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

REPORTED BY FIELD NOT FOCUSABLE (Prob# USRD 3067)

Execute the following command to uninstall the NX variable:

```
pdm_options_mgr -c -s FOCUS_REPORTED_BY -v <XXX> -a pdm_option.deinst
```

```
pdm_options_mgr -c -s FOCUS_REPORTED_BY -v <XXX> -a pdm_option.deinst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

Optional Steps for Specific Issues when Uninstalling CA Service Desk Manager 14.1.02 only on 14.1

TWO WORKFLOW TASKS STATUS MAY SHOW PENDING (Prob# USRD 3200)

Execute the following command to uninstall the NX variable:

```
pdm_options_mgr -c -s INSERT_WF_PREVIOUS -v Yes -a pdm_option.deinst
```

```
pdm_options_mgr -c -s INSERT_WF_PREVIOUS -v Yes -a pdm_option.deinst -t
```

For each secondary CA SDM server that you configured manually, add or update the NX variable in each secondary CA SDM server in the NX.env file located in the *NX_ROOT* directory and restart the server.

UNEXPECTED BEHAVIOUR ON CLICKING CAB CONSOLE B (Prob# USRD 3258)

Follow these steps:

1. From the command line, execute the following commands from the $NX_ROOT\data folder:

   ```
   pdm_load -u -f USRD_2789_backup_macro.dat
    pdm_load -u -f USRD_2789_backup_param.dat
   ```

2. Clear the cache, by executing the following commands:

   ```
   pdm_cache_refresh -t usp_pdmMacro
    pdm_cache_refresh -t usp_pdmMacroParam
   ```

Post-Backout Steps for Unified Self-Service 14.1.02

Post-Backout Steps for Unified Self-Service 14.1.02 (Windows)

Ensure that you have administrator privileges to uninstall USS 14.1.02. Perform the following post-backout steps:

1. Stop USS Services.

2. Execute the following command:

   ```
   APPLYPTF-64 bit
   ```

3. Select ***Backout PTF*** on local or remote nodes.
4. Click **Next**.
5. Enter the fix number in the first field.
6. Leave all other options intact.
7. Click **Next** to uinstall.
8. Start USS services.

Post-Backout Steps for Unified Self-Service 14.1.02 (Linux)

Ensure that you have root user privileges. Perform the following steps:

1. Stop USS Services.
2. Run the following command to uninstall the patch:

   ```
   applyptf -b T51R166 -e $US4SM
   ```

   Note: *US4SM* is the default Unified Self-Service install directory.

3. Start USS services.

(Optional) Upgrade Apache Tomcat

To upgrade Apache Tomcat for Unified Self-Service, perform the following steps:

- (Optional) Upgrade Apache Tomcat to 7.0.59 for Unified Self-Service (Linux) (see page 737)
- (Optional) Upgrade Apache Tomcat to 7.0.59 for Unified Self-Service (Windows) (see page 740)

(Optional) Upgrade Apache Tomcat to 7.0.59 for Unified Self-Service (Linux)

Unified Self-Service (USS) provides out-of-the box Apache Tomcat 7.0.40. You can upgrade to Apache Tomcat 7.0.59 (Linux) by performing the following steps:

1. Stop USS services.
2. Navigate to *$US4SM/OSOP*.

   a. Create a backup of the *tomcat-7.0.40* folder.

b. Rename folder *tomcat-7.0.40* to *tomcat-7.0.40_original*

c. Create an empty folder *tomcat-7.0.40* at *$US4SM\OSOP*

> **Note:** *$US4SM* is the default Open Space installation directory.

3. Click here (http://archive.apache.org/dist/tomcat/tomcat-7/v7.0.59/bin/apache-tomcat-7.0.59.zip) and download the Apache Tomcat 7.0.59 version:

   a. Unzip the *apache-tomcat-7.0.59.zip* file.

   b. Copy the content of *apache-tomcat-7.0.59* folder to *$US4SM/OSOP/tomcat-7.0.40* folder and provide the permissions and access rights of *tomcat-7.0.40_original* to *tomcat-7.0.40*.
   The folder tomcat-7.0.40 contains the following files and folders:

   - bin
   - jre
   - LICENSE
   - NOTICE
   - RUNNING.txt
   - webapps
   - conf
   - lib
   - logs
   - RELEASE-NOTES
   - temp
   - work

4. Copy the following files to the *$US4SM/OSOP/tomcat-7.0.40* folder:

   - *$US4SM/OSOP/tomcat-7.0.40_original/bin/setenv.bat*
   - *$US4SM/OSOP/tomcat-7.0.40_original/bin/setenv.sh.backup*
   - *$US4SM/OSOP/tomcat-7.0.40_original/bin/setenv.sh*

5. Copy the *$US4SM/OSOP/tomcat-7.0.40_original/conf/Catalina* folder to *$US4SM/OSOP /tomcat-7.0.40/conf*

6. Open the *$US4SM/OSOP/tomcat-7.0.40/conf/catalina.properties* file and replace:

   common.loader=${catalina.base}/lib,${catalina.base}/lib/.jar,${catalina.home}/lib,${catalina. home}/lib/*.jar*

   with

   common.loader=${catalina.base}/lib,${catalina.base}/lib/.jar,${catalina.home}/lib,${catalina. home}/lib/*.jar,${catalina.home}/lib/ext,${catalina.home}/lib/ext/*.jar*

7. Save and close the file.

8. Navigate to *$US4SM/OSOP/tomcat-7.0.40_original/conf* folder and copy the *server.xml* and overwrite the file existing in *$US4SM/OSOP/tomcat-7.0.40/conf/* .

9. Navigate to *$US4SM /OSOP/tomcat-7.0.40_original/* and copy the *jre* folder to *$US4SM/OSOP /tomcat-7.0.40*

10. Copy the files and folder from *$US4SM/OSOP/tomcat-7.0.40_original/lib/ext* to *$US4SM /OSOP/tomcat-7.0.40/lib* folder:

11. Delete the following folders in *$US4SM/OSOP/tomcat-7.0.40/webapps:*

    - docs
    - example
    - host-manager
    - manager
    - ROOT

12. Copy the *$US4SM/OSOP/tomcat-7.0.40_original/webapps* folder to *$US4SM/OSOP/tomcat-7.0.40*

13. Copy the *$US4SM/OSOP/tomcat-7.0.40_original/.donotdelete* folder to *$US4SM/OSOP /tomcat-7.0.40*

14. Delete content from the following folders:

    - *$US4SM /OSOP/tomcat-7.0.40/temp*
    - *$US4SM /OSOP/tomcat-7.0.40/work*

15. Start the USS services.

(Optional) Upgrade Apache Tomcat to 7.0.59 for Unified Self-Service (Windows)

Unified Self-Service (USS) provides out-of-the box Apache Tomcat 7.0.40. To upgrade to Apache Tomcat 7.0.59 on Windows, perform the following steps:

1. Stop USS services.
2. Navigate to the *$US4SM\OSOP* folder or the location where you have installed USS.
    a. Create a backup of the *tomcat-7.0.40* folder.
    b. Rename *$US4SM\OSOP\tomcat-7.0.40* to *$US4SM\OSOP\tomcat-7.0.40_original*
    c. Create an empty folder for tomcat-7.0.40 at *$US4SM\OSOP*

    > **Note:** *$US4SM* is the default Open Space installation directory.

3. Click here (http://archive.apache.org/dist/tomcat/tomcat-7/v7.0.59/bin/apache-tomcat-7.0.59.zip) to download Apache Tomcat 7.0.59.
    a. Unzip the downloaded file.
    b. Copy the content of *apache-tomcat-7.0.59* folder to *$US4SM\OSOP\tomcat-7.0.40*
    The folder tomcat-7.0.40 contains the following files and folders:

- bin
- conf
- lib
- logs
- temp
- webapps
- work
- LICENSE
- NOTICE
- RELEASE-NOTES
- RUNNING

4. Navigate to *$US4SM\OSOP\tomcat-7.0.40_original\bin* and copy the following files to *$US4SM\OSOP\tomcat-7.0.40:*
   - InstallTomcat-NT.bat
   - setenv.bat
   - setenv.bat.backup
   - setenv.sh
   - StartTomcat-NT.bat
   - StopTomcat-NT.bat
   - Tomcat.bat
   - UninstallTomcat.bat
   - wrapper.conf
   - wrapper.conf.backup
   - wrapper.exe
   - wrapper-license-app.conf
5. Navigate to *$US4SM\OSOP\tomcat-7.0.40_original\conf\,* copy and replace the *Catalina* folder in *C:\Program Files\CA\Self Service\OSOP\tomcat-7.0.40\conf\Catalina*
6. Navigate to *$US4SM\OSOP\tomcat-7.0.40\conf* and edit the *catalina.properties* file and and replace the following line:
   common.loader=${catalina.base}/lib,${catalina.base}/lib/.jar,${catalina.home}/lib,${catalina.home}/lib/*.jar*
   with
   common.loader=${catalina.base}/lib,${catalina.base}/lib/.jar,${catalina.home}/lib,${catalina.home}/lib/*.jar,${catalina.home}/lib/ext,${catalina.home}/lib/ext/*.jar*
7. Save and close the file.
8. Navigate to *$US4SM\OSOP\tomcat-7.0.40_original\conf* and copy the *server.xml* file and replace with the *server.xml* file in *$US4SM\OSOP\tomcat-7.0.40\conf*
9. Navigate to *$US4SM\OSOP\tomcat-7.0.40_original\ folder* and copy the *jre* folder to *$US4SM \OSOP\tomcat-7.0.40*
10. Navigate to *$US4SM\OSOP\tomcat-7.0.40_original\lib* and copy the following files and folder to *$US4SM\OSOP\tomcat-7.0.40\lib:*
    - ext
    - wrapper.dll

- wrapper.jar

11. Navigate to *$US4SM\OSOP\tomcat-7.0.40\webapps* folder and delete the following folders from*:*
    - docs
    - example
    - host-manager
    - manager
12. Navigate to *$US4SM\OSOP\tomcat-7.0.40_original* and copy the *webapps* folder to *$US4SM \OSOP\tomcat-7.0.40*
13. Navigate to *$US4SM\OSOP\tomcat-7.0.40_original\ folder* and copy *.donotdelete* folder to *$US4SM\OSOP\tomcat-7.0.40*
14. Navigate to *$US4SM\OSOP\tomcat-7.0.40* and delete the content in the following folders:
    - temp
    - work
15. Start USS services.

Run SMPatchReport Utility to Get Installed Patches List

The SMPatchReport Utility automatically identifies and lists the CA Service Management product patches (CA SDM, CA APM, CA Service Catalog, and USS) that are installed on your local system. It provides you the option of generating a PDF or emailing the patch report summary. To email the patch report summary, you must configure the SMTP mail server properties. For more information, see Set the SMTP Server Configuration Properties (see page) .

Note: If you have multiple systems in your environment with different versions of CA Service Management product patches installed, you must run this utility on each system individually to generate the patch report summary.

Prerequisites

1. Setting 32-bit Java is mandatory for Windows and Non-Windows
2. For Windows, you must set the path variable under Environment Variables.
3. For Non-Windows, export Java path till bin/java/ in JAVA_HOME.

Run SMPatchReport Utility (Windows)

1. Navigate to *common patch installer/filestore/SMPatchReport* location on your local system.

2. Double-Click **Report.exe** to run the utility.
   The utility identifies and lists all the CA Service Management product patches that are installed in the system.

3. Select **PDF** or **E-Mail** options to generate a PDF or email the patch report summary respectively.

> **Note:** To view the generated PDF, ensure that you have a PDF reader installed in your system. For example, Adobe Acrobat Reader.

Run SMPatchReport Utility (Non_Windows)

1. Change directory to *common patch installer/filestore/SMPatchReport* location on your local system.

2. Execute **Report.sh** to run the utility.

   The utility identifies and lists all the CA Service Management product patches that are installed in the system.

3. Select **PDF** or **E-Mail** options to generate a PDF or email the patch report summary respectively.

> **Note:** To view the generated PDF, ensure that you have a PDF reader installed in your system. For example, Adobe Acrobat Reader.

Set the report.config.property File

The report.config.property file is located under *common patch installer/filestore/SMPatchReport*. Set the following properties to configure smtp mail server and other properties:

- **smtp.mail.to**: Specifies the email address to which email notifications are sent. In case of multiple email addresses, separate the values using a comma (,).

- **smtp.mail.from**: Specifies the email address from which email notifications are sent.

- **smtp.mail.authenticate**: Authenticates the user with SMTP server.
  The default value is **false**, which allows you to send email without authentication. If the value is set to **true**, the system attempts to authenticate the user. In this case, *smtp.mail.username* and *smtp.mail.password* must be set.

- **smtp.mail.username**: Specifies the user name of the account that connects to the SMTP server.
- **smtp.mail.password**: Specifies the password for the user name used in the *smtp.mail.username* property. The password must be encrypted. For more information on encrypting a password in the report.config.properties file, see Encrypt Password (see page 744) .
- **smtp.mail.host**: Specifies the host name of the SMTP server to connect to or the IP address of the server to which the email is sent.
- **smtp.mail.port**: Specifies the port number on which the SMTP service runs. This property value defaults to TCP port number 25, which is reserved for SMTP. Email administrators can change this value.
- **report.log.path**: Specifies the location where the SMPatchReport log is created. By default, it is created in your current directory.

Encrypt a Password

To encrypt password*,* set the value for *smtp.mail.password* property in the report.config,properties file. Perform the following steps to encrypt a password :

1. Open the Command Prompt window.
2. Change your working directory to SMPatchReport.
3. Ensure that 32-bit java is available on the system.
4. (Windows) Execute the following command to encrypt the password:

   ```
   java -cp ./lib/SMPatchReport.jar;./lib/sd-utils.jar;./lib/jsafeFIPS.jar;./lib
   /log4j-1.2.15.jar;. com.ca.patch.Util.StringEncrypter encrypt TextToEncrypt
   ```

5. (Non-Windows) Execute the following command to encrypt the password:

   ```
   Java -cp ./lib/sd-utils.jar:./lib//SMPatchReport.jar:./lib/jsafeFIPS.jar:./lib
   /log4j-1.2.15.jar:. com.ca.patch.Util.StringEncrypter encrypt TextToEncrypt
   ```

6. The Encrypted password is displayed on the console. Copy the password from the console and set the value in the *smtp.mail.password* property.

Troubleshooting the Installation Process

Issue: CA SDM Database Patch Fails

Sometimes, ApplyPTF fails to apply the CA Service Management 14.1.02 patch as some files are used by another process. As a result, the *Cum2* folder is not created under the *CASDM/Patches* folder.

Resolution:

Exit and launch the installer again.

Deploying Oracle RAC with CA Service Management

This section describes how to deploy the CA Service Management Products (CA Service Desk Manager, CA Service Catalog, CA IT Asset Manager, and Unified Self-Service) with Oracle Real Application Clusters (RAC). You can deploy one or combination of these products as required. Oracle RAC provide high availability to applications by removing the single server as a single point of failure.

Oracle Real Application Clusters (RAC) Install Requirements

Note: For more information about installing Oracle RAC, see Oracle documentation.

Ensure to verify and complete the following Oracle RAC installation prerequisites:

- Download Oracle Database 11g Release 2 (11.2.0.3.0 and above) (Oracle Grid infrastructure and database) software from Oracle (http://www.oracle.com/technetwork/database/enterprise-edition/downloads/112010-win64soft-094461.html) Downloads. Create the Oracle database (SID).
- The Single Client Access Name (SCAN) must be defined in the Domain Name Service (DNS) or Oracle Grid Naming Service (GNS).
- Create at least one single DNS or GNS name that resolves to three IP addresses using a round-robin algorithm. For the installation to succeed, the SCAN must resolve to at least one IP address.
- SCAN Virtual IP (VIP) addresses must be on the same subnet as the virtual IP addresses and public IP addresses.
- The virtual machines can be limited to 2 GB of swap but results in a prerequisite install check failure. The best practice define a 3+ GB of swap.
- Ensure that you have the 64-bit version of Windows Server and Oracle 11g Release 2.
- Install the Oracle Grid Infrastructure following the Oracle Documentation installation procedures.

How to Install Oracle RAC With CA Service Management

To install Oracle RAC with CA Service Management (CA Service Desk Manager, CA Service Catalog, CA IT Asset Manager, and/or Unified Self-Service), complete the following steps:

Follow these steps:

1. Install Oracle 11gr2 32-bit client software on system or systems where you plan to install the CA Service Management products.

2. Create a TNS entry on the system or systems.

3. Enable the client-side connect-time failover by setting FAILOVER=ON in the corresponding client-side TNS entry:

```
TESTRAC =
(DESCRIPTION =
(ADDRESS_LIST=
(FAILOVER = ON)
(ADDRESS = (PROTOCOL = TCP)(HOST = <scan_host_name>)(PORT
= <1521>))
)(CONNECT_DATA = (SERVICE_NAME = <netservice name>))
```

Install the CA Service Management Products with Oracle RAC

For Installing the CA Service Management Product or products with Oracle RAC, perform the following steps:

Follow these steps:

1. Launch the CA Service Management installer.
   For more information, see Install CA Service Management. (see page 296)

2. Select **CA Service Management** from Select the Required Installer screen.

3. Review and accept the license agreement information.

4. Select **Oracle** as the database type in the Database Configuration Screen and enter the following Oracle database details

   a. **Database Server**: Enter the Oracle database host name <SCAN_HOST_NAME>.

   b. **Tablespace Path (on DB Server)**: Enter +DATA.
      Complete all fields on the Oracle Database Configuration Screen. For more information, see Install CA Service Management (see page 296).

5. Select the required CA Service Management product or products.

6. Follow the on-screen instructions on the installer wizard and complete the CA Service Management installation.
   For more information about Oracle RAC Failover issue with CA Service Catalog, see Release Notes (see page 210).
   For more information about Oracle RAC Failover issue with CA SDM, see Release Notes (see page 184).
   For more information about Oracle RAC Failover issue with CA ITAM, see Release Notes (see page 257).

How to Move the CA MDB Data from the Source to the Target Systems

You can move the CA MDB database from the source system and configure it to work on the target system.

Important! We recommend that you test the procedure in a test environment before implementing on a production system. Currently, moving the CA MDB data is not supported for clustered database, load balancer, and application cluster.

Prerequisites

Before you move the CA MDB data, perform the following tasks:

1. Back up the CA MDB database on your target system.
2. Install the following products on the source and target systems:
   - CA Service Desk Manager 14.1 and above
   - CA Service Catalog 14.1 and above
   - CA Asset Portfolio Manager 14.1 and above
   - Unified Self-Service 14.1 and above
3. Ensure that the source and target systems have an identical installation configuration setup.

CA Service Management Tables

Affected CA Service Management Tables

The following tables are impacted when you move the CA MDB database on Microsoft SQL Server or Oracle:

Common Tables	CA SDM	CA Service Catalog	CA APM	CA Unified Self-Service Tables
	ci_mdr_provider	usm_configuration	al_meta_refresh_state	os_ExternalSource

Common Tables	CA SDM	CA Service Catalog	CA APM	CA Unified Self-Service Tables
al_cdb_comp_installstate_bkup			**Note:** This table is applicable only for CA Service Management 14.1.01 installation.	
al_cdb_componentinstallstate	options		al_meta_binary_store	os_ExternalSourcePropertiesUser_
al_cdb_config_params_bkup	sapolicy		al_process_account	PortalPreferences
al_cdb_configurationparameters	usp_servers object_promotion promo_hist **Note:** These tables are displayed only if CA Service Management 14.1.02 is installed in your environment.		al_apmp_def al_apmp_operation al_apmp_content_types al_apmp_progress_status al_apmp_progress al_apmp_record_filter al_apmp_run_stage	
al_cdb_files	usp_domsrvr		**Note:** These tables are displayed only if CA Service Management 14.1.02 patch is installed in your environment.	
ca_application_registration	usp_configuration usp_webeng-domsrvr usp_webengine usp_webengine_alias usp_domsrvr			

Move the CA MDB Database on Microsoft SQL Server

If you have installed Microsoft SQL Server database in your system, perform the following steps:

1. Review CA Service Management Tables (see page 747) to verify the tables that are impacted when you move the CA MDB database on Microsoft SQL Server.

2. Stop the following CA Service Management services on both the source and target application servers:

   Note: Some of these services might not be applicable if the associated products or components are not installed in your environment.

   a. **Common Admin Service**:

      - CA Service Management Admin

   b. **CA SDM**:

      Note: If you have any shared UNC paths, ensure that you copy the paths from the source system to the target system.

      - CA Service Desk Manager ODBC Data Access
      - CA Service Desk Manager ODBC Agent
      - CA Service Desk Manager Server

   c. **CA Service Catalog Services**:

      - CA Service Accounting
      - CA Service Catalog

   d. **CA Asset Portfolio Management Services**:

      - IIS Admin Service
      - CA Asset Portfolio Management - Data Importer Engine
      - CA Asset Portfolio Management - Event Service
      - CA Asset Portfolio Management - Export Service
      - CA Asset Portfolio Management - HW Reconciliation Engine
      - CA Asset Portfolio Management - LDAP Import Service
      - CA Asset Portfolio Management - Registration Service

- CA SM Server

e. **Unified Self-Service Services**:

- CA Unified Self-Service Jetty Server
- CA Unified Self-Service Server

3. On the source system, back up the **mdb** and **uss_mdb** database, and copy the mdb back up files to the target system.
4. (Optional) If you are using a named instance (non-default MDB name), ensure that you have selected the appropriate MDB instance name for the backup.
5. On the target system, perform the following steps to back up the tables:

   a. Navigate to Microsoft SQL Management Studio, right-click **MDB** (or the appropriate MDB instance name applicable for your system), and select **Tasks**, **Generate Scripts**.

   b. Click **Select Specif ic database obj ects**.

   c. Select the **Tables** option and choose the appropriate tables.

   d. Click **Next**.

   e. Select **Advanced** and navigate to **Types of Data**.

   f. Change it from **Schema Only** to **Schema and Data**, and click **OK**.

      By default, your selection is now saved to a file **%user%\documents\script.sql**.

   g. Specify different file names for MDB and USS_MDB.

   h. Perform steps **a-f** for uss_mdb.

      Two script files are generated.

6. On the target system, perform the following steps to detach the existing *mdb and uss_mdb:*

   a. Navigate to Microsoft SQL Management Studio, right-click **MDB** (or appropriate MDB name), **Tasks**, **Detach**.

   b. On the Detach Database screen, select **Drop Connections**.

   c. Click **OK**.

7. Restore *mdb and uss_mdb* backup on the target system that was copied from the source system. Select **Overwrite the existing database** (WITH REPLACE) from the **Options** tab. Ensure that the database name on the target system is retained.

Note: Restore must complete without errors.

8. Run the following Microsoft SQL *auto_fix_user* script for user mdbadmin and ussdbadmin users:

   - sp_change_users_login 'AUTO_FIX','mdbadmin'
   - sp_change_users_login 'AUTO_FIX', 'apmdba' (Applicable only if CA APM is installed and upgraded from previous release versions)
   - sp_change_users_login 'AUTO_FIX', 'uapmadmin' (Applicable only if CA APM is installed and upgraded from previous release versions)
   - sp_change_users_login 'AUTO_FIX', 'uapmbatch' (Applicable only if CA APM is installed and upgraded from previous release versions)
   - sp_change_users_login 'AUTO_FIX', 'uapmreporting' (Applicable only if CA APM is installed and upgraded from previous release versions)
   - sp_change_users_login 'AUTO_FIX', 'usmadmin' (Applicable only if CA Service Catalog is installed and upgraded from previous release versions)
   - sp_change_users_login 'AUTO_FIX', 'ServiceDesk' (Applicable only if CA SDM is installed and upgraded from previous release versions)
   - sp_change_users_login 'AUTO_FIX','ussdbadmin' (Applicable only for USS)

9. Verify that the mdbadmin and ussdbadmin users are now mapped to **mdb**/**uss_mdb** and have the **bulkadmin**, **public** roles.

10. On the target system, delete data from the following tables and commit the changes:

    a. Use **mdb** and run the following queries to delete data from the required tables:

       Common Tables:

       - delete from al_cdb_comp_installstate_bkup
       - delete from al_cdb_componentinstallstate
       - delete from al_cdb_config_params_backup
       - delete from al_cdb_configurationparameters
       - delete from al_cdb_files
       - delete from ca_application_registration

       CA SDM Tables :

       - delete from options
       - delete from usp_servers

- delete from sapolicy
- delete from ci_mdr_provider
- delete from usp_domsrvr
- delete from usp_configuration
- delete from usp_webeng_alias
- delete from usp_webeng_domsrvr
- delete from usp_webengine
- delete from object_promotion (applicable only if CA Service Management 14.1.02 is installed)
- delete from promo_hist (applicable only if CA Service Management 14.1.02 is installed)

CA Service Catalog tables:

- delete from usm_configuration

CA APM tables:

- delete from al_meta_binary_store
- delete from al_process_account

Delete the following CA APM tables, if you have CA Service Management 14.1.02 installed in your system:

- delete from al_apmp_def
- delete from al_apmp_operation
- delete from al_apmp_content_types
- delete from al_apmp_progress_status
- delete from al_apmp_record_filter
- delete from al_apmp_run_stage

b. Select **USS_mdb** and run the following queries to delete data from the required tables:

- delete from PortalPreferences
- delete from os_ExternalSource
- delete from os_ExternalSourceProperties

- delete from User_

11. Execute the **script.sql** scripts that was created in **Step 5**.

> **Note:** Ignore the warning message, There is already an object named ... in the Database.

12. (Optional) To disable email notifications, modify the ca contact table query: **Update ca_contact set email_address = ''**.

> **Note:** If USS is installed, disabling the email notifications may cause missing announcements in the target system. We recommend that you add the email addresses for required contacts before performing **Step 13**.

13. Start the services on both the source and the target systems and on the target system, perform the following steps for each product:

    a. **Common Admin Service**:
    CA Service Management Admin

    b. **CA SDM Services**:
    Perform the following steps before you start the CA SDM services:

        i. If your environment has customized CA PAM content, export all the relevant CA PAM Content from the source CA PAM server and import to the target CA PAM server. Complete the required CA PAM content configuration.
        For more information, see CA Process Automation (see page 292) .

        ii. Copy the **site/mods** directory from the source CA SDM server to the target CA SDM server.

> **Note:** This is applicable only if your application environment is customized. This is not applicable for the out-of-the-box (OOTB) content.

        iii. Run the ***pdm_configure*** command without selecting the load default data option.

        iv. Start the following CA SDM services:

- CA Service Desk Manager ODBC Data Access
- CA Service Desk Manager ODBC Agent

- CA Service Desk Manager Server

c. **CA Service Catalog Services**:
Perform the following steps before you start the CA Service Catalog services:

- If your source system has customized CA PAM content, export all relevant PAM content from the source CA PAM server and import to the target CA PAM server. Complete the required configurations for CA PAM content.
For more information, see CA Process Automation . (see page 292)

- If your source system has customized CA EEM policies, export all the relevant CA EEM policies from the source CA EEM server and import to the target CA EEM server.
For more information, see CA Embedded Entitlements Manager . (see page 283)

- Copy filestore directory from the source CA Service Catalog server to the target CA Service Catalog server.

  Note: This is applicable only if customization is carried out on the application environment. This is not applicable for the OOTB content.

- Launch the CA PAM server and access **SLCM_Globaldataset**. and validate that the domain and the CA Service Catalog root business unit names are same.

- Start the following CA Service Catalog services:

  - CA Service Accounting

  - CA Service Catalog

d. **CA Asset Portfolio Management Services**:

- IIS Admin Service

- CA Asset Portfolio Management - Data Importer Engine

- CA Asset Portfolio Management - Event Service

- CA Asset Portfolio Management - Export Service

- CA Asset Portfolio Management - HW Reconciliation Engine

- CA Asset Portfolio Management - LDAP Import Service

- CA Asset Portfolio Management - Registration Service

- CA SM Server

e. **Unified Self-Service Services**:

- CA Unified Self-Service Jetty Server
- CA Unified Self-Service Server

14. Execute the **pdm_k_reindex** command on the CA SDM target system to index knowledge documents that are created and copied from the source system.
15. Verify that CA Service Management applications are accessible. All applications must be up and running.
16. Validate that all CA Service Management Integration scenarios are working seamlessly.

Move the CA MDB Database on Oracle

Perform the following steps to copy and restore CA MDB if you have installed Oracle database in your system:

1. Review CA Service Management Tables (see page 747) to verify the tables that are impacted when you move the CA MDB database on Oracle.
2. Stop the following CA Service Management services on both the source and target application servers.

Note: Some of these services might not be applicable if the associated products or components are not installed in your environment.

a. **Common AdminService**:

- CA Service Management Admin

b. **CA SDMServices**:

Note: If you have any shared UNC paths, ensure that you copy the paths from the source system to the target system.

- CA Service Desk Manager ODBC Data Access
- CA Service Desk Manager ODBC Agent
- CA Service Desk Manager Server

c. **CA Service Catalog Services**:

- CA Service Accounting

- CA Service Catalog

d. **CA Asset Portfolio Management Services**:

- IIS Admin Service
- CA Asset Portfolio Management - Data Importer Engine
- CA Asset Portfolio Management - Event Service
- CA Asset Portfolio Management - Export Service
- CA Asset Portfolio Management - HW Reconciliation Engine
- CA Asset Portfolio Management - LDAP Import Service
- CA Asset Portfolio Management - Registration Service
- CA SM Server

e. **Unified Self-ServiceServices**:

- CA Unified Self-Service Jetty Server
- CA Unified Self-Service Server

3. On the source system, navigate to *C:\app\Administrator\product\11.2.0\dbhome_1\BIN* path to export the database. To Create and grant permissions to the directory, execute the following commands:

```
CREATE OR REPLACE DIRECTORY test_dir AS 'C:\app\Administrator';
GRANT READ, WRITE ON DIRECTORY test_dir TO mdbadmin;
GRANT READ, WRITE ON DIRECTORY test_dir TO ussdbadmin;
```

Note: Ensure that you use the appropriate MDB instance name applicable for your system.

```
expdp mdbadmin/N0tallowed@mdb directory=test_dir dumpfile=mdb.dmp
logfile=expdbmdb.log
```

Note: Ensure that you use the appropriate uss_mdb instance name applicable for your system.

```
expdp ussdbadmin/N0tallowed@uss_mdb directory=test_dir dumpfile=ussmdb.dmp
logfile=expdbussmdb.log
```

4. Copy the **mdb.dmp** and **ussmdb.dmp** files to *C:\app\Administrator* on the target system.
   On target system, take a backup of mdb first and then, take a backup of the required tables.
   To create and grant permissions to the directory, execute the following commands for mdb and uss_mdb:

   ```
   CREATE OR REPLACE DIRECTORY test_dir AS 'C:\app\Administrator';
   GRANT READ, WRITE ON DIRECTORY test_dir TO mdbadmin;
   GRANT READ, WRITE ON DIRECTORY test_dir TO ussdbadmin;
   ```

   Note: Ensure that you use the appropriate MDB instance name.

   ```
   expdp mdbadmin/N0tallowed@mdb directory=test_dir dumpfile=mdb.dmp
   logfile=expdbmdb.log
   ```

   Note: Ensure that you use the appropriate USS MDB instance name.

   ```
   expdp ussdbadmin/N0tallowed@uss_mdb directory=test_dir dumpfile=ussmdb.dmp
   logfile=expdbussmdb.log
   ```

5. If CA Service Management 14.1.02 is installed in your system, the additional tables listed here for CA SDM and CA APM also must be included in the following query:

   - **CA SDM**: object_promotion, promo hist
   - **CA APM**: al_apmp_def, al_apmp_operation, al_apmp_content_types, al_apmp_progress_status, al_apmp_progress, al_apmp_record_filter, l_apmp_run_stage

     ```
     expdp mdbadmin/N0tallowed@mdb tables=al_cdb_comp_installstate_bkup,
     al_cdb_componentinstallstate,
     al_cdb_config_params_backup,
     al_cdb_configurationparameters,
     al_cdb_files,
     ca_application_registration,
     options,
     usp_servers,
     sapolicy,
     ci_mdr_provider,
     usp_domsrvr,
     usp_configuration,
     usp_webeng_domsrvr,
     usp_webengine,
     usp_webeng_alias,
     usm_configuration,
     al_meta_refresh_state,
     al_meta_binary_store,
     al_process_account grants=y indexes=y rows=y constraints=y triggers=y
     directory=test_dir dumpfile=expdptables.dmp logfile=expdbtables.log
     ```

6. Execute the following command for uss_mdb:

   ```
   expdp system/N0tallowed@uss_mdb tables=os_ExternalSource,
   os_ExternalSourceProperties,
   PortalPreferences, User_ grants=y indexes=y rows=y constraints=y triggers=y
   directory=test_dir dumpfile=expdpusstables.dmp logfile=expdbusstables.log
   ```

7. Import the backup database copied from the source system. Execute the following commands:

   Note: Ensure that you use the appropriate MDB instance name applicable for your system.

   ```
   impdp mdbadmin/N0tallowed@mdb directory=test_dir dumpfile=mdb.dmp
   logfile=impdbmdb.log TABLE_EXISTS_ACTION = TRUNCATE
   ```

   Note: Ensure that you use the appropriate USS MDB instance name.

   ```
   impdp ussdbadmin/N0tallowed@uss_mdb directory=test_dir dumpfile=ussmdb.dmp
   logfile=impdbussmdb.log TABLE_EXISTS_ACTION = TRUNCATE
   ```

8. Drop the tables after import by executing the following commands. Dropping the tables removes the table definitions and rows.

   - **Common Tables**:

     ```
     DROP TABLE al_cdb_comp_installstate_bkup;
     DROP TABLE al_cdb_componentinstallstate;
     DROP TABLE al_cdb_config_params_backup;
     DROP TABLE al_cdb_configurationparameters;
     DROP TABLE al_cdb_files;
     DROP TABLE ca_application_registration;
     ```

   - **CA SDM**:

     ```
     DROP TABLE ci_mdr_provider;
     DROP TABLE options;
     DROP TABLE usp_servers;
     DROP TABLE sapolicy;
     DROP TABLE usp_domsrvr;
     DROP TABLE usp_configuration;
     DROP TABLE usp_webeng_alias;
     DROP TABLE usp_webeng_domsrvr;
     DROP TABLE usp_webengine;
     ```

     If you have installed CA SDM 14.1.02, execute the following commands to drop tables:

     ```
     DROP TABLE object_promotion;
     DROP TABLE promo_hist;
     ```

     CA Service Catalog:

     ```
     DROP TABLE usm_configuration;
     ```

     CA APM:

     ```
     DROP TABLE al_meta_binary_store;
     DROP TABLE al_process_account;
     ```

     For CA APM 14.1.01 installation, execute the following commands to drop tables:

```
DROP TABLE al_meta_refresh_state;
```

For CA APM 14.1.02, execute the following commands to drop tables: :

```
DROP TABLE al_apmp_def;
DROP TABLE al_apmp_operation;
DROP TABLE al_apmp_content_types;
DROP TABLE al_apmp_progress_status;
DROP TABLE al_apmp_progress;
DROP TABLE al_apmp_record_filter;
DROP TABLE l_apmp_run_stage;
```

- **USS**

```
DROP TABLE os_externalsource;
DROP TABLE os_externalsourceproperties;
DROP TABLE portalpreferences;
DROP TABLE User_;
```

9. Restore the backup of tables from **step 4**. Execute the following command:

```
impdp mdbadmin/N0tallowed@mdb directory=test_dir dumpfile=expdptables.dmp
logfile=expdbtables.log
```

10. For USS, restore the backup of tables from **step 5**: Execute the following command:

```
impdp ussdbadmin/N0tallowed@uss_mdb directory=test_dir dumpfile=expdpusstables.
dmp logfile=impdpusstables.log
```

11. Start the services on both the source and the target systems. On the target system, perform the following steps for each product:

    a. **Common Admin Service**:

    - CA Service Management Admin

    b. **CA SDM Services**:
    Perform the following steps before you start the CA SDM services:

    - If your environment has customized CA PAM content, export all the relevant CA PAM Content from the source CA PAM server and import to the target CA PAM server. Complete the required CA PAM content configuration.
      For more information, see CA Process Automation (see page 292) .

    - Copy the **site/mods** directory from the source CA SDM server to the target CA SDM server.

      Note: This is applicable only if your application environment is customized. This is not applicable for out-of-the-box (OOTB) content.

    - Run the ***pdm_configure*** command without selecting the load default data option.

    - Now, start the following CA SDM services:

      - CA Service Desk Manager ODBC Data Access

- CA Service Desk Manager ODBC Agent
- CA Service Desk Manager Server

c. **CA Service Catalog Services**:
Perform the following steps before you start the CA Service Catalog services:

- If your source system has customized CA PAM content, export all relevant PAM content from the source CA PAM server and import to the target CA PAM server. Complete the required configurations for CA PAM content.
For more information, see CA Process Automation . (see page 292)
- If your source system has customized CA EEM policies, export all the relevant CA EEM policies from the source CA EEM server and import to the target CA EEM server.
For more information, see CA Embedded Entitlements Manager . (see page 283)
- Copy filestore directory from the source CA Service Catalog server to the target CA Service Catalog server.

  Note: This is applicable only if customization is carried out on the application environment. This is not applicable for the OOTB content.

- Launch the CA PAM server and access **SLCM_Globaldataset**.
Validate that the domain and the CA Service Catalog root business unit names are same.
- Now, start the following CA Service Catalog services:
  - CA Service Accounting
  - CA Service Catalog

d. **CA Asset Portfolio Management Services**:

- IIS Admin Service
- CA Asset Portfolio Management - Data Importer Engine
- CA Asset Portfolio Management - Event Service
- CA Asset Portfolio Management - Export Service
- CA Asset Portfolio Management - HW Reconciliation Engine
- CA Asset Portfolio Management - LDAP Import Service
- CA Asset Portfolio Management - Registration Service
- CA SM Server

e. **Unified Self-Service Services**:

- CA Unified Self-Service Jetty Server
- CA Unified Self-Service Server

12. Run the **pdm_k_reindex** command on the CA SDM target system to index knowledge documents that are created and copied from the source system.

13. Verify that CA Service Management applications are accessible. All applications must be up and running.

14. Validate that all CA Service Management Integration scenarios are working seamlessly.

Administering

Common Administration

CA Service Desk Manager

CA Service Catalog

CA Asset Portfolio Management

Administering CA Service Management

CA Service Management provides the ability to perform several administrative tasks that are common to the integrated products from a single interface. Earlier, it was required to manage tenants, users, roles, and other configurations such as CA EEM integration from the respective products' interfaces. However, with CA Service Management, you can manage all the common administrative tasks from the same interface.

Each administrative and configuration task is a service offering that you can access from Unified Self-Service or from CA Service Catalog. The configurations you make are applied to all the installed products of the solution.

As an Administrator, if you want to move MDB from the production to a pre-production environment, you can move the database from the source system and configure it to work on the target system. For more information, see How to Move the CA MDB Data from the Source to the Target Systems . (see page 747)

Note: The common administration service offerings are available only when you install CA Service Catalog as part of the solution. We recommend that you install Unified Self-Service with all combination of product installations and manage the solution administration through Unified Self-Service.

You can perform the following tasks using the service offerings:

- Manage tenants (see page 766)
  Create a new tenant and map tenant structures across integrated products to specify a single tenant structure.

- Manage roles (see page 771)
  Create service management roles and map roles across integrated products.

- Manage users (see page 776)
  Add existing users to the solution; create new users and assign roles to the users.

- Configure LDAP server settings (see page 779)
  Add LDAP servers to the solution to import and synchronize contacts from LDAP user records.

- Configure common components (see page 781)
  Manage component settings that are required to integrate CA Service Management products. Components that you can manage include CA EEM, CA Business Intelligence, CA Process Automation, and mail server.

- Manage product integrations (see page 782)
  Manage the settings of integrated products in the solution.

To view a list of available administrative service offerings and learn how to use them, see Administrative Service Offerings (see page 765).

When to Use the Solution Administration Capability

It is important to understand the scenarios in which you can leverage the solution administration capability:

Scenario 1: When you install a single product

If you install CA Asset Portfolio Management or CA Service Desk Manager, the common administration service offerings are not applicable. You must perform any administrative tasks through the respective product's administration page.

However, if you install CA Service Catalog only, you can use the administrative service offerings to perform administrative tasks of CA Service Catalog.

Scenario 2: When you install a combination of products

- CA Service Desk Manager and CA Asset Portfolio Management
  The common administration service offerings are available only when you install CA Service Catalog. In this scenario, you must use the respective product's administration pages to perform any administrative tasks. For example, to create a user you must create separate users in CA Service Desk Manager and CA Asset Portfolio Management.

- CA Service Desk Manager and CA Service Catalog (or) CA Asset Portfolio Management and CA Service Catalog
  You can use the administrative service offerings to perform administrative tasks. We recommend that you install Unified Self-Service and access the administrative service offerings through the self-service user interface.

- CA Service Desk Manager, CA Asset Portfolio Management, and CA Service Catalog
  You can use the administrative service offerings to perform administrative tasks. We recommend that you install Unified Self-Service and access the administrative service through the self-service user interface.

Any "modifications" or "adaptions" or "configurations" that are done administratively through the interface (web browser, command-line, Web Screen Painter) are "supported", meaning CA Support can assist with basic suggestions and trouble-shooting. CA Support does not do the changes for the customer, they are the customer's responsibility. For example, adding a field to a table and putting the field on a form through Web Screen Painter is a fully supported "modification". Another example, installing or uninstalling a feature through the Options Manager administration is a fully supported "configuration".

Anything to do with SPEL code, Java scripting (or any language scripting), or a customer-specific change to the underlying base code-line (done by CA Services or a Partner), is not supported by CA Support. The customer can do these things, but the customer is responsible for the support, maintenance, and trouble-shooting when things go wrong. If such "customizations" affect expected out-of-the-box behavior, CA Support will ask the customer to remove the customizations and see if the behavior persists.

Administrative Service Offerings

Administrative service offerings let you perform administrative tasks that are common to the products in the solution from a single location. Each service offering has a life cycle and has several phases. By default, the administrative service offerings life cycle has no approvals. To understand more about the request life cycle, see Request Life Cycle (see page 2115).

The table below lists the administrative service offerings and the tasks you can perform:

Service Offering	Task Description
Enable /Disable Multi-tenancy	Enable or disable tenancy management.
Add Tenant	Create a new tenant to access the capabilities of the solution.
Map Tenants	Map the existing tenant structures across integrated products to create a single logical tenant structure.
Manage Tenants	View and update tenants in your organization.
Add Role	Add a role that specifies permissions across products in the solution.
Manage Roles	Search and update service management roles to change what the user sees after logging in to the product. Map the service management roles to appropriate roles in integrated products.
Add User	Add new users to the solution and assign roles to the users.
Manage Users	Search and update details of users of the solution.
Add LDAP Server	Add an LDAP server to import a list of users from an external user store.
Synchronize Users	Automatically create users and assign roles to the users of a product in the solution, that earlier did not have any roles in other products
Manage LDAP Servers	View and update LDAP servers that you have integrated with solution.
Import Users from LDAP	Import a list of users from an external user store such as an active directory.
Configure Components	Manage settings of CA EEM, CA Business Intelligence, CA Process Automation, and mail server.
Manage Integrations	Manage the settings of integrated products in the solution.

Manage Tenants

Multi-tenancy is the ability for multiple independent tenants (and their users) to share a single implementation of CA Service Management. Through CA Service Management, you can create and manage the tenants of products in the solution from a single location. As part of tenancy management, you can perform the following tasks by using the administrative service offerings:

- Create new tenants.
- Map tenancy structures across integrated products (see page 768).
- Search for a list of available tenants.
- Update tenant details.

This article contains the following topics:

Enable or Disable Multi-tenancy

To mange tenants in the solution, you must enable multi-tenancy. You can disable multi-tenancy when you have no tenants in the solution or when you do not want to manage tenants.

Note: When you disable multi-tenancy, tenant related data is available to everyone who has access to the application.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.
2. In the Home page, click Request a Service.
   The Request Page Appears.
3. Under Categories, click Service Management Administration.
4. Click Enable/Disable Multi-Tenancy.
5. Specify whether to enable or disable multi-tenancy and click Submit.

Create Tenant

You can define as many tenants as required to manage multiple separate enterprises that provide support to clients. When you create a new tenant, the tenant views the CA Service Management implementation as solely for its own use and cannot update or view another tenant's data.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.

2. In the Home page, click Request a Service.
   The Request Page Appears.

3. Under Categories, click Service Management Administration.

4. Click Add Tenant.

5. Specify the details and click Submit.

View and Update Tenants

You can view a list of all the tenants that you manage in your organization. When required, you can make changes to tenant details. For example, you can change the terms of usage of a tenant to meet the new terms. If you no longer want to manage the tenant, you can inactivate it.

Note: You cannot update the parent details of the tenant using the administrative service offerings. To update the parent details, you must access the respective product's user interface.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.

2. In the Home page, click Request a Service.
   The Request Page Appears.

3. Under Categories, click Service Management Administration.

4. Click Manage Tenants.

5. Search for the list of available tenants.

6. Select the tenant that you want to update and click Update.

7. Update the tenant details and click Submit.

Map Tenancy Structures across Products in the Solution

As a solution Administrator, if you installed CA Service Management with a combination of products, you must map tenancy structures across the products to create a single tenant structure. If you already have more than one product in your environment and have implemented multi-tenancy, you can leverage your existing tenancy data for performing tenant management from a single location. It is possible that you have named your tenants differently in different products. So, as a first step, you map the tenants in different products and specify how to match them.

For example, *Tenant1* in CA SDM corresponds to *BusinessUnit3* in CA Service Catalog and *Tenant4* in CA APM. Hence, you specify the mapping information to simplify your tenancy management tasks. Once you perform the mapping, you can manage tenants from a single location.

Follow these steps:

1. Step 1: Know When to Map Tenancy Structures (see page 768).
2. Step 2: Review Your Existing Tenancy Structures (see page 768).
3. Step 3: Understand Default and Customized Tenancy Mapping (see page).
4. Step 4: Complete the Tenancy Mapping (see page 770).

Know When to Map Tenancy Structures

It is important to map tenancy structures in the following scenarios:

- You upgraded older versions of your products to CA Service Management. For example, you upgraded CA SDM 12.9 and CA Service Catalog 12.9 to CA Service Management.
- You first installed CA Service Management, but not all the products. However, you choose to integrate another product. For example, you initially installed CA SDM and CA APM as part of the solution. At a later point of time, you decided to install CA Service Catalog.

Review Your Existing Tenancy Structures

Before you perform any of the tenancy management tasks, it is important to review your existing tenant structures in each of the products you installed.

Follow these steps:

1. To view the tenants and the tenant structure in CA SDM, complete the following steps:
   a. Log in to CA SDM as an Administrator
   b. On the Administration tab, select Security and Role Management.
   c. Click the tenant to view the tenant information

   For more information, click Multi-tenancy in CA Service Desk Manager (see page 1343).
2. To view the tenants and the tenant structure in CA APM, complete the following steps:

a. Log in CA APM as an Administrator.

b. Click Administration, Tenancy Management.
The Multi-Tenancy Administration page appears.

c. On the left, click Tenant.

d. Click Go to view all the tenants.

e. Click the tenant to view the tenant information.

For more information, click Implementing Multi-tenancy (see page 1606).

3. To view the tenants and the tenant structure in CA Service Catalog, complete the following steps:

a. Log in to CA Service Catalog as an Administrator.

b. Select Administration, Business Units.

c. Expand the business unit tree and find the business unit that you want.

d. Click a business unit to view the business unit information.

For more information, click Multi-tenancy in CA Service Catalog (see page 1395).

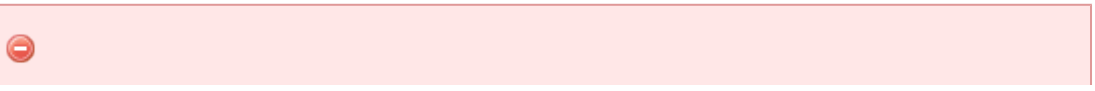
Understand Default and Custom Tenancy Mapping

When you map tenancy structures across the products in the solution, you can choose to automatically map tenants or map them manually. You must understand the different mapping processes and identify the one that better suits your requirements.

Default Tenancy Mapping

In the automatic tenant mapping process, you can choose to automatically map your tenancy structures. Tenant structures are mapped as follows:

- Service Providers of the products are first mapped to each other. In Unified Self-Service, the default tenant is the service provider.
- Based on the names and database IDs of the tenants, each tenant is mapped to tenants in the other product.
- If the number of tenants at a level are different in the products, a new tenant is created. For example, at level 2, CA SDM has four tenants but CA Service Catalog has five tenants. A new tenant is created and is mapped to the fifth tenant in CA Service Catalog.
- Tenants are mapped only if they are at the same level in the products. For example, a first-level tenant in CA Service Desk Manager is mapped only to first-level business unit in CA Service Catalog.



Important! When you choose to map tenant structures automatically, the mapping is successful only if all the products you upgraded to CA Service Management have the same database. If the products are installed on different databases, tenant information on databases other than the CA Service Management database is not migrated. For example, you installed CA SDM 12.9 and CA Service Catalog 12.9 on *database_server1* and *database_server2* respectively. While upgrading, you installed the solution on *database_server1*. Hence, tenant information on *database_server2* is not considered.

Custom Tenancy Mapping

You can map tenancy structures manually to meet your business requirements. Map your tenancy structures using the following rules:

- Do not map tenants that are at different levels. For example, do not map a seventh-level business unit in CA Service Desk Manager to a third-level tenant in CA Service Catalog.
- Do not map the same tenant more than once.
- Do not map a child without mapping all its parents. Map the parents from the tenant level directly above the child through the level directly under the Service Provider tenant.
- Verify that tenant names are unique across all products. For example, if you have a tenant named AAA in CA Service Desk Manager and CA Service Catalog, rename at least one of them to a unique, meaningful name.
- Verify that CA Service Catalog has no duplicate tenant names within its own tenant structure.

Complete the Tenancy Mapping

The Map Tenants service offering lets you perform the tenancy mapping.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.
2. In the Home page, click Request a Service.
   The Request Page Appears.
3. Under Categories, click Service Management Administration.
4. Click Map Tenants.
5. To map tenancy structures automatically, complete the following steps:
   a. Select Default Tenant Mapping.
   b. Click Submit.
6. To map tenancy structures manually, complete the following topics:

a. Select Custom Tenant Mapping.

b. Perform the mapping to meet your requirements and click Update Mapped Tenants.

c. Click Submit.

Manage Service Management Roles

User Role defines the tasks that a user typically performs. You define roles to control security and user interface navigation. Each role defines a focused view of the system by exposing only the functionality necessary for users in that role.

A user's default role determines the system view that is presented upon login. Users with multiple role assignments can switch from one role to another to see different views of the system without having to log out and log back in again.

CA Service Management lets you define service management roles that span across multiple products in the solution. A service management role is group of product roles that lets you assign multiple product roles to user at once. In the solution, you manage several service management roles. For example, System Administrator is a service management role. The System Administrator is responsible for managing configurations and administering roles and users of the individual products in the solution. Earlier, the role of an administrator was different in different products in the solution. Now, through the solution, you create a System Administrator service management role that defines the role of an administrator without having to create the roles separately in each of the products.

You can create and manage roles of integrated solutions from a single location. As part of role management, you can perform the following tasks by using the administrative service offerings:

- Define service management roles.
- Map the service management roles to appropriate roles in integrated products.
- Search for roles.
- Update role details.

This article contains the following topics:

Define a Role

You can create a service management role to meet your business requirements.

When you create a service management role, identify the corresponding roles in the integrated products. The integrated product role is either a predefined role or a role that you manually created. For example, a service management role you create must define the following:

- Name of the service management role: Business User

- Tasks performed by the role: Requests services, reports issues, and collaborates for self-help.
- Role in CA SDM: Employee, Customer
- Role in CA Service Catalog: End User
- Role in CA APM: Default User

Note: Every service management role you create must have a corresponding role in at least one of the integrated products.

The solution provides several predefined service management roles. For more information on predefined service management roles and the corresponding integrated product roles, see Predefined Service Management Roles (see page 772).

To see predefined roles in the each of the installed products, see the following information:

- Predefined roles in CA SDM (see page 1166)
- Predefined roles in CA Service Catalog (see page 1413)
- Predefined roles in CA APM (see page 1570)

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.
2. In the Menu, click My Requests.
   The Request page appears.
3. Click Create and select Request.
4. Under Categories, click Service Management Administration.
5. Click Add Role.
6. Specify the details and click Submit.

Predefined Service Management Roles

The solution provides several predefined service management roles. When you add a new role from predefined service management roles, the solution automatically identifies the corresponding roles in the integrated products.

The table details the predefined service management roles:

Service Management Role	Description	Roles in other products
System Administrator	System Administrators are responsible for managing configurations and administering roles and users of the individual products in the solution.	▪ CA SDM role: System Administrator ▪ CA Service Catalog role: Administrator ▪ CA APM role: System Administrator ▪ Unified Self-Service role: Administrator
Business User	Business users request services, report issues, and collaborate for self-help for issues related to IT.	▪ CA SDM role: Employee, Customer ▪ CA Service Catalog role: End User ▪ CA APM role: Default User ▪ Unified Self-Service role: End User
Approver	Approvers manage the change order process, but typically not the analysts who work on change order tickets.	▪ CA SDM role: Process Manager ▪ CA Service Catalog role: Request Manager ▪ CA APM role: NA ▪ Unified Self-Service role: End User
Service Catalog Administrator	Service Catalog Administrators create, define, and manage services for a specific tenant or business unit.	▪ CA SDM role: NA ▪ CA Service Catalog role: Catalog Administrator ▪ CA APM role: NA ▪ Unified Self-Service role: End User
Service Desk Administrator	Service Desk Administrators administer CA Service Desk Manager.	▪ CA SDM role: Adminstrator

Service Management Role	Description	Roles in other products
		▪ CA Service Catalog role: NA ▪ CA APM role: NA ▪ Unified Self-Service role: End User
L1 Analyst	L1 Analysts provide first-line support within your organization.	▪ CA SDM role: Service Desk Staff ▪ CA Service Catalog role: Request Manager ▪ CA APM role: Default User ▪ Unified Self-Service role: End User
L2 Analyst	L2 Analysts provide second-line support within your organization, which requires more advanced subject matter expertise.	▪ CA SDM role: IT Staff ▪ CA Service Catalog role: Request Manager ▪ CA APM role: Default User ▪ Unified Self-Service role: End User
Configuration Analyst	Configuration Analysts perform tasks within the configuration item life cycle process and second-line CMDB support within your organization.	▪ CA SDM role: CMDB Analyst ▪ CA Service Catalog role: Request Manager ▪ CA APM role: Asset Technician ▪ Unified Self-Service role: End User
Asset Manager	Asset Managers manage asset life cycle and asset fulfillment.	▪ CA SDM role: NA ▪ CA Service Catalog role: Request Manager ▪ CA APM role: Asset Fulfiller

Service Management Role	Description	Roles in other products
		▪ Unified Self-Service role: End User
Asset Management Administrator	Asset Management Administrators administer CA IT Asset Manager.	▪ CA SDM role: NA ▪ CA Service Catalog role: NA ▪ CA APM role: System Administrator ▪ Unified Self-Service role: End User
Service Owner	Service Owners are responsible for managing a specific IT service.	▪ CA SDM role: CMDB Administrator ▪ CA Service Catalog role: Catalog Administrator ▪ CA APM role: NA ▪ Unified Self-Service role: End User
Executive User	Executive users are decision makers, who would be primarily interested in metrics to understand performance and efficiency. The users must have view-only access to reports and dashboards.	▪ CA SDM role: Employee ▪ CA Service Catalog role: End User ▪ CA APM role: Default User ▪ Unified Self-Service role: End User

View and Update Roles

You can search for the available roles in the solution. When required, you can make changes to the role details. For example, you can change the name of the service management role.

You can also map the service management roles to appropriate roles in integrated products. For example, you first created a service management role with the following role definitions:

- Role in CA SDM: Employee, Customer

- Role in CA Service Catalog: End User
- Role in CA APM: Default User

However, at a later of point of time you decided to change the role in CA APM to Asset Technician.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.
2. In the Home page, click Request a Service.
   The Request Page Appears.
3. Under Categories, click Service Management Administration.
4. Click Manage Roles.
5. Search for the list of available roles.
6. Select the role that you want to update and click Update.
7. Update the role details and click Update.
8. Click Submit.

Manage Users

An important part of CA Service Management administration is to define the users accessing the solution. You must establish user security when you add new users to the product and assign a user ID and password. CA Service Management lets you create and manage users of integrated products from a single location. As part of user management, you can perform the following tasks by using the various administrative service offerings:

- Define users.
- Import user details from LDAP.
- Assign roles to users.
- Update user details.

This article contains the following topics:

Create a User

You can add a new user and define solution access rights to the user. When you create a user, the user details are available across the integrated products. For example, if you installed CA Service Desk Manager and CA Service Catalog, you can create a user and the user information is available in both the products.

When you add a new user, assign a role to the user. You can choose any predefined service management role or a custom role service management that you created.

If you have configured LDAP servers, you can also import the list of users. For more information, see Import Users Details from LDAP (see page 777).

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.

2. In the Home page, click Request a Service.
   The Request Page Appears.

3. Under Categories, click Service Management Administration.

4. Click Add User.

5. Specify the user details and click Submit.

Import User Details from LDAP

You can import a list of users from an external user store such as an active directory. Importing users helps you save time when defining your users and makes it easy to synchronize contacts with network user data.

You can import user details from only those LDAP servers that you configure with the solution. Therefore, before you import user details from an LDAP server, ensure that you add the LDAP server to the solution. For more information, see Add LDAP Servers (see page 779).

Note: To ensure user authentication, the LDAP server from which you import user details must be integrated with CA EEM.

When you add or create user details in an active directory, ensure that the you review the user name policies (such as special characters, mandatory parameters) of all the integrated products in the solution and specify the appropriate details.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.

2. In the Home page, click Request a Service.
   The Request Page Appears.

3. Under Categories, click Service Management Administration.

4. Click Import Users from LDAP.

5. Specify the details of the LDAP server from which you want to import users and click Submit.

Synchronize User Details across Integrated Products

You can synchronize users in the following scenarios:

- You upgraded older versions of your products to CA Service Management. For example, you upgraded CA SDM 12.9 and CA Service Catalog 12.9 to CA Service Management.
- You first installed CA Service Management, but not all the products. However, you choose to integrate another product. For example, you initially installed CA SDM and CA APM as part of the solution. At a later point of time, you decided to install CA Service Catalog.

In both the scenarios, the users of one product do not have a role assigned in other products of the solution. To ensure, that the every user has a role in the solution, you must synchronize the users.

When you use the synchronize contacts service offering, users of a product in the solution, that earlier did not have a role in other products, are automatically assigned a role. To assign a role, the service offering performs the following tasks in the order mentioned below:

- Identify the current role of the user in the product. For example, the role of User1 in CA SDM is Employee.
- Determine the service management role that the user's role corresponds to. For example, Employee in CA SDM corresponds to Business User service management role.
- Identify the corresponding role in the other products of the solution. For example, a Business User has the role of End User in CA Service Catalog, and Default User in CA APM.
- Search for the user details in the other integrated products. If the user does not exist, create the user. For example, if User1 details are not available in CA APM, User1 is created.
- Assign the respective product roles to the user.

If a user doesn't have any role assigned, you must specify the default role to be assigned to the user. For example, you imported user details from an LDAP server, but did not assign roles to the users. You specify the default role to be assigned to the user and then synchronize the users.

Note: You can assign only a service management role as a default role.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.

2. In the Home page, click Request a Service.
   The Request Page Appears.

3. Under Categories, click Service Management Administration.

4. Click Synchronize Users.

5. Select the default role and click Submit.

View and Update User Details

You can search for the list of users and update the details, when required. For example, you initially imported users from an LDAP server and later want to change the email id of a few users. You can also inactivate a user when you do not manage the user or the user is no longer part of your organization.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.

2. In the Home page, click Request a Service.
   The Request Page Appears.

3. Under Categories, click Service Management Administration.

4. Click Manage Users.

5. Search for the list of available users.

6. Select the user that you want to update and click Update.

7. Update the user details and click Submit.

Manage LDAP Servers

You can integrate multiple LDAP servers with CA Service Management. The administrative service offerings let you perform the following tasks:

- Add LDAP servers to the solution
- View and update LDAP server details, when required.

This article contains the following topics:

Add LDAP Server

CA Service Management allows you to import user details from an LDAP server. To import users from LDAP servers, you must first add the LDAP server to the solution. You can import users from only those LDAP servers that you added to the solution.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.

2. In the Home page, click Request a Service.
   The Request Page Appears.

3. Under Categories, click Service Management Administration.

4. Click Add LDAP Server.

5. Specify the details of the LDAP server and click Submit

Manage LDAP Servers

You can view and modify the LDAP servers integrated with the solution. When you no longer want an LDAP server integrated with the solution, you can inactivate it.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.

2. In the Home page, click Request a Service.
   The Request Page Appears.

3. Under Categories, click Service Management Administration.

4. Click Manage LDAP Servers.

5. Search for the list of available LDAP servers.

6. Select the LDAP server that you want to update and click Update.

7. Update the LDAP server details and click Submit.

Configure Common Components

CA Common Components are the components that are shared by all the products in the solution and have specific functions to perform. For example, you can configure CA Business Intelligence to generate reports. You can install the components through the CA Service Management solution or install them separately when required.

You can manage the settings of the following common components:

- CA Process Automation
- CA Business Intelligence
- CA EEM

This article contains the following topics:

When to configure the Common Components

You configure the CA common components in the following scenarios:

- You upgraded older versions of your products to CA Service Management and the older versions of the products already use the components.
  In this scenario, you must specify the details of the installed common components. If you integrated each product with different instances of common components, you must identify the instance that you want to integrate with the solution. For example, you integrated CA SDM with CA EEM on *server1* but integrated CA APM with CA EEM on *server2*. You must determine the CA EEM server instance that you want to integrate with the solution.
- You installed CA Service Management for the first time and installed the common components separately.
  In this scenario, you must specify the details of the installed common components to integrate with the solution.
- You already specified the common component details but want to change the settings.

For example, you installed CA Process Automation on *server1* and it is scheduled for maintenance soon. To avoid any downtime, you install CA Process Automation on *server2* and integrate the solution with *server2*.

Important! After you configure the common components, restart the CA SDM and CA Service Catalog services. If you have installed CA APM, you must recycle the Application Pool.

How to Configure the Common Components

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.

2. In the Home page, click Request a Service.
   The Request Page Appears.

3. Under Categories, click Service Management Administration.

4. Click Configure Components.

5. To configure the settings of a component, select the respective tab.
   For example, to update CA EEM settings, click the CA EEM tab.

6. Specify the details and click Submit.
   Note: When you change CA EEM settings, you may experience issues with logging in to the products of the solution. To resolve these issues, you must manually integrate CA EEM with the individual products. For more information, see Troubleshooting (see page 3250).

Manage Product Integrations

You can manage the settings of integrated products in the solution. After you integrated products in the solution, you can change several configuration settings of the integrated products. Based on the new settings, the products are automatically integrated. For example, you changed the host name of the server on which you installed CA SDM. You specify the new host name using the service offering and integration is performed automatically.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.

2. In the Home page, click Request a Service.
   The Request Page Appears.

3. Under Categories, click Service Management Administration.

4. Click Product Integrations.

5. To configure the settings of a product, select the respective tab.
   For example, to update CA SDM settings, click the CA Service Desk Manager tab.

6. Specify the settings and click Submit.

7. (Optional) Any changes you make the CA SDM details are not updated in the *ca_registration* table in the MDB. If necessary, you must update the details in the table manually.

8. (Optional) If CA Process Automation is integrated with CA Service Catalog, any changes you make to the CA Service Catalog details are not updated in the CA SDM and CA Service Catalog datasets in CA Process Automation. You manually update the changes in CA Process Automation.

Business Value Dashboards

A Business value dashboard is a real-time graphical representation of an organization's Key Performance Indicators (KPI) that enables decision makers such as IT managers to make informed decisions. The dashboards represent detailed information about the following:

- Service support metrics such as the categories of incidents or requests, the associated volume, cost, and time spent for incident resolution.
- Operational and functional efficiency information such as, how support groups are occupied, information on ticket transfer from one group to another and the impact on time and cost.

Each dashboard is a service offering that is exposed through CA Service Catalog and accessible through the Unified Self-Service interface.

As an Administrator, you are responsible for the following:

- Configuring the business value dashboard reports
- Defining the users and user access permissions to the dashboards
- Troubleshooting any issues related to business value dashboards

Complete the following steps to implement business value dashboards:

1. Know When the Business Value Dashboards are Available (see page 783)
2. Review the Business Value Dashboards Prerequisites (see page 784)
3. Determine the Business Value Dashboards User Permissions (see page 786)
4. Configure the Business Value Dashboard Reports (see page 786)
5. (Optional) Learn How to Schedule the Business Value Dashboard Reports (see page 787)
6. (Optional) Understand the Important Metrics (see page 791)

Know When the Business Value Dashboards are Available

It is important to understand the various scenarios when you can access the business value dashboards.

Installation Scenarios

The type of installation determines the type and availability of the dashboards.

Type of Installation	Dashboards Availability
New installation For example, as part of CA Service Management, you installed CA Service Catalog and CA SDM for the first time.	Dashboards are available automatically. No configuration is required.
Upgrade For example, you upgraded older releases of CA Service Catalog or CA SDM or both to release 14.1.	Dashboards are available automatically. No configuration is required.
You first installed CA Service Catalog and at a later point installed CA SDM.	Import the the CASM.biar file manually. The file is available at the following location: [ISO_ROOT\filestore\BOXI\biconfig] **Note:** Verify that CA Service Catalog and CA SDM BIAR files are already imported.

Products Installed

The dashboards and the comprising reports that are available to you are based on the products you installed as part of the CA Service Management solution.

Products Installed	Available Dashboards
CA Service Catalog only	Service Demand - Requests
CA Service Desk Manager only	Service Demand - Incidents Operational Effectiveness
CA Service Catalog and CA Service Desk Manager	Service Demand - Requests Service Demand - Incidents Service Demand Operational Effectiveness

Review the Business Value Dashboards Prerequisites

Before you use the dashboard reports, ensure that you considered the following prerequisites:

- Both CA Service Desk Manager and CA Service Catalog must use the same CA Business Intelligence server.
- Run the following queries on an Oracle MDB:

```
create or replace function MDBADMIN.left(str1 varchar2 :=NULL,num1 NUMBER)
RETURN VARCHAR2
```

```
as

ascii_chr varchar2(32767);

begin

ascii_chr:= substr(str1,1, num1);

return ascii_chr;

end;


Update report_labels set language_code ='en' where language_code='en ';
```

- Install the Arial Unicode MS font on the server where the BIAR file will be imported. Additionally, the same font must be available on the machine from where the reports will be viewed. The font files must be copied to the Windows font folder directory.
  Following code must be added to the fontalias.xml located in below location:
  <BusinessObjects Installation Path>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64\fonts

```
<FONT NAME="Arial Unicode MS">

<FONTFAMILY PLATFORM="ttf" NAME="Arial Unicode MS">

<FONTATTRIBUTE BOLD="false" ITALIC="false" LOGICAL="Arial Unicode MS" PHYSICAL="ARIALUNI.TTF"/>

</FONTFAMILY>

<FONTFAMILY PLATFORM="win" NAME="Arial Unicode MS"/>

<FONTFAMILY PLATFORM="java" NAME=" 'Arial Unicode MS', 'Arial Unicode MS'"/>

<FONTFAMILY PLATFORM="html" NAME=" 'Arial Unicode MS', 'Arial Unicode MS'"/>

</FONT>
```

- Enable the Key Performance Indicators (KPIs) for Operational Effectiveness Dashboard.
  Enabling KPI for Operational Effectives Business Objects Dashboard is mandatory to retrieve the Group information when CA SDM incidents are transferred to multiple Groups for ticket resolution. Consider the following:
  To show Support Groups Productivity and Functional Escalations in Operational Effectiveness dashboard, navigate to the CA SDM Administration tab, Options Manager, KPI and ensure that the status of kpi_ticket_data_table is installed.

- Configure the NX_KPI_TICKET_DATA_TABLE_DELAY variable to specify how frequently the incident data (for example, incident transfer) is updated in the database. The recommended value is 900 seconds.
  To configure the variable, complete the following steps in the order mentioned below:

  - Navigate to [SDM Root folder].
  - Open the NX.env file in notepad.
  - Search for @NX_KPI_TICKET_DATA_TABLE_DELAY and specify the value.
    For example, @NX_KPI_TICKET_DATA_TABLE_DELAY = 900.

- Make sure that every analyst is associated with a support group. Data related to an analyst with no support group is not displayed on business dashboard.

- Every time an analyst moves from one group to another, make sure to note down the analyst metrics in the previous group. The business dashboards display any metrics related to the older group as belonging to the new group.

Determine the Business Value Dashboards User Permissions

The role and user permissions determine the users accessing the dashboard and the users configuring the dashboards. To provide permissions to any user to configure the reports or access the dashboard, you must add the user to the CA Service Management group.

Important! You must add the *CASMAdmin* user to the CA Service Management group. The CASMAdmin user has the privileges to access the solution dashboard and also run the reports.

Follow these steps:

1. Log in Central Management Console as an administrator.
   http://cabi-hostname:Port_number/BOE/CMC
2. Under Organize, click Users and Groups.
3. Click User List.
4. Right-click the user you want to add to the CA Service Management group and click Join Group.
5. Select CAServiceManagement and move it from Available Group(s) to Destination Group(s).
6. Click Ok and save the changes.

Configure the Business Value Dashboard Reports

This article contains the following topics:

Scheduled and On-demand Reports

CA Service Management provides you the flexibility of generating reports, when required. The report generation is classified as Scheduled reporting and On-demand reporting.

Scheduled Reporting

You can use the scheduled reports when your organization requires reports to be generated at frequent intervals. Also, when you have a large data to generate reports from, you can use the scheduled reports. For example, a report is to be generated on a weekly basis. So, you use the scheduled reports and configure them to generate reports once in a week.

Note: We recommend that you use scheduled reporting when the data size is more than 10,000 records.

On-demand Reporting

You can use the On-demand reports to generate the business value dashboards when required or to process small data. For example, your organization does not require reports to be generated at frequent intervals. However, you need to generate a report whenever an executive user requires you to generate it.

Note: We recommend that you use scheduled reporting when the data size less than 10,000 records.

To know the data size, identify the count of the following tables in your MDB:

- *usm_subscription_detail* for the number of requests
- *call_req* for the number of incidents

Dashboards and the Associated Reports

Each dashboard has several reports and sub-reports associated that you can view and configure to meet your requirements. The reports are accessible through the BusinessObjects Central Management Console.

Follow these steps to access the reports associated with the dashboards:

1. Log in Central Management Console as an administrator.
   http://cabi-hostname:Port_ (http://cabi-hostnamePort_)number/BOE/CMC
2. Navigate to Folders, All Folders, CA Reports, CA Service Management.
3. Do one of the following:
   - Click View on Demand Dashboard to view the reports that you can generate on-demand.
   - Click Scheduled Dashboard to view or schedule reports as per your requirement.
   - Click Sub Reports to view the sub reports of Service Demand and Operational effectiveness dashboards.

Learn How to Schedule the Business Value Dashboard Reports

This articles explains how to schedule dashboard reports and tasks you must perform before and after scheduling the reports.

Note: Perform these tasks only if you or the end user access the dashboards from the Unified Self-Service user interface.

Complete the following:

- Configure the Business Value Dashboard Service Offerings (see page 788)
  - Identify the Report ID (see page 788)
  - Configure the Service Offering (see page 788)
- Schedule the Business Value Dashboard Reports (see page 789)
- Verify the Scheduled Dashboards (see page 791)

Configure the Business Value Dashboard Service Offerings

Each dashboard is a service offering that is exposed through CA Service Catalog and accessible through the Unified Self-Service interface.

By default, the dashboard service offerings represent data generated by on-demand reports. To display scheduled reports, you must perform several configurations on service offerings.

Complete the following steps:

- Identify the Report ID (see page)
- Configure the Service Offering (see page 788)

Identify the Report ID

Follow these steps:

1. Log in to Central Management Console as an administrator or a user with permissions to schedule report generation.
   http://cabi-hostname:Port number/BOE/CMC
2. Navigate to Folders, All Folders, CA Reports, CA Service Management, Scheduled Dashboard.
3. Right click the report that you want to schedule and select Properties.
4. From the ID, CUID field, make a note of the CUID of the report.
   For example, in **ID, CUID:17810, ATKoKrurIjlCqTvnya20W1s**, the CUID is ATKoKrurIjlCqTvnya20W1s.

Configure the Service Offering

Follow these steps:

1. Log in to CA Service Catalog as an Administrator.
2. Navigate to Catalog, Service Offerings, Offerings.
3. Expand Service Management Dashboards.
4. Select the service offering that represents the dashboard for which you want to schedule a report.
   For example, Operational Effectiveness.
5. Click the copy icon.
6. Create a copy of the service offering in the same folder and specify the name of the new service offering.
   For example, Operational Effectiveness - Scheduled Report.
7. Click the new service offering copy.
   In this example, click Operational Effectiveness - Scheduled Report.

8. In the Details tab, set the Availability date.
9. In the Permissions tab, enable permissions for the appropriate roles.
10. In the Definition tab, click Edit Service Option.
11. From the Form field, make a note of the Form name.
12. Navigate to Catalog, Forms.
13. Expand Forms, Service Management Dashboards Forms.
14. Click the form that you earlier noted and create a copy of the form as you created a copy of the service offering.
15. Click the new form and the click Script.
16. Search for the following statement. In this example, the form is the Operational Effectiveness form.

```
cabiURL = 'http://' + ca_fd.js.cabiHostName + ':' + ca_fd.js.cabiPort + '/BOE
/OpenDocument/opendoc/openDocument.jsp?
iDocID=AbEmxu8mNftBjHQIMRu2uLs&sIDType=CUID&sReportMode=weblayout&token=' + rows
[0].value;
```

17. Replace the iDocID variable with the appropriate CUID that you earlier noted.
    For example, replace AbEmxu8mNftBjHQIMRu2uLs with ATKoKrurIjlCqTvnya20W1s.
18. Click Save.
19. In the new service offering you created, update the Form name in the Definition tab to the new form name.
20. Save the changes.

Schedule the Business Value Dashboard Reports

Schedule a report when the date size is more than 10,000 records. It is important to configure both the reports and the associated sub-reports.

To know the data size, identify the count of the following tables in your MDB:

- *usm_subscription_detail* for the number of requests
- *call_req* for the number of incidents

Follow these steps:

1. Log in to Central Management Console as an administrator or a user with permissions to schedule report generation.
   http://cabi-hostname:Port_number/BOE/CMC
2. **To schedule the Service Demand-Incidents dashboard, complete the following steps:**

a. Navigate to Folders, All Folders, CA Reports, CA Service Management, Sub Reports.

b. Right-click Incident Cost Details, Incident Effort Details, Incident Volume Details and select Schedule.

c. Configure the appropriate parameters and click Schedule.

d. Navigate to Folders, CA Reports, CA Service Management, Scheduled Dashboard, Service Demand – Incidents.

e. Right-click Service Demand- Incidents and click Schedule.

f. Configure the appropriate parameters and click Schedule.
Note: Ensure you that parameter values you configure for reports and their sub-reports are the same.

3. **To schedule the Service Demand-Request dashboard, complete the following steps:**

a. Navigate to Folders, All Folders, CA Reports, CA Service Management, Sub Reports.

b. Right-click Request Volume/Cost for Services and select Schedule.

c. Configure the appropriate parameters and click Schedule.

d. Navigate to Folders, CA Reports, CA Service Management, Scheduled Dashboard, Service Demand – Requests.

e. Right-click Service Demand- Requests and select Schedule.

f. Configure the appropriate parameters and click Schedule.
Note: Ensure you that parameter values you configure for reports and their sub-reports are the same.

4. **To schedule the Service Demand dashboard, complete the following steps:**

a. Navigate to Folders, All Folders, CA Reports, CA Service Management, Sub Reports, Service Demand Scheduling.

b. Right-click on each of the reports and select Schedule.

c. Configure the appropriate parameters and click Schedule.

d. Navigate to Folders, CA Reports, CA Service Management, Scheduled Dashboard, Service Demand.

e. Right-click Service Demand and select Schedule.

f. Configure the appropriate parameters and click Schedule.
Note: Ensure you that parameter values you configure for reports and their sub-reports are the same.

5. **To schedule the Operational Effectiveness dashboard, complete the following steps:**

a. Navigate to Folders, All Folders, CA Reports, CA Service Management, Sub Reports.

b. Right-click FCR For Incident Categories, Groups By Effort Incurred On Resolution Functions, MTTR for Incident Categories and select Schedule.

c. Configure the appropriate parameters and click Schedule.

d. Navigate to Folders, CA Reports, CA Service Management, Scheduled Dashboard, Operational Effectiveness.

e. Right-click Operational Effectiveness and select Schedule.

f. Configure the appropriate parameters and click Schedule.
Note: Ensure you that parameter values you configure for reports and their sub-reports are the same.

Verify the Scheduled Dashboards

After you schedule the report generation, you must verify if the dashboards are created correctly. Each dashboard is a service offering that is exposed through CA Service Catalog and accessible through the Unified Self-Service interface.

Follow these steps:

1. Log in to Unified Self-Service as a user with permissions to access the dashboards.
If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.

2. In the Home page, click Request a Service.
The Request Page Appears.

3. Under Categories, click Service Management Dashboards.
You must see the service offerings that you configured.

4. Click an appropriate service offering to see the related information.

Understand the Important Metrics

The three parameters related to request and incidents/categories that are significant to decision makers are cost, effort, and volume.

It is important to understand how these parameters are calculated:

Effort

Effort is the time total time spent on an incident resolution. The time spent may be by one user or multiple users in resolving an incident. The effort is calculated only when the users appropriately log in the time spent on an incident. It is important that your organization recommends time logging.

The **Time Spent** field in the incident details determines the time spent on the incident.

Volume

Volume is the total number of requests/incidents in a specific category. It is important that each incident/request has a specific category associated with it. For example, Hardware, Networking, Applications are categories.

Cost

Cost is a function of effort spent and the resource rate. It is also the cost of a service.

Each incident/request has a category associated and the total cost of a category is the sum of all costs of incidents/requests in a specific category.

- For an incident, cost is calculated as follows:

  Cost of an incident = Total time spent (in hours) by a resource * Rate (per hour) of the resource
  The following example describes how the cost parameter is calculated for an incident involving multiple resources.

Data	Analyst_1	Analyst_2
Resource Rate (per hour)	$ 100	$ 75
Time spent (in hours)	10	15

  Total cost = ($100 * 10) + ($75*15) = $ 2125
  Note: The **Cost** field in the **Contact Details** page determines the resource rate.

- For a request, the cost is the cost field that you associate for a service offering.

Offline Reporting through Microsoft SQL Server Database Replication

This section covers the the following topics:

Introduction

CA Service Management lets you generate reports that help you analyze important information. Every time that you generate a report, the application (CA SDM, CA APM, or CA Service Catalog) accesses the database to fetch information. When your database contains large volumes of data, the data retrieval process impacts the performance of your application. An effective way to reduce performance issues is to replicate or create an offline version of your database. While users continue to access the application to perform day-to-day tasks, the application accesses the replicated or offline database for any report generation activity.

Note: The database replication process is applicable only if you use Microsoft SQL Server in your environment.

This article contains the following topics:

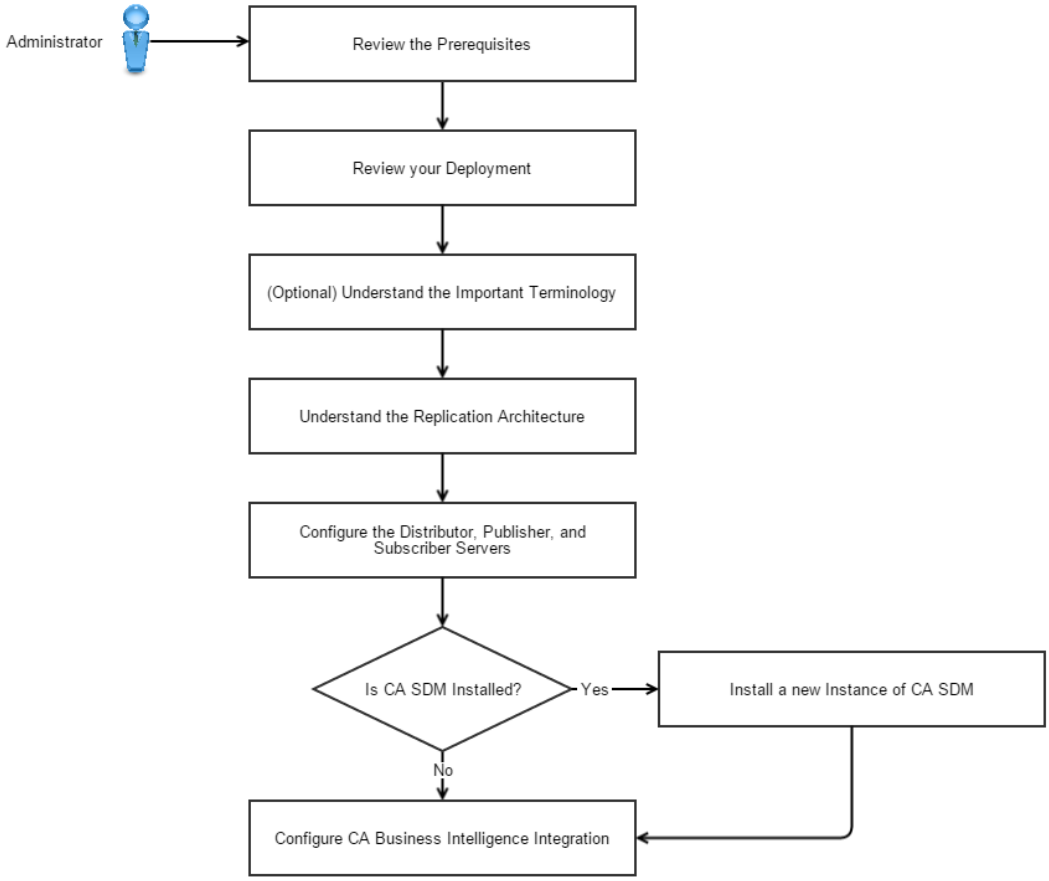
The Environment

You can implement offline reporting in the following environment:

- **Products installed:** CA Service Management 14.1 or version 12.9 of CA SDM, CA APM, and/or CA Service Catalog
- **Database:** Microsoft SQL Server 2008/2012/2014

The following diagram illustrates how a solution administrator implements database replication for offline reporting:

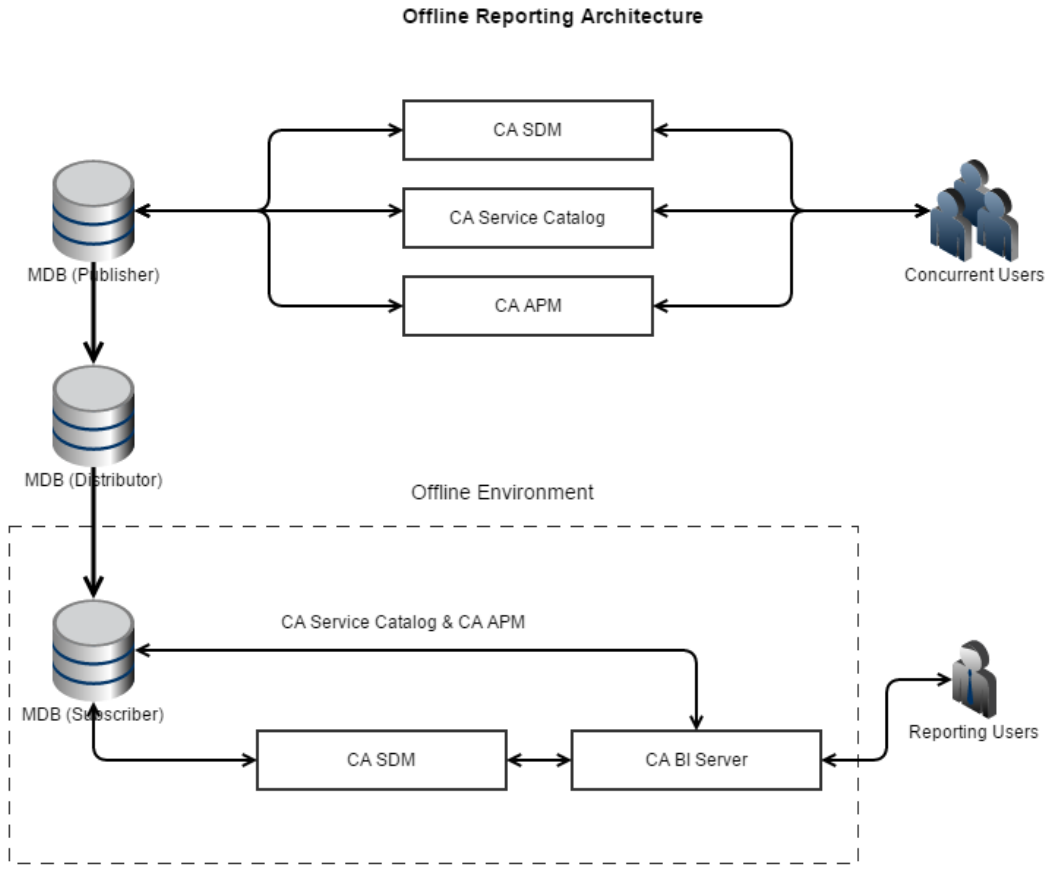
Implementing Offline Reporting through Database Replication



For more information about how to install the Replication feature, see Microsoft SQL Server documentation.

The Architecture

The following diagram illustrates the architecture of a replicated database environment for offline reporting:



Benefits

In CA Service Management, database replication is performed through the transactional replication process.

Replicating the database through transactional replication has the following benefits:

- Incremental changes are propagated to the Subscribers as they occur.
- Report generation does not require any changes to be made by the Subscriber and thus data need not be propagated back to the Publisher. In transactional replication, Subscribers are read-only and thus do not affect the performance of your environment.
- Low latency between the time changes is made at the Publisher and the changes arrive at the subscriber.
- Effective management of high insert, update, delete activity when compared to other types of replication

Note: With support for transactional replication in CA Service Management 14.1 or version 12.9 of CA SDM, CA APM, and/or CA Service Catalog, support for merge replication process is deprecated. If you already implemented merge replication on CA Service Management 14.1, we recommend you to disable it and implement transactional replication.

Best Practice

Scenario 1: New Installation of CA Service Management

If your environment is following the database replication process for the first time, it is recommended you install CA Service Management, and enable transactional replication.

Scenario 2: Upgrade CA Service Management

If your environment follows the database replication process, it is recommended you disable the replication process (merge or transactional), upgrade CA Service Management, and enable the transactional replication.

Scenario 3: Integration of CA Service Management Products

If your environment follows the database replication process, it is recommended you disable the replication process (merge or transactional), Integrate the CA Service Management products, and enable the transactional replication.

Glossary

The following terms are used frequently in the configuration information. Understand the meaning of the terms before you start configuring offline reporting:

Production Database

Production database refers to the database server that CA Service Management uses. This is the database from where you replicate another database for offline reporting.

Production database is typically the database server in a production environment.

Reporting Database

Reporting database refers to the database that you replicated from the production database. The reporting database is used only for offline reporting.

Publisher

The Publisher is a server that makes data available for replication to other servers. In addition to being the server where you specify the data to be replicated, the Publisher also detects the data that has changed and maintains information about all publications at that site.

In the offline reporting scenario, the publisher is typically the production database server.

Distributor

The Distributor is a server that contains the distribution database and stores meta data, history data, and/or transactions. The Distributor can be a separate server from the Publisher (remote Distributor), or it can be the same server as the Publisher (local Distributor).

Subscriber

Subscriber is a server that receives replicated data. Subscribers subscribe to publications, not to individual articles within a publication, and they subscribe only to the publications that they need, not necessarily all of the publications available on a Publisher.

Verify the Prerequisites

We recommend that you complete this checklist before you proceed.

1. You must have DBA privileges.
2. The following Windows services must be running. We recommend that you set the start mode to **Automatic**.
   - SQL Server
   - SQL Server Agent
   - SQL Server Browser
3. The SQL Server Agents must run on publisher, distributor, and the subscriber servers.
4. You can perform either of the following steps:
   a. **Use a domain account for every agent.** Add the domain account to the SQL Server logins and assign the sysadmin role. Set **Master** as the default database.
   b. **For each agent, create a local Windows account on the respective servers.** Add the Windows user account that you created to the SQL Server logins and assign the sysadmin role. Set **Master** as the default database.
5. Create a Snapshot Folder. Ensure that the Snapshot Folder is a network folder and not a local folder.
6. To implement replication, Microsoft mandates that every table is associated with a primary key. Hence, ensure any new table that you want to replicate has a primary key that is associated with it.
7. To connect to the database, the replication utility requires an SQL server authentication-based login credentials. We recommend the default system admin account to be used.

Review CA Service Management Deployment

Before you configure offline reporting, review the products that you installed as part of the CA Service Management solution.

Approach

Refer to the instructions in either of the following approaches depending on your deployment type.

Approach 1: Back-up and Restore the Existing Instance of MBD

The approach is a three-step procedure.
Step 1: Back up and Restore (see page 798)
Step 2: Implement Replication (see page 798)
Step 3: Set up and configure CA SDM (see page 798)

Step 1: Back up and Restore

Back up the production server database and restore to the offline server. For more information, see MSDN documentation.

Step 2: Implement Replication

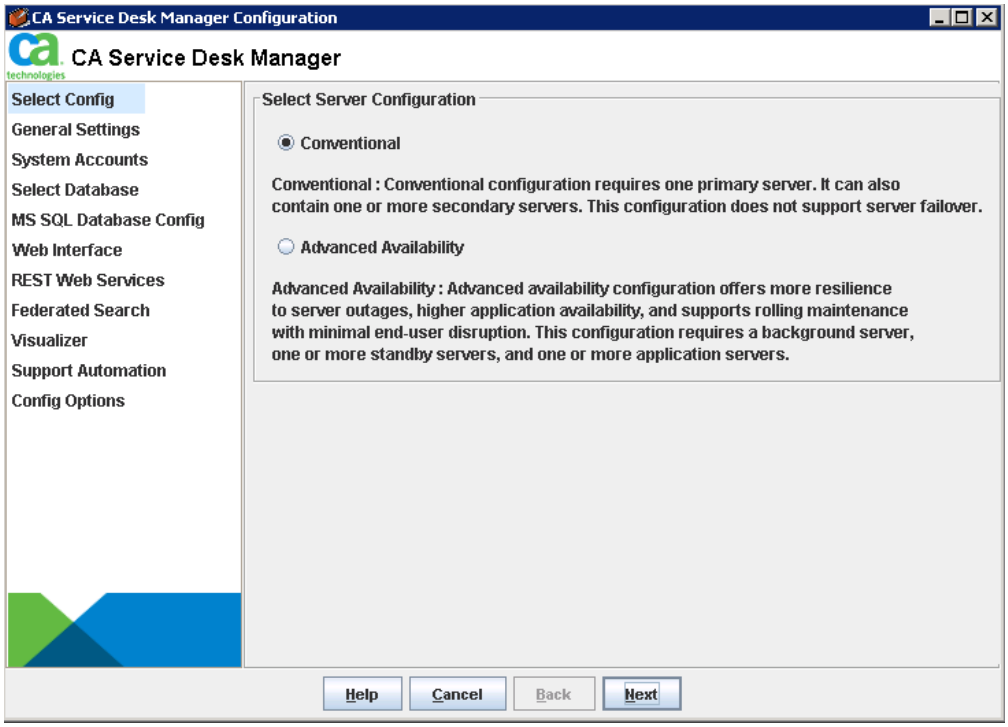
An effective way to reduce application performance issues is to replicate or create an offline version of your database. The users can continue to access the application to perform day-to-day tasks, the application accesses the replicated or offline database for any report generation activity. For more information, s ee How To Implement Replication (see page 805).

Step 3: Set up and Configure CA SDM

Follow these steps:

1. Launch the CA SDM installer from the following location:
   - **CA Service Management 14.1:** <Installation_Media_Root>\products\SDM\setup.exe
2. Follow the on-screen instructions until you reach the Configuration window.

3. Click **Cancel**



(see page 797)

4. Using a text editor, open the NX_ROOT\pdmconf\NX.env_nt.tpl file (NX_ROOT is the installation directory for CA SDM) and perform the following steps:

    a. Use the following sample code to verify that auditing is commented out:

    ```
    # Create audit log entry for field update.
    ! @NX_AUDIT_UPD=
    # Create audit log entry for deletion.
    ! @NX_AUDIT_DEL=
    ```

    b. Add the following code and parameters at the end of the file:

    ```
    @NX_EVENT_LOG_EXCLUDE=ALL
    @NX_SESSION_LOG_EXCLUDE=ALL
    ```

5. Using a text editor, open the NX_ROOT\pdmconf\pdm_startup.tpl file.

6. Edit the file by changing the line *[default procset MAIN_PROCSET]* to *[default procset OFFLINE_REPORTING]*.

7. Save and close the file.

8. Complete the following steps in Microsoft SQL Server Management Studio:

    a. Expand **Databases, mdb, Security, Users**.

b. Right-click **mdbadmin** and select **Properties**.

c. In the **Database User** window, next to **Default schema**, click the search option.

d. In the **Select Schema** window, enter *[dbo]* and click **Browse**.

e. In the **Browse for Objects** window, select the **mdbadmin** object and click **OK**.

f. In the **Database User** window, select the following entries under **Role Members** and click **OK.**

- ams_group
- db_ddladmin
- db_owner
- db_securityadmin
- regadmin
- service_desk_admin_group
- service_desk_ro_group
- usmgroup
- workflow_admin_group

9. Update the *usp_servers* table entry for local_host column. Run the following commands on the offline reporting data base server for the MDB:

```
update usp_servers
set local_host='<Offline CA SDM Server Name>'
where id=1001
```

Note: Perform this step when you install CA SDM on the restored MDB on the offline server.

10. Configure CA SDM with replicated db and do not select “load-default’ data check box. To configure CA SDM run the following command on the command prompt:

```
CMD>:\ pdm_configure
```

11. In the Windows command prompt, run the following command to view the status of the services:

```
pdm_status
```

12. To verify the installation, navigate to the following URL:

```
http://<Offline_Reporting_Server>:<SDM_Port_Number>/CAisd/pdmweb.exe
```

13. Configure CA Business Intelligence and integrate with offline MDB.

> **Note:** If multi-tenancy is enabled on the production instance of CA SDM, then manually install the same on the offline instance of CA SDM. For more information about enabling multi-tenancy, see *Administration Guide, Defining Business Structure, Multi-Tenancy, How Multi-Tenancy Works, The Multi-Tenancy Option,* available in the CA SDM Release 12.9 version bookshelf on CA Support Online (https://support.ca.com/cadocs/0/CA%20Service%20Desk%20Manager%2012%209-ENU/Bookshelf.html).

Approach 2: New MDB Instance

The approach is a three-step procedure.

- Step 1: Install MDB (see page 801)
- Step 2: Implement Replication (see page 801)
- Step 3: Set up and configure CA SDM (see page 801)

Step 1: Install MDB

Follow these steps:

1. Mount the installation media on your drive.
2. Launch the CA SDM installer from the following location:
   - **CA Service Management 14.1:** <Installation_Media_Root>\products\setup.exe

   The Installation Menu appears.
3. Click the Product Installs tab.
4. Click CA MDB.
5. Continue following the on-screen instructions to complete the installation.

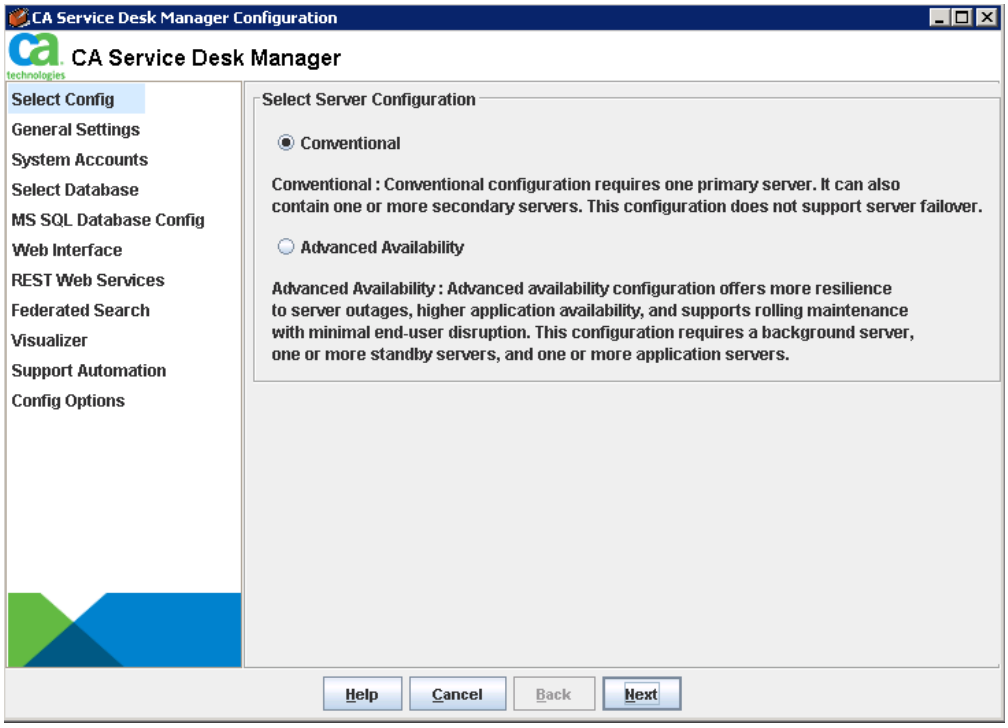
Step 2: Implement Replication

An effective way to reduce application performance issues is to replicate or create an offline version of your database. The users can continue to access the application to perform day-to-day tasks, the application accesses the replicated or offline database for any report generation activity. For more information, s ee How To Implement Replication (see page 805).

Step 3: Set up and Configure CA SDM

Follow these steps:

1. Launch the CA SDM installer from the following location:
   - **CA Service Management 14.1:** <Installation_Media_Root>\products\SDM\setup.exe
2. Follow the on-screen instructions until you reach the Configuration window.
3. Click **Cancel**.



4. Using a text editor, open the NX_ROOT\pdmconf\NX.env_nt.tpl file (NX_ROOT is the installation directory for CA SDM) and complete the following steps:
   a. Use the following sample code to verify that auditing is commented out:

```
# Create audit log entry for field update.
! @NX_AUDIT_UPD=
# Create audit log entry for deletion.
! @NX_AUDIT_DEL=
```

   b. Add the following code and parameters at the end of the file:

```
@NX_EVENT_LOG_EXCLUDE=ALL
@NX_SESSION_LOG_EXCLUDE=ALL
```

5. Using a text editor, open the NX_ROOT\pdmconf\pdm_startup.tpl file.
6. Edit the file by changing the line *[default procset MAIN_PROCSET]* to *[default procset OFFLINE_REPORTING]*.

7. Save and close the file.

8. Complete the following steps in Microsoft SQL Server Management Studio:

    a. Expand **Databases, mdb, Security, Users**.

    b. Right-click **mdbadmin** and select **Properties**.

    c. In the **Database User** window, next to **Default schema**, click the search option.

    d. In the **Select Schema** window, enter *[dbo]* and click **Browse**.

    e. In the **Browse for Objects** window, select the **mdbadmin** object and click **OK**.

    f. In the **Database User** window, select the following entries under **Role Members** and click **OK.**

    - ams_group
    - db_ddladmin
    - db_owner
    - db_securityadmin
    - regadmin
    - service_desk_admin_group
    - service_desk_ro_group
    - usmgroup
    - workflow_admin_group

9. Insert the offline server details in the *usp_servers* table. Run the following commands on the offline reporting data base server for the MDB:

```
INSERT INTO [dbo].[usp_servers]
([id],[del],[local_host],[timezone],[nx_desc],[last_mod_dt],[last_mod_by],
[server_id],[server_type],[database_type],[external_dns_name],[platform],
[linked],[slump_port],[upload_path])
VALUES(1001,0,'<Offline CA SDM Server Name>',NULL,'Local System
(<Offline CA SDM Server Name>)',NULL,NULL,14538,0,0,'',1,1,2100,NULL)
```

10. Configure CA SDM with replicated db and do not select “load-default’ data check box. To configure CA SDM run the following command on the command prompt:

```
CMD>:\ pdm_configure
```

11. In the Windows command prompt, run the following command to view the status of the services:

```
pdm_status
```

12. To verify the installation, navigate to the following URL:

    ```
    http://<Offline_Reporting_Server>:<SDM_Port_Number>/CAisd/pdmweb.exe
    ```

13. Configure CA Business Intelligence and integrate with offline MDB.

> **Note:** If multi-tenancy is enabled on the production instance of CA SDM, then manually install the same on the offline instance of CA SDM. For more information about enabling multi-tenancy, see *Administration Guide, Defining Business Structure, Multi-Tenancy, How Multi-Tenancy Works, The Multi-Tenancy Option,* available in the CA SDM Release 12.9 version bookshelf on CA Support Online (https://support.ca.com/cadocs/0/CA%20Service%20Desk%20Manager%2012%209-ENU/Bookshelf.html).

Configure CA Business Intelligence Integration

CA Business Intelligence, the reporting application that you earlier configured to access the production database must now access the reporting database. However, the way CA Business Intelligence integrates with the reporting database depends on the products you installed as part of CA Service Management.

> **Tip!** We recommend that you have the bookshelf for CA Business Intelligence available during the integration process.

- **CA SDM:** CA Business Intelligence does not access the reporting database directly. If you installed CA SDM, then configure CA BI with the CA SDM offline server to access the reporting database. For more information, see Integrate CA Service Desk Manager with CA Business Intelligence Manually (see page 3263).
- **CA Service Catalog:** CA Business Intelligence does access the reporting database directly. For more information, see Integrate CA Service Catalog with CA Business Intelligence Manually (see page 3293).
- **CA APM:** CA Business Intelligence does access the reporting database directly. For more information, see Integrate CA Asset Portfolio Management with CA Business Intelligence Manually (see page 3482).

> **Note:** Configure CA Business Intelligence to access the reporting database and not the production database.

Implement Replication

This article describes the process to implement replication.

- Configure the Distributor, Publisher, and Subscriber Servers (see page 805)
- Perform the Validation Check (see page 805)

Tip! Initiate the replication process during a planned maintenance window as it involves creating a snapshot of the database. While this process is in progress, access to your database is locked. The time period depends on the volume of data in the production database. For instance, time period for a new database is 5-6 minutes, whereas for a 112-GB database, it is 6 hours and 20 minutes.

Configure the Distributor, Publisher, and Subscriber Servers

You can configure the servers in one of the following ways:

- Run the Configuration Utility (see page 806)
- Manual Configuration (see page 808)

Perform the Validation Check

Perform the checks in Distributor/Publisher based on your configurations.

Follow these steps:

1. Navigate to Microsoft SQL Server Management Studio.
2. Expand **Databases,** and verify the new database "**Distribution**".
3. Expand **Security**, **Logins**, and verify the new login "**Distributor_admin**".
4. Expand **Server Objects**, **Linked Servers**, and verify the new linked server "**repl_distributor**".
5. Expand **SQL Server Agent, Jobs,** and verify the 6 new jobs that are created automatically.
6. Expand **Replication**, **Local Publications,** and verify the newly created publication.
7. Expand the **New Publication,** and verify the newly created subscription.
8. To confirm snapshot creation, right-click on the **Publication** and select **View Snapshot Agent Status.**

Important! Failure in the above steps indicates that the replication process is unsuccessful. In this case, the user must navigate to the log file created as part of replication and check for errors.

Run the Configuration Utility

This section explains the steps to run the configuration utility.

Download the Configuration Utility

For CA Service Management 14.1, apply the patch available on CA Support Online (http://www.ca.com/us/support/ca-support-online/product-content/recommended-reading/technical-document-index/ca-service-management-solutions-patches.aspx) .

Select a Mode

You can choose to either specify the details in the utility or perform a silent replication.

- For the interactive mode process, ensure you review the 'ReplicationInputData.csv' file to comprehend the required input values.
- For the silent replication process, ensure that you specify all the details in the 'ReplicationInputData.*csv*' file before you run the utility.

Run the Configuration Utility

Follow these steps:

1. Unzip the configuration utility file.
2. Run the *CreateReplication.bat* file.
3. Specify if you want to perform a silent replication.
   The replication process starts.
4. If you choose to specify the details in the utility, follow the on-screen instructions.
5. After to you specify all the details, the replication process starts.
   The progress is displayed
6. To understand whether the replication process was successful, view the *Replication.log* file.

Include/Exclude Tables for Replication

During the replication process, the configuration utility replicates only the tables that are part of CA Service Management. Tables that are related to other products are not replicated. For example, if you integrated CA SDM with CA Business Intelligence, the configuration utility replicates only CA SDM tables and not CA Business Intelligence tables. However, you can manually include these tables for replication.

Include a Table for Replication

Follow these steps:

1. In the configuration utility folder, open the **Creation Script** folder.
2. Open the *CreatePublication.sql* file using a text editor.
3. Copy the following code:

```
IF (EXISTS (SELECT * FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME = 'Table_Na
me'))
BEGIN
exec sp_addarticle @publication = N'publication_mdb', @article = N'Table_Name',
@source_owner = N'dbo', @source_object = N'Table_Name', @type = N'logbased',
@description = null, @creation_script = null, @pre_creation_cmd = N'drop',
@schema_option = 0x000000000803509F, @identityrangemanagementoption = N'manual',
@destination_table = N'Table_Name', @destination_owner = N'dbo',
@vertical_partition = N'false', @ins_cmd = N'CALL sp_MSins_dboxent_map',
@del_cmd = N'CALL
sp_MSdel_dboxent_map', @upd_cmd = N'SCALL sp_MSupd_dboxent_map'
END
GO
```

4. Paste the code before the following entry in the file:

```
PRINT 'Publication created'
```

5. Replace 'Table_Name' in the code with the name of the table you want to include.

Exclude a Table for Replication

Follow these steps:

1. In the configuration utility folder, open the **Creation Script** folder.
2. Open the *CreatePublication.sql* file using a text editor.
3. Search for the name of the table and find the following entry. For example, if the name of the table is **xent_map**, you find the following code in the file:

```
IF (EXISTS (SELECT * FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME = 'xent_map
'))
BEGIN
```

```
exec sp_addarticle @publication = N'publication_mdb', @article = N'xent_map',
@source_owner = N'dbo', @source_object = N'xent_map', @type = N'logbased',
@description = null, @creation_script = null, @pre_creation_cmd = N'drop',
@schema_option = 0x000000000803509F, @identityrangemanagementoption = N'manual',
@destination_table = N'xent_map', @destination_owner = N'dbo',
@vertical_partition = N'false', @ins_cmd = N'CALL sp_MSins_dboxent_map',
@del_cmd = N'CALL
sp_MSdel_dboxent_map', @upd_cmd = N'SCALL sp_MSupd_dboxent_map'
END
GO
```

4. Delete the code and save the file.

Manual Configuration

You can manually implement database replication if you do not want to use the utility.

Complete the following steps:

1. Configure Distribution on the Production Database Server (see page 808).
2. Create a Publication on the Production Database using Transactional Replication (see page 809).
3. Update the Publication Properties (see page 812)
4. Configure Subscription on the Reporting Database (see page 814).

Configure Distribution on the Production Database Server

For database replication, you must first configure the distributor. The distributor is the same server as the production database server.

Follow these steps:

1. In Microsoft SQL Server Management Studio, connect to the server that will be the Distributor (in many cases, the Publisher and Distributor are the same server), and then expand the server node.
2. Right-click the **Replication** folder, and then click **Configure Distribution**.
3. In the Distributor pane, select **'<ServerName>' will act as its own Distributor; SQL Server will create a distribution database and log** and click Next.
4. In the **SQL Server Agent Start** pane, select **Yes, configure SQL Server Agent service to start automatically** and click Next.
5. In the **Snapshot Folder** pane, specify a root snapshot folder (for a local Distributor) and click **Next**.
6. In the **Distribution Database** pane, review and edit the information, if necessary, and click **Next**.

7. In the **Publishers** pane, optionally enable other Publishers to use the Distributor, and click **Next**.

8. In the **Wizard Action** pane, select an appropriate action and click **Finish**.

Create a Publication on the Production Database using Transactional Replication

After you configure the distributor, you must create a publication on the publication database. The subscriber or the replication database shall subscribe to the publication for successful data replication.

Follow these steps:

1. In the Microsoft SQL Server Management Studio, connect to the production database server.

2. Expand the **Replication** folder, right-click **Local Publications** and select **New Publication**.

3. In the **Publication Database** pane, select the database you want to replicate and click **Next**.

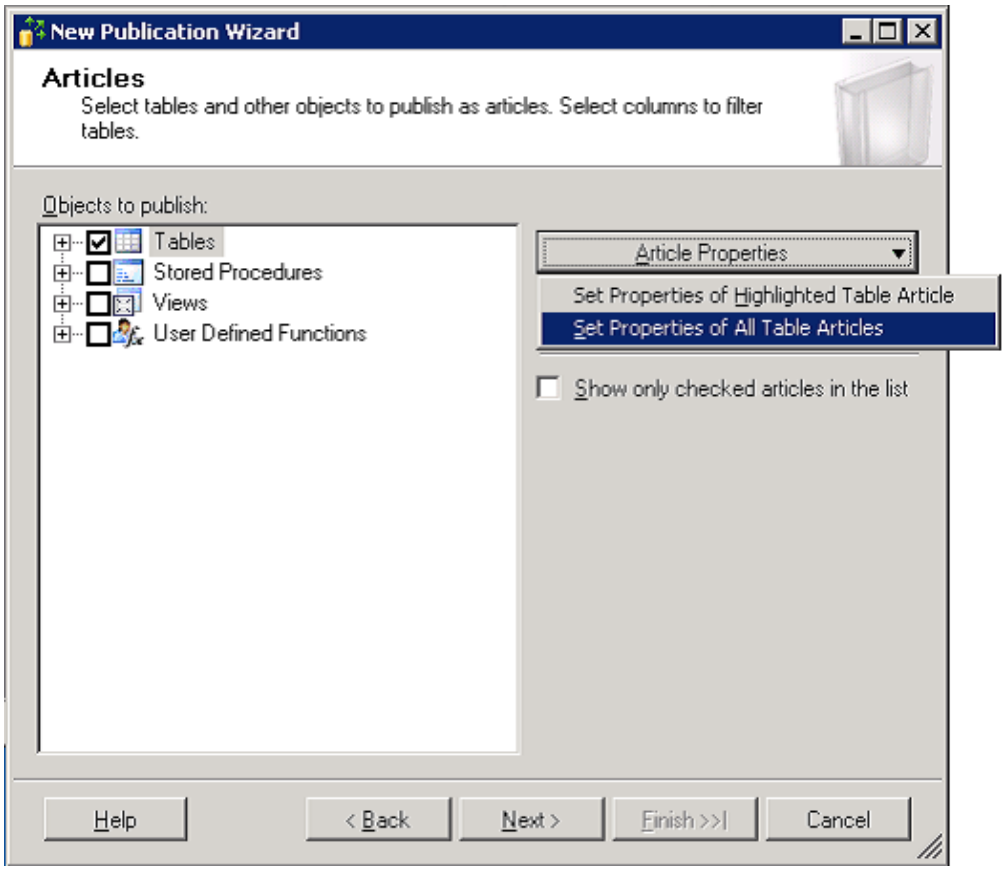
4. In the **Publication Type** pane, under **Publication Type** select **Transactional publication** and click **Next**.

5. In the **Articles** pane, select **Tables**, expand **Tables** and exclude the following entries:

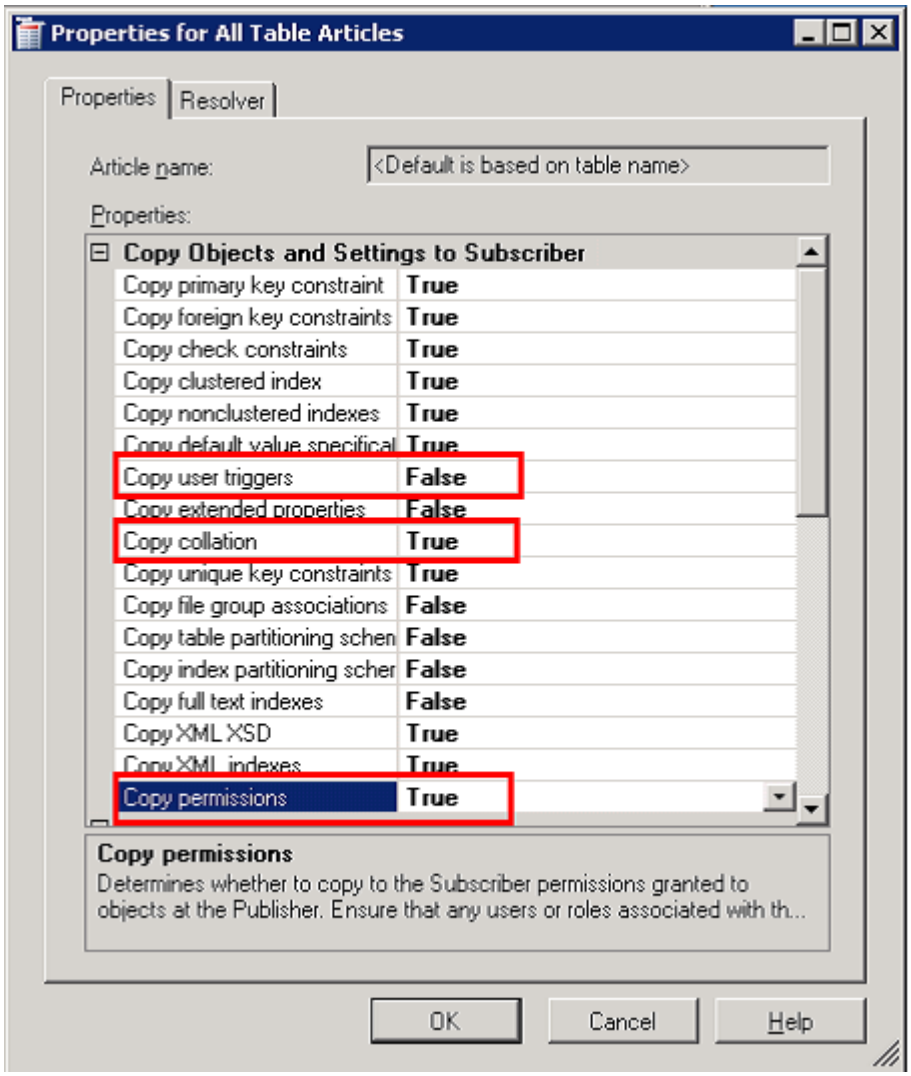
   - ci_twa_ci
   - dlgtsrv
   - ebr_fulltext
   - ebr_fulltext_adm
   - ebr_patterns
   - ebr_properties
   - ebr_synonyms
   - ebr_synonyms_adm
   - options
   - server_types
   - usp_alias
   - usp_bopsid
   - usp_config_daemon_type
   - usp_config_other_daemons
   - usp_configuration

- usp_domsrvr
- usp_interval_log
- usp_mailbox
- usp_record_lock
- usp_servers
- usp_session_ext
- usp_webeng_alias
- usp_webeng_domsrvr
- usp_webengine

6. Click **Article Properties,** select **Set Properties for All Table Articles**.

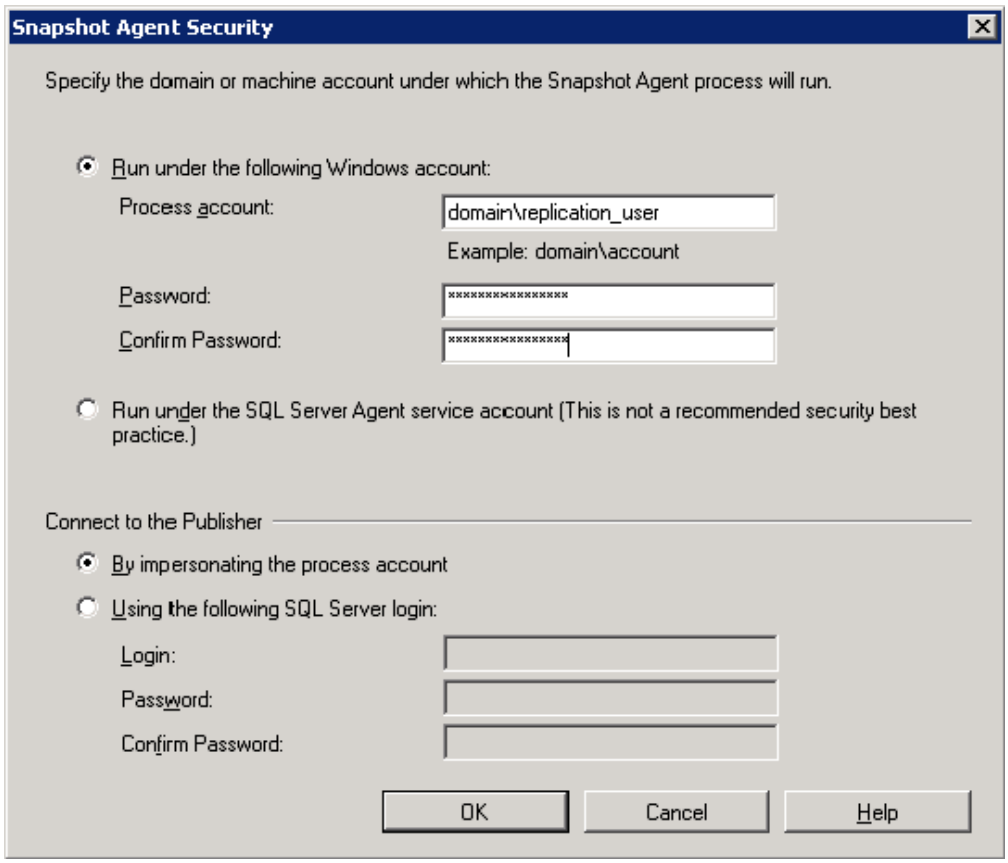


7. In the **Properties for All Table Articles** window, expand **Copy Objects and Settings to Subscriber**.



8. Perform the following steps:
    a. Set **Copy user triggers** to **False**.
    b. Set **Copy collation** to **False**.
    c. Set **Copy permissions** to **True**.
9. Click **OK** and then click **Next**.
10. In the **Filter Table Rows** ensure that you do not add any filters and click **Next**.
11. In the Snapshot Agent page, select **Create a snapshot immediately and keep the snapshot available to initialize subscriptions** and click **Next**.
12. In the **Agent Security** pane, click **Security Settings**.
    The **Snapshot Agent Security** window appears.
13. Select **Run under the following Windows account**, specify the details and click **OK.**

Note: For testing purposes, you can use a local administrator account that has access to the replication snapshot shared folder. Do not change the **Connect to the Publisher** option and retain the default value to impersonate the process account.



14. In the **Agent Security** pane, click **Next**.
15. In the **Wizard Action** pane, select **Create the Publication** and click **Next**.
16. In the Complete the Wizard pane, specify a name for the publication and click **Finish**. The publishing process begins.
17. Update the publication properties (see page).

Update the Publication Properties

Follow these steps:

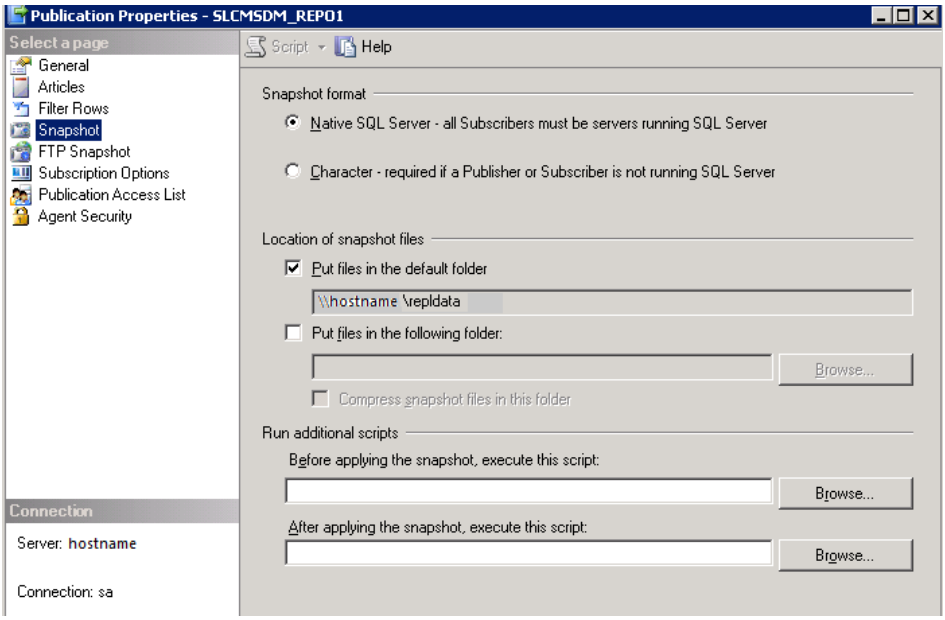
1. In the Microsoft SQL Server Management Studio, connect to the production database server.
2. Expand **Replication, Local Publications**.

3. Right-click the publication that you created and select **Properties.**

> **Note:** If you change a property that requires the regeneration of the snapshot, you are prompted to regenerate the snapshot.

4. In the **Publication Properties** window, complete the following steps:

   a. In the tree on the left, click **Snapshot**.

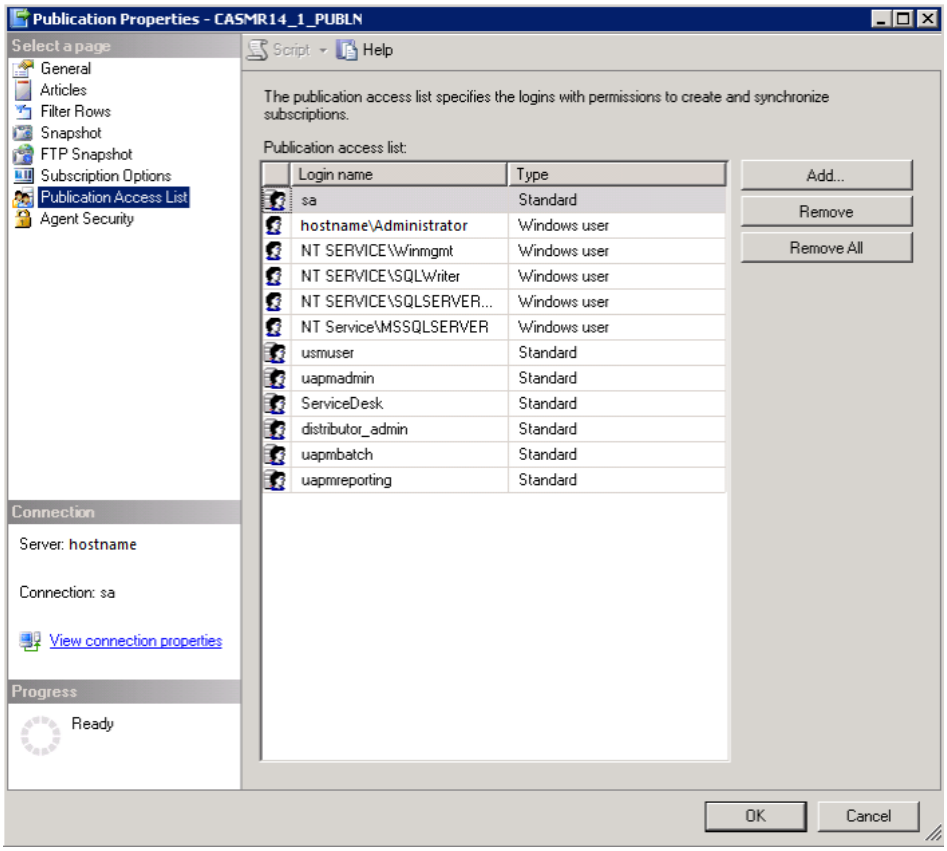


   b. Clear the **Put files in the default folder** check box.

   c. Select the **Put files in the following folder** check box.

   d. Specify the path to the file share.

   e. In the tree on the left, click **Publication Access List**.



f. Click **Add**.

g. In the **Add Publication Access** window add *ServiceDesk, uapmadmin, uapmreporting, usmuser* (and *mdbadmin,* if available) users

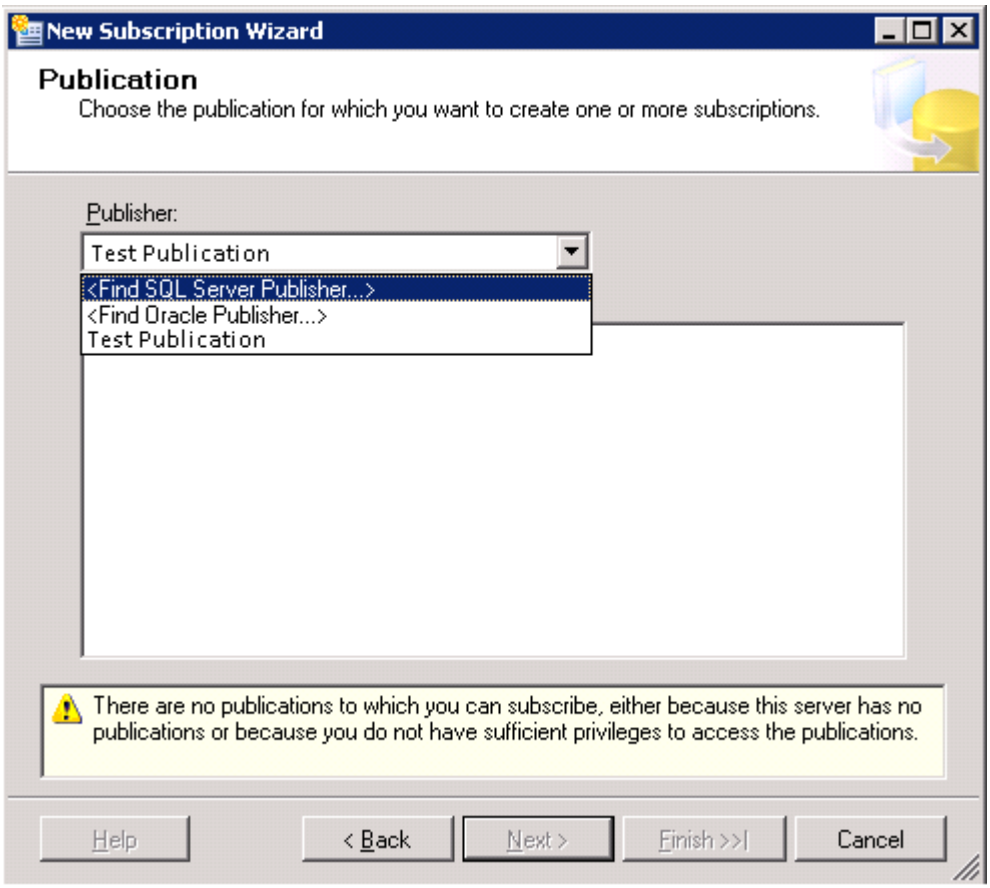
h. Click **OK** and then click **Yes.**

Configure Subscription on the Reporting Database

To replicate the database, the reporting database (subscriber) must subscribe to the specific publication of the publisher database.

Follow these steps:

1. In the Microsoft SQL Server Management Studio, connect to the reporting database server.
2. Expand the **Replication** folder, right-click **Local Subscription** and select **New Subscription.**
3. In the **New Subscription Wizard** window, click **Next**.
4. In the **Publications** pane, click **<Find SQL Server Publisher>** in the **Publisher** drop-down list.



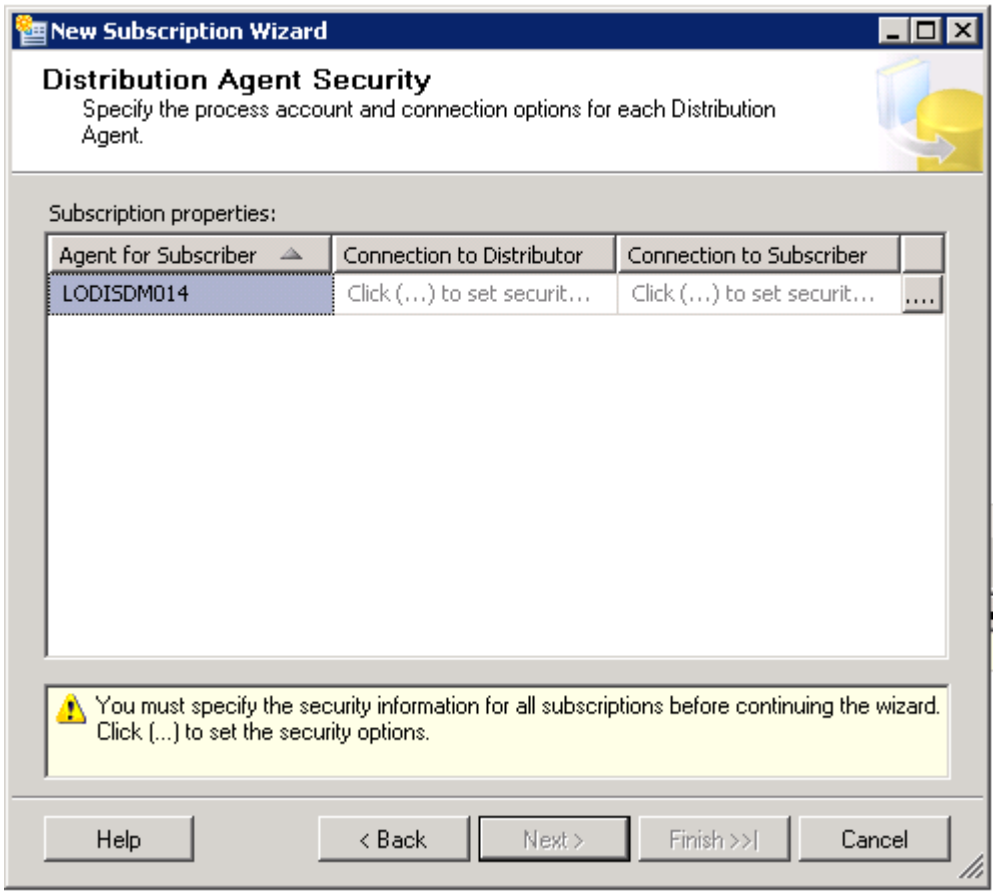
5. Specify the production database and the appropriate details and click **Connect.**
   After successful connection, the **Publication** pane displays all the available publications in the database server.

6. Select the publication that you previously configured and click **Next**.

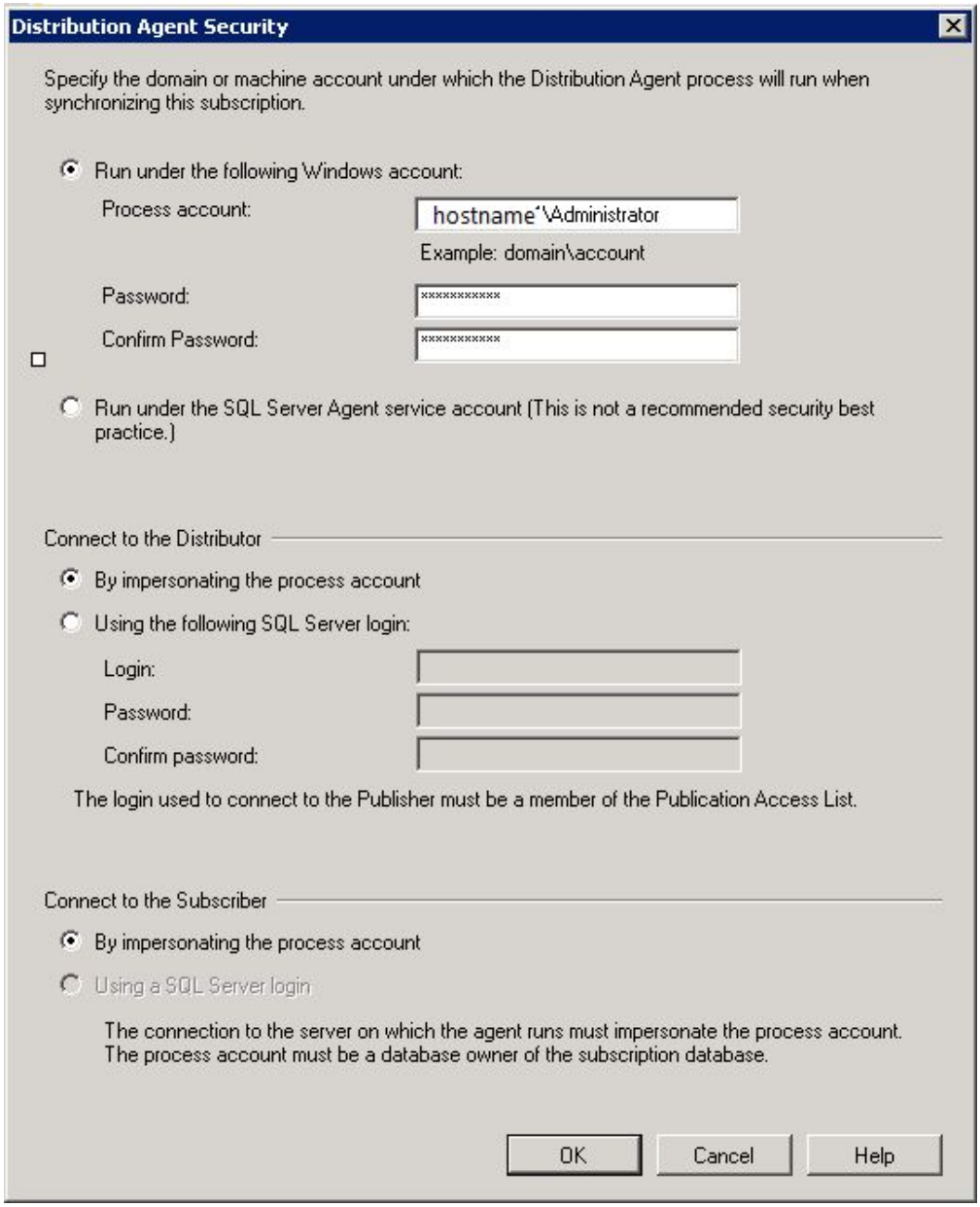
7. In the **Distribution Agent Location** pane, select **Run each agent as its Subscriber (pull subscriptions)** and click **Next**.

8. In the **Subscribers** pane, ensure that **Subscription Database** is **mdb** and click **Next.**

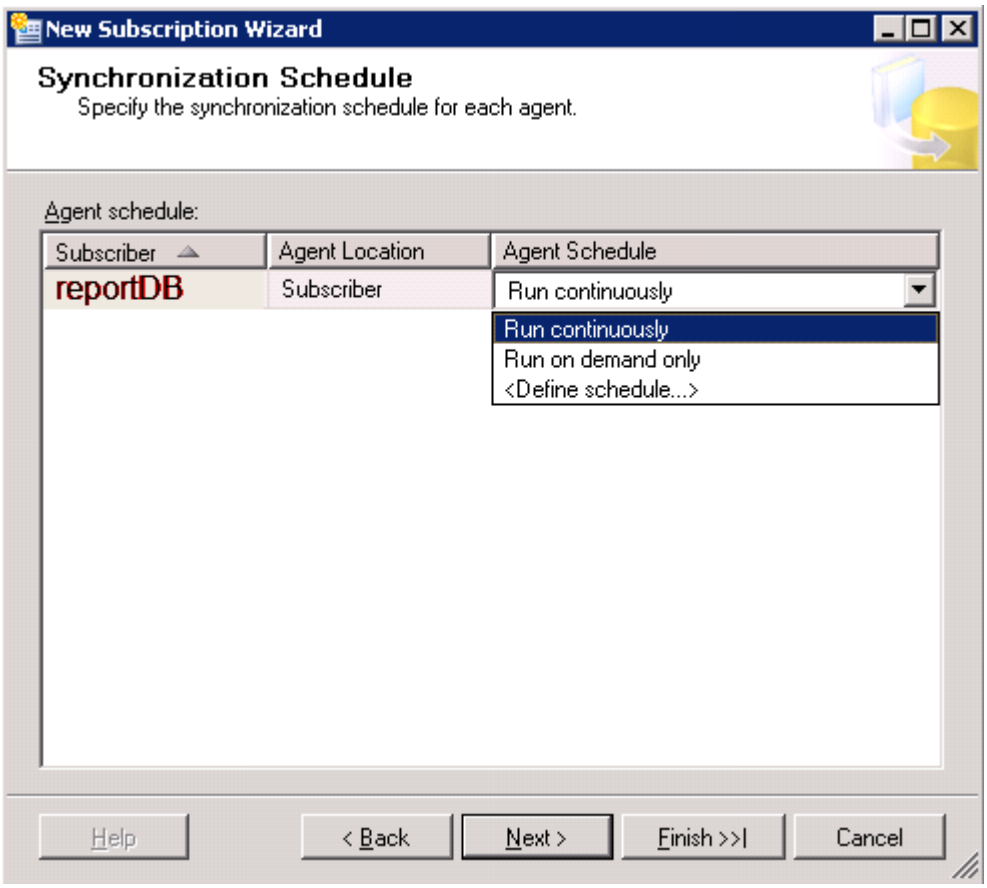
9. In the **Distribution Agent Security** pane, click the button next to **Connection to the Subscriber** .



10. Specify the security credentials for the Subscriber Agent, click **OK,** and click **Next**.



11. In the **Synchronization Schedule** pane, under **Agent Schedule** select **Run continuously**. To schedule the replication process, select **Define Schedule**.



12. In the **Initialize Subscriptions** pane, click **Next**.
13. In the **Wizard Action** pane, select **Create the subscription** and click **Next**.
14. In the **Complete the Wizard** pane, click **Finish**.
15. After the subscription creation process is complete, click **Close**.

Troubleshoot

The following topics explain how to troubleshoot issues:

- Replication Process Fails (see page 818)
- Unable to Copy Data to the Replicated Database (see page 819)

Replication Process Fails

When you run the configuration utility for the database replication, the replication process may fail for several reasons. To know why the replication process failed, you can view the *Replication.log* file available in the **Configuration Utility** folder.

For information about the error messages, refer to Microsoft SQL Server documentation for the respective error message.

After you understand the log messages, run the **DisableReplication.bat** file before you start the replication process again.

If database replication using the configuration utility fails repeatedly, perform the replication process manually. For more information see, Manual Configuration (see page 808).

Unable to Copy Data to the Replicated Database

During replication, some information may not be copied to the subscriber server. Since data is not copied to the replication database, reports are not available.

This is a known issue. See the following Microsoft SQL Server documentation for more information:

http://support.microsoft.com/en-us/kb/956032.

Configuring CA Service Desk Manager

This section contains the following articles:

How to Configure Surveys

This article contains the following topics:

Customer surveys let CA SDM administrators systematically collect and analyze customer feedback about service desk performance. You can modify surveys to suit the needs of your site.

Configure Your System for Surveys

Before you can use surveys, you need to configure your system properly, which involves two steps:

1. Install and configure the CA SDM web interface. When a user accesses the URL for a survey, the web interface formats the survey and populates the survey information.

2. Using the Options Manager, configure and install the web_cgi_url option to specify the location of the CA SDM web engine. For more information, see Install/Uninstall Options Manager Options (see page 1336).

Prepare a Survey

You prepare surveys using the Customer Survey List, which is a typical list window. For example, you can use this window to view all surveys or a subset based on search criteria that you enter; you can create new surveys; you can view details on a particular survey; and you can report on the surveys currently listed.

Each survey has the following features that you can define:

- A name that you can use for searching and reporting purposes
- An introduction that you can use to explain the purpose of the survey to customers
- An ordered list of questions for the customer to answer, each of which includes a set of possible answers
- An optional area where the user can enter free-form comments
- A completion message to display after the user submits the survey

Define Survey Notifications

You can use the Survey tab on the Update Activity Notification page to define a survey notification for an activity notification. When the selected activity notification is triggered, the contact who initiated the activity receives the survey notification. An activity log is generated both when a survey notification is sent and when one is received back from a customer.

Follow these steps:

1. On the Administration tab, browse to Notifications, Activity Notifications.
   The Activity Notification List appears.

2. Select the desired activity notification.
   The detail page displays.

3. Click the Edit button.
   The Update Activity Notification page displays.

4. Edit the fields as appropriate.

5. Select the appropriate object type from the drop-down list.

6. Click the Survey tab.
   This tab contains the following fields:

   - **Send Survey**
     This check box allows you to activate or deactivate the survey. If selected, the survey is sent to the contact when the selected activity notification is triggered.

   - **Default Survey**
     Specify a default survey using the search icon or specify your own in the text box.

   - **Notification Method**
     Choose *one* of the following notification methods:

     - Email

     - Notification

     - Pager_Email

   - **Survey Message Title**
     Enter the title for the survey.

   - **Survey Message Body**
     Enter a message for the contact. When a contact receives notification of a survey, the message body automatically includes a URL that they can access from their web browser to find and fill out the survey form.

7. Save the activity notification.
   When the selected activity notification is triggered, the contact who initiated the activity receives the survey notification.

Survey Reporting

Within CA SDM you can report on surveys from within the administration tab of the web client in all of the usual ways. For example, from the Customer Survey List window, you can choose Reports from the File menu, and then choose a Summary or Detail report. You can also choose Print Form from the various detail windows to print the form data for your surveys, questions, and answers.

You can also fashion your own reports based on the survey data maintained in the CA SDM database.

Create a Managed Survey

The Managed Survey lets the CA SDM administrator select a desired survey sample population and match it to a specific survey. The administrator can then distribute targeted requests for respondents to take the survey at a specific time. This gives the administrator the flexibility of creating open survey periods, while maintaining the ability to have activity-based and category-based surveys related to Requests, Change Orders, and Issues.

The purpose of Managed Surveys is to provide a mechanism for managing surveys. This function can be useful when for survey forms that need to be monitored from time to time (for example, surveys only used during a short period every year or surveys that have been offline too long).

Important! If you want to send the survey to a large number of contacts, set the default value of NX_SURVEY_ILIMIT in NX.env to a higher limit, such as 1073741824.

You can create a managed survey from the Service Desk node on the Administration tab.

Follow these steps:

1. Click the Administration tab.
   The Administration page appears.

2. Click Service Desk, Surveys.
   Click Managed Surveys, Managed Survey List.
   The Managed Survey List appears.

3. Click Create New.
   The Create New Managed Survey page appears.

4. Complete the fields as appropriate.
   See Managed Survey Fields (see page 823) for field descriptions.

5. Use the controls available on the tabs at the bottom of this page to configure the managed survey as appropriate.
   See Managed Survey Tabs (see page 823) for more information.

6. Click Save.
   The managed survey definition is saved and the Managed Survey Detail page appears.

The following buttons are available:

- **Event History**
  Opens the Event History window, which lists the status, time loaded, fire time, and condition for each event associated with the managed survey.

- **Attach Event**
  Opens the Attach Managed Survey Events window, which allows you to attach events with an object type of Managed Survey.

Managed Survey Fields

The following fields require explanation:

- **Name**
  Identifies the title of the managed survey.
- **Managed Survey Status**
  Select *one* of the following options:
- (Default) Survey Period Open
  - Configuration in Progress
  - Survey Cancelled
  - Survey on Hold
  - Survey Period Closed

  You can create a managed survey status from the Service Desk node on the Administration tab.
- **Active**
  Specifies whether the managed survey is active or inactive.
- **Assignee**
  Specifies the contact that is assigned as the survey owner.
- **Group**
  Specifies the group that is associated with the survey.
- **Survey**
  Allows you to search for existing surveys.

Managed Survey Tabs

The following tabs are available on the Create Managed Survey, Managed Survey Detail and Update Managed Survey pages:

- **Activities**
  Allows you to view the Managed Survey Activity Log List. To display only the log entries of interest, you can filter the list by specifying:
  - Earliest Log Date
  - Latest Log Date
  - Activity Type

- Created By

- **Objects**
  Allows you to specify assignee (managed survey owner) or associated groups as notification recipients for the managed survey.

- **Contacts**
  Allows you to specify one or more contacts as notification recipients for the managed survey.

- **Types**
  Allows you to specify one or more contact types as notification recipients for the managed survey (for example, Analyst, Customer, Manager, or Vendor).

- **Initial Message**
  Allows you to view or edit the text for the initial message title and body. Also allows you to specify the notification method for the initial message (for example, e-mail, CA SDM notification, FAXserve, or pager e-mail).

- **Reminder Message**
  Allows you to view or edit the text for the reminder message title and body. Also allows you to specify the notification method for the reminder message (for example, e-mail, CA SDM notification, FAXserve, or pager e-mail).

Create a Survey Template

You can create a survey template from the Service Desk node on the Administration tab.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. Click the Administration tab.

2. Click Service Desk, Surveys, Survey Templates.
   The Customer Survey List appears.

3. Click Create New.
   The Create New Survey page appears.

4. Complete the appropriate fields.
   See Survey Template Fields (see page 825) for field definitions.

Note: The Survey Name field and the Active? dropdown are required.

5. Click Save.
   The template is saved and questions can be added.

6. Click Add Question to specify the question's sequence, comment label, status and question text. Or click Add Answer to open the Survey Answer Template Detail page.

> **Note:** If multi-tenancy is installed, the list page displays a tenant column and a tenant drop-down list in the search filter. Specifying <empty> in the search filter searches for public objects. On detail pages, select the appropriate tenant from the drop-down list. If you select <empty>, the object is public.

Survey Template Fields

The following fields require explanation:

- **Comment Label**
  Indicates the label for the comment text box.

  > **Note:** Use this field when you indicate that you want to include comments in the survey.

- **Active**
  Sets the template to active or inactive.

- **Submit Cycle**
  Indicates to send the survey every 'nth' time.

- **Survey Introduction**
  Shows the introduction text of the selected survey.

- **Survey Completion Message**
  Shows the text when the survey is completed.

- **Include Comments**
  Allows a customer to enter free-form comments by adding a text box to the end of the survey form.

- **Use Stricter Rules?**
  Prevents a user from submitting the same survey more than once.

Notifications

Contents

With CA SDM, you can automatically notify key personnel about ticket activities (researching, escalating) and events (opening a ticket, for example). You can also notify key personnel about Knowledge Report Card (KRC) and Support Automation Assistance Sessions. When a significant activity or event occurs, CA Service Desk Manager creates a notification message that does the following:

- Identifies the ticket activity or the notification event
- References the ticket
- Includes other optional information
- Can identify potential contacts

You can view a notification message for a ticket because of a system action. A system action includes opening, closing, or modifying a ticket through its history information.

Setting up automatic notifications involves the following tasks:

- Defining activity notifications that determine the types of activities that generate notifications.
- Defining object contact notifications that determine the object contacts that can be used to send notifications in an activity notification.
- Identifying the methods used to send messages.

Create Object Contact Notifications

Object contact notifications let you notify the recipients based on the current value of a field on the ticket. Instead of identifying a person to notify, as in a notification method, you identify an object. For example, you can identify the To field to ensure that notification goes to the person currently identified in the To field, even if the value has changed since the ticket was defined.

Follow these steps:

1. Select Notifications, Object Contact Notifications on the Administration tab.
   The Object Contact Notification List page opens.

2. Click Create New.
   The Create New Object Contact Notification page opens.

3. Complete the following fields:

   - **Symbol**
     Defines a unique identifier for the object contact notification.

   - **Status**
     Specifies if the object contact notification is active or inactive.

   - **Object Type**
     Displays the name of the object to which the attribute applies.

   - **Object Attribute Name**
     Provides the name of the object contact notification (in the Symbol field) in Majic, which is internal CA code. The attribute name depends on the Object Type selection:

     - If the Object Type is Issue or Workflow Task, the attribute name is assignee, requester, or group; these are the attribute names in the chg objects and they map to fields in the Change_Request tables.

     - If the Object Type is an Issue Activity log, the attribute name must start with the attribute name in the activity log object that links it to a specific instantiation of the chg object. The attribute name could be change_id.group.

   - **Description**
     Describes the object contact notification.

4. Click Save.
   The new object contact notification is displayed in the Object Contact Notification List.

Previous Assignee Notifications

You can define Previous Assignee or Group values for an activity notification that detects changes to key fields when a ticket is saved. Previous values let you notify a previous assignee when a ticket is transferred, or notify both the current and previous groups when the priority of a ticket is escalated.

The Previous value fields of a ticket are local fields that exist only in memory and not in the database. The fields are populated during the save operation of the ticket only when respective attributes are changed and cleared at the completion of the notification processing. A previous value field is associated with a particular activity type through an activity association.

You can define Previous values that detect changes to the following key fields of a ticket:

Field	Requests, Incidents, Problems	Change Orders	Issues
Status	Yes	Yes	Yes
Active	Yes	Yes	Yes

Field	Requests, Incidents, Problems	Change Orders	Issues
Assignee	Yes	Yes	Yes
Request Area/Category	Yes	Yes	Yes
Group	Yes	Yes	Yes
Impact	Yes	Yes	Yes
Priority	Yes	Yes	Yes
Urgency	Yes	No	No
Severity	Yes	No	No

There are several contacts that you can specify for each object type (request, incident, problem, change order, or issue), which notify the current and previous contacts when an activity occurs.

- **Assignee** -- Person assigned to handle the ticket.
- **Assignee Previous** -- Person previously assigned to handle the ticket.
- **Group** -- Group assigned to handle the ticket.
- **Group Previous** -- Group previously assigned to handle the ticket.

After the notification rule is saved, the Assignee Previous and Group Previous fields display on the Object Contact Notifications List page.

Example: Configure Current and Previous Values for Key Fields

The following usage example describes how an administrator configures current and previous values for key fields to help ensure that the previous support representative is notified when a request is transferred away from them.

1. **Situation --** A support representative is frustrated because a ticket was transferred away from them and they were never notified.
2. **Task --** The administrator adds the Assignee and Assignee Previous object contacts to the notification rule for the Transfer activity notification. They attach a message template and specify the current and previous assignees to notify on the request form.
3. **Action --** When the request is saved, the Assignee and Assignee Previous fields of the request are populated. When the activity occurs (ticket is transferred), the condition for the rule is evaluated.
4. **Result --** If the condition is met, a notification message that describes the ticket activity is sent to the current assignee and the previous assignee.

Notify Contacts When a Ticket is Transferred Example

You can notify both the current and previous contacts when a CA SDM ticket is transferred.

Example: Notify both the current and previous contacts when a ticket is transferred

1. On the Administration tab, browse to Notifications, Activity Notifications.
   The Activity Notifications List page appears.

2. Select the Transfer activity notification.
   The Transfer Activity Notification Detail page appears.

3. In the Object Type field, select Requests/Incidents/Problems.

4. On the Notification Rules tab, under Symbol, select the Default Transfer Notification Rule.
   The Default Transfer Notification Rule page appears.

5. On the Object Contacts tab, click Update Object Contacts.

6. Click Search.
   The Notification Rule Update Recipients page appears.

7. From the Object Contacts list, select Assignee and Assignee Previous from the list on the left, and click the contact selection button (>>).
   The selected item is added to the list on the right.

   Note: Use the CTRL or SHIFT keys plus the left mouse button to select multiple object contacts.

8. Click OK.

9. Save the notification rule.
   The Object Contacts list displays the selected object contact.

10. On the Default Transfer Notification Rule page, click Message Template. Select a template and ensure that the Auto Notification option is enabled.

11. Create a request, specify an Assignee, and click Save.

12. On the Request Detail page, select Activities, and Transfer from the File menu.

13. Specify a new Assignee, and click Save.
    The notification is sent to the current and previous assignees when the transfer activity occurs.

Configuration Item Notifications

A configuration item (CI) notification lets you define an activity notification that is associated with a specific CI that is associated with a specific CA SDM ticket. This feature lets you track information about the users, organizations, and vendors of a CI. You can specify the CI object contacts on the Notification Rules Update Recipients page, such as CI Maint Org, CI Primary Contact, and so on.

Notify the Primary Contact of a Configuration Item for an Issue Example

You can define an activity notification for a primary contact that are sent for a specific CI for a specific CA SDM ticket.

Example: Notify the primary contact of a configuration item for an issue

1. On the Administration tab, browse to Notifications, Activity Notifications.
   The Activity Notification List page appears.

2. Select the Initial Activity Notification from the list.
   The Initial Activity Notification Detail page appears.

3. Select the object type you want to use.

4. On the Notification Rules tab, select the Default Notification Rule link.
   The Default Notification Rule page appears.

5. Select the Default Message Template link and ensure that the Auto Notification option is enabled.

6. Select the Object Contacts tab, and click Update Object Contacts.
   The Object Contact Notification Search page appears.

7. Click Search. A list of object contacts appears.

8. Select CI's Primary Contact from the list on the left, and click the contact selection button (>>).
   The selected item is added to the list on the right.
   You can use the CTRL or SHIFT keys plus the left mouse button to select multiple object contacts. You can add one object for a request and multiple objects for a change order or issue.
   The object contact is in the list on the right.

9. Click OK.

10. Save the notification rule.
    The Object Contacts list displays the selected object contact.

11. Complete the following tasks:

    - On the Service Desk tab, create or update an existing CI.

    - Add the primary contact listed on the Object Contacts tab. The selected object contact appears on the Configuration Items Detail page.

    - Add the CI to the Issue.

When an activity event occurs, the rule is implemented and the condition is evaluated. If the criteria for the condition is met, a notification message that describes the ticket activity is sent to all contacts of the CI associated with this notification rule.

Notification Log Reader

The Notification Log Reader displays the notifications received for the logged-in user by date, urgency, and status. With the Notification Log Reader, you can do the following:

- Change the sort order and set menu options to have the Notification Log Reader appear automatically when new messages are received.
- Double-click a notification message to request that CA SDM display the detail page for the ticket associated with the notification.
- Monitor notification messages by entering specific selection criteria to query the database for analysis or for selection of notification messages based on data entered in the fields. For example, you can list only those notification messages that have not been cleared by changing the Message Status field to Not Cleared.
- Clear notification messages to keep your list of notifications to a manageable size. Cleared notifications are not displayed when you first access the Notification Log Reader, although you can display them, if needed.

Set Notification Log Reader Options

You can set options for the Notification Log Reader to define how you are notified when new messages are received for an issue.

Follow these steps:

1. On the ServiceDesk tab, browse to View, Log Reader.
   The Notification Log Reader page appears.
2. Use the check box to the left of each notification to set the following options. You can select items to perform operations such as Clear Selected or Delete Selected.
   - **Header**
     Displays the header of the message, which usually contains the number of the ticket and the activity type.
   - **Start Date**
     Displays the date and time the notification was sent to your Log Reader window.
   - **Status**
     Displays the status of the notification.
   - **Urgency**
     Defines the level of urgency for the notification (low, normal, high, or emergency), which indicates the relative importance of different activities. Urgency levels are predefined; however, the system administrator is responsible for setting up other aspects of notification, such as notification methods and activity associations. The system administrator also defines the method of notification used for contacts and groups for each urgency level.

- **Message Text**
  The full message text for the notification.

The Log Reader displays any changes.

3. Click Close.
   The Notification Log Reader page closes and the options are set.

Personalized Responses

You can create personalized responses and attach them to requests, issues, and change order records when adding activities to the record. For example, you can append a personalized response on the Status Change or Log Comment windows available from the Activities menu.

Create a Personalized Response

You can create a personalized response to append to requests, issues, and change order records.

Follow these steps:

1. From the Administration tab, navigate to Service Desk, Personal Responses.
   The Personal Response list page displays.

2. Click Create New.
   The Create New Personalized Response page displays.

3. Complete the fields on the page:

   - **Response Owner**
     Specifies the contact who owns the response. If this field is left blank, the response is available to all analysts.

   - **Response**
     Specifies the text delivered to all those who receive this response. This field can be up to 1000 characters long.
     You can use variables in this field, for example:

```
Ticket ref_num: @{call_req_id.ref_num}

Assignee: @{call_req_id.assignee.combo_name}

Customer: @{call_req_id.customer.combo_name}

Description: @{call_req_id.description}
```

4. Select the type of records for which you want this response available. Click Save.
   A personalized response is created.

Personalized Response Variable Substitution

Variables can be embedded in the text of a Personal Response. These variables allow information to be substituted from the corresponding Request, Change Order, Issue, Problem or Incident. The syntax of the variables is the same as is used elsewhere in the CA SDM product, such as in the Activity Notification Message Templates and the Manual Notify Activity Message Text. The information can

only be substituted from the corresponding Request, Change Order, Issue, Problem or Incident. Activity Notification Message Templates and the Manual Notify Activity Message Text allow information from the Activity Log Record to be included as well.

Check boxes for each object type (Requests, Change Orders, Issues, Incidents, and Problems) allow Responses to be filtered during selection. If the object type is not checked, the Response is not available for that object. For example, if only the Request box is checked, the Response is only presented in Activities for a Request.

A single Response can be used for all object types (Requests, Change Orders, Issues, Problems or Incidents). Because each object has different attributes, information that does not apply to the object is not substituted (for example, attempting to substitute the Request Number in a Response for an Issue).

A Response text example and the variable substitutions that occur for each object type follows:

```
This is Request # '@{call_req_id.ref_num}'
This is Change Order #' '@{change_id.chg_ref_num}'
This is Issue # '@{issue_id.ref_num}'
```

For a *Request*, the following substitution occurs:

```
This is Request # 'cr_demo:11'
This is Change Order # "
This is Issue # "
```

For a *Change Order*, the following substitution occurs:

```
This is Request # "
This is Change Order # 'chg_demo:3'
This is Issue # "
```

For an *Issue*, the following substitution occurs:

```
This is Request # "
This is Change Order # "
This is Issue # 'iss_demo:6'
```

By using the "Display this Response for" check boxes, you can create different versions of a Response with the appropriate substitution variables for the corresponding object (Requests, Change Orders, Issues, Problems or Incidents).

The format of the substitution variables for the different objects is as follows.

Object	Variable Format
Request / Incident / Problem	@{call_req_id.attr}
Change Order	@{change_id.attr}
Issue	@{issue_id.attr}

The substitution occurs when the Response is copied to the User Description field. The Response is copied after it is selected from the Personalized Response drop-down list and the drop-down list loses focus.

Internal Logs

You can define whether a particular access type is qualified to view internal logs. If allowed to view internal logs, contacts see a check box labeled Internal on each of the Log Activity windows, which they can select to mark the activity as internal. When activities are marked as internal, only contacts with an access type that is qualified to view internal logs sees the activity or is notified of it.

View the Log Reader

The Log Reader lists the notifications that are received for the logged-in user. You can filter the list by clicking Show Filter and specifying search criteria in the search fields. From the menu select View, Log Reader.

If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

View Notification History

You can see the notification history for the currently logged in user (from the main CA SDM page or a list page, select View, Notification History) , or for the currently open ticket record (select View, Notification History on the menu bar)

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

View Response Time Statistics

You can monitor the response time of your system to evaluate performance issues. Choose View, Response Time Statistics.

Create a Notification Method

A notification method lets you inform people when an activity that affects a ticket takes place. You can assign different notification methods for different notification levels (low, medium, high, or emergency).

Follow these steps:

1. Select Notifications, Notification Methods on the Administration tab.
   The Notification Method List page opens.

2. Click Create New.
   The Create New Notification Method page opens. Complete the following fields, as appropriate:

   - **Symbol**
     Defines a unique identifier for this record.

   - **Write to File**
     Specifies if the context information of the notification method is written to a file. If you select this option, the TEMP (Windows) or TMP (UNIX) environment variable determines the directory used for creating notification files. The environment used depends on who started the CA SDM services. On Windows, for example, configure the System Variables environment and specify TEMP if it is not already defined. If the system cannot find the environment variable, notification files are written to the root directory of the default drive.

   - **Supports SMTP**
     Specifies that SMTP addresses are supported for email recipients.

   - **Record Status**
     Specifies if the database record is active or inactive.

   - **Description**
     Gives a description of the notification method.

   - **Notification Method**
     Shows the name (including the path if it is required) of the program or executable script that runs, and any applicable switches. For example: Launchit c:\\backup\\applog.bat or pdm_mail -p.

     Note: Because the notification method runs from the CA SDM server, put the notification method script in a directory that can be accessed from the path on the server. Alternatively, specify the full path to the script. On UNIX, depending on the shell you are running, you can check the path by executing which pathname_to_script command.

     Out of the box, the following Notification Methods are provided:

     - Email
     - Notification
     - Pager_Email
     - xMatters/Email
     - xMatters/Notification

- xMatters/Pager_Email

> **Note:** CA SDM supports only one notification method at a time. If you are using Email, then you cannot use Notification at the same time. This applies to all out of the box notification methods like Email, Notification, Pager_Email, xMatters /Email, xMatters/Notification, and xMatters/Pager_Email. When xMatters integration is disabled, the Notification Method must be manually reset to either Email, Notification, or Pager_Email.

Select one of the notification method from the Low, Normal, High, or Emergency drop-down list. When xMatters is integrated, select Notification Method as **xMatters/Email**. It indicates that the notification will be sent to the xMatters agent for incidents, requests, or problems. CA SDM objects like Change Orders, Issues, or Knowledge Documents are processed using the Email notification method.

3. Click Save.
   The notification method is defined and the Notification Method Detail page appears. If there appears to be a problem with the notification methods, examine the logs. The logs are in the $NX_ROOT/log directory on UNIX or $NX_ROOT\log on Windows.

Create a Notification Rule

This article contains the following topics:

Create the notification rule to specify the contacts to be notified and under what circumstances.

> **Note:** If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

> **Note:** The "Document about to expire" activity notification is activated seven days before the actual expiration date that displays in the knowledge document.

Follow these steps:

1. Select Notifications, Notification Rules from the Administration tab.
   The Notification Rule List page opens.

2. Click Create New.
   The Create New Notification Rule page opens.

3. Complete the following fields:

- **Symbol**
  Defines a unique identifier for this notification rule. For example, enter Ticket Description Update.

- **Object Type**
  Defines the object to which the rule applies. For example, select Request/ Incident/ Problem for an activity related to a ticket.

4. Click Save & Continue.

5. Click Condition to select the macro you can use to define a condition for this rule. Do one of the following actions to define the condition:

   Note: A notification rule without a condition notifies all contacts every time the activity occurs.

   - Search for the macro from the list and select it.

   - Click Create New to create a macro.

6. Click Message Template to add a message template that you have created for this rule. Do one of the following:

   - Search for the template from the list and select it.

   - Click Create New to create a message template.

7. Choose the appropriate contacts to notify from the following tabs:

   Note: Use the Update Contacts button that appears on each tab to search for and select more contacts to notify.

   - **Object Contacts**
     Displays the available organizations, vendors, and configuration items for the selected Object type that receive notification about tickets. For example, you can select Affected End User or Affected End User's Admin Org to notify.

   - **Contacts**
     Displays the individuals who are added to the notification rule, regardless of their association with the ticket.

   - **Contact Types**
     Displays the users who are defined within the notification rule with the same classification, such as analyst or customer.

8. Click Save.
   The notification rule is created.

Example Notify the Current and Previous Assignees

You can configure previous values for an activity notification that detects changes to key fields when a ticket is saved. Using previous values, you can notify both the current and previous assignee when a ticket is transferred, and much more.

Follow these steps:

1. Open the Transfer activity notification.
   The Transfer Activity Notification Detail page opens.

2. Verify the following fields are set to the following values:

   - **Object**: Requests/Incidents/Problems.

   - **Notification Rules**: Default Transfer Notification Rule for request/incident/problem

3. Click Default Transfer Notification Rule for request/incident/problem rule.
   The Default Transfer Notification Rule for request/incident/problem Notification Rule Detail page opens.

4. Verify that the Auto Notification option is enabled on the Default Transfer message template for request/incident/problem template.

   Note: The Auto Notification check box sends the notification associated with this template automatically when the activity occurs. For example, you set up an initial notification, set up the objects to notify, and set up the message template, but you are not ready to turn on the notifications. In this case, you do not select Auto Notification. When you are ready to start automatic notifications, you select the check box. The notification becomes active and occurs as defined.

5. On the Object Contacts tab, click Update Object Contacts.
   The Object Contact Notification Search page opens.

6. Click Search.
   The Notification Recipients - Update page opens.

7. From the Object Contacts list, select Assignee and Assignee Previous and click the move button (>>).
   The selected items are added to the list on the right.

   Note: Use the CTRL or SHIFT keys plus the left mouse button to select multiple object contacts.

8. When the object contacts are in the list on the right, click OK.

9. Click Close Window.
   The Object Contacts list displays the selected object contacts.

10. Complete the following steps to test this notification:

    a. Create a request, specify an assignee, and save the request.

    b. On the Request Detail page, select Activities, Transfer. Specify a new assignee and save the request.

    The notification is sent to both the current and previous assignees when the ticket is transferred.

Example Notify the Primary Contact of a CI/Asset

You can define a notification rule for an activity notification that is sent for a specific configuration item associated with a service desk ticket. These notifications let you notify the person responsible for maintaining the configuration item when a request, problem, incident, change order, or issue is created.

Follow these steps:

1. Open the Initian activity notification.
   The Initial Activity Notification Detail page opens.

2. Verify the following fields are set to the following values:

   - **Object**: Requests/Incidents/Problems.

   - **Notification Rule**: Default initial Notification Rule for request/incident/problem

3. Click Default initial Notification Rule for request/incident/problem.
   The Default initial Notification Rule for request/incident/problem Notification Rule Detail page opens.

4. Verify that the Auto Notification option is enabled on the Default initial message template for request/incident/problem template.

   Note: The Auto Notification check box sends the notification associated with this template automatically when the activity occurs. For example, you set up an initial notification, set up the objects to notify, and set up the message template, but you are not ready to turn on the notifications. In this case, you do not select Auto Notification. When you are ready to start automatic notifications, you select the check box. The notification becomes active and occurs as defined.

5. On the Object Contacts tab, click Update Object Contacts.
   The Object Contact Notification Search page opens.

6. Click Search.
   The Notification Recipients - Update page opens.

7. Select the Primary Contact of the CI from the list on the left and click the move button {>>).
   The selected items are added to the list on the right.

   Note: Use the CTRL or SHIFT keys plus the left mouse button to select multiple object contacts.

8. When the object contacts are in the list on the right, click OK.

9. Click Close Window.
   The Object Contacts list displays the selected object contacts.

10. Complete the following steps to test this notification:

    a. On the Service Desk tab, create or update an existing CI.

    b. Add the primary contact listed on the Object Contacts tab. The selected object contact appears on the Configuration Items Detail page.

    c. Add the CI to the Issue.

    When the activity occurs, a notification message that describes the ticket activity is sent to the contact responsible for the CI.

Create Message Templates

Create a message template that contains the values to use for the notification message. When you send multiple notification messages, you can use the message templates to simplify your workload.

Follow these steps:

1. Select Notifications, Message Templates from the Administration tab.
   The Message Template List page opens.

2. Click Create New.
   The Create New Message Template page opens.

3. Complete the fields as appropriate.

   - **Symbol**
     Defines a unique identifier for this message template.

   - **Object Type**
     Specifies the object type associated with this template. For example, select Request/ Incident/ Problem for any notification related to a ticket.

- **Record Status**
  Specifies the status of the template as either active or inactive. Set the status to Active to use the message template.

- **Auto Notification**
  Specifies to send the notification associated with this template automatically, when the activity occurs. For example, you set up an initial notification, set up the objects to notify, and set up the message template, but you are not ready to turn on the notifications. In this case, you do not select Auto Notification. When you are ready to start automatic notifications, you select the check box. The notification becomes active and occurs as defined.

- **Notify Level**
  Indicates the relative importance of sending this notification. For example, select Emergency if you want to send the email notification to the contact immediately when the associated activity occurs.

- **Notification Message Title**
  Specifies the summary title of the message. You can use variables to insert the incident number in the message title. For example, @{call_req_id.type.sym} @{call_req_id. ref_num} @{type.sym}.

- **Notification Message Body**
  Specifies the content of the message. You can use variables to insert the analyst name, end-user name, and description into the message. For example,

```
@{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}.

Assigned to: @{call_req_id.assignee.combo_name}

Customer: @{call_req_id.customer.combo_name}

Description: @{call_req_id.description}


Click on the following URL to view:

@{call_req_id.web_url}
```

  You can use the ARTIFACT keyword to specify how artifacts are handled in outbound messages, message templates, notifications, and auto-replies. The ARTIFACT keyword uses the following values:

  - **NONE** -- Specifies no validation of artifacts. This value is the same as not using the keyword.

  - **PROTECTED** -- Validates a ticket against the hash for confirmation. If confirmation fails, the artifact is considered invalid and filtering fails when filtering searching for an artifact ({{object_id}}).

  - **SECURE** -- Decrypts the ticket number. If the value is not a valid password, the artifact is considered invalid and filtering fails when filtering is searching for an artifact ({{object_id}}).

- **HTML Message**
  Specifies the HTML message that is displayed to the recipient. If the recipient receives the message on an external device, such as a cell phone or PDA, the message displays in plain text only. Click Edit HTML Message to open the HTML Editor.

- **Quick View**
  Displays the message as it appears to the recipient.

- **HTML Source**
  Displays the message in the HTML source code.

4. Click Save.
   The message template is created.

Create a Manual Notification

You can define a manual activity notification that is sent for a specific activity. An activity is an action that someone performs, such as resolving a service desk ticket or sending a managed survey. Even daily activities such as returning a call, canceling or closing a record, increasing priority, or updating status can result in a notification being sent.

Manual notifications let you do the following activities:

- Use temporary email addresses
- Add default users to manual notifications
- Show in an email notification all other recipients of the notification
- Process the outgoing email queue after a server error that leaves emails in the queue
- Notify the attached Object Contacts, Contacts, and Contact Types

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Service Desk tab, select one of the following:
   - Incident from the Incident List page
   - Problem from the Problem List page
   - Request from the Request List page
   - Change order from the Change Order List page
   - Issue from the Issue List page

2. Select Activities, Manual Notify on the menu bar.

   The Manual Notification page appears.

3. Add the recipients of the notification in the To or Cc fields. The following fields enable you to add the recipients:

   Note: This feature will only be available if you apply a patch for CA Service Management Release 14.1.01. Find the patch and the download details from CA Support Online.

   Important! You cannot add the same recipient in both To and Cc fields.

   Note: The option to add recipients in the To and Cc list can be enabled if you install the **mail_show_to_cc_list** option from the Options Manager. If you disable the option, you can add recipients in the To list only**.** This option shows all the recipients of the email notification. For manual email notification, both To and Cc list recipients are displayed and for automatic email notification, only To list recipients are displayed. Pager email notification method does not support the listing of all the recipients in To or CC list.

   - **Available Recipients:** Lists relevant contacts and Contact Objects that you can add to the Recipients list, as specified in the Manual Notify settings in Activity Notifications options. When you select a contact object name, only the contact names that are associated with the object are added to the Recipients list. After selecting the recipient(s), click **Add To Recipients** (required) or click **Add Cc Recipients** (optional). The selected recipient(s) appear (s) on the respective Selected Recipient list.

   - **Contact:** Enter characters into the contact field of the ticket. The field displays results as you type and generates a list of suggested results. After selecting the contacts, click **Add To Contact** (required) or click **Add Cc Contact** (optional). The selected contact appears on the respective Selected Recipient list.

   - **Email address:** Accepts an SMTP address for an email recipient. You can specify any valid email address including addresses that are not associated with a contact record. Separate multiple addresses with a semi-colon. This field appears when the option notification_allow_temp_address is installed using Options Manager. After selecting the email address, click **Add To Email** (required) or click **Add Cc Email** (optional). The selected email address appears on the respective Selected Recipient list.

4. Complete the following fields, as appropriate:

- **Urgency:** Specifies the relative importance of the notification (by default: low, normal, high, or emergency). The system administrator defines the Urgency levels.
- **Preferred Method:** Specifies the notification method to use, such as Email or Notification.

  Note: When you specify an email address, set the method to one that supports SMTP, otherwise, remove email addresses from the Selected Recipients list.

- **Internal:** Makes the notification visible to internal contacts only.
- **Message Title** : Specifies a title for the notification message. This title is a short description of the message, similar to an email subject line. The default title is the ticket type and number, and the words "Manual Notify" (for example, "Incident 32 Manual Notify").
- **Message Text:** Specifies the entire text of the notification. You can click Spelling to check the spelling of the message text.
- **Personalized Response:** Specifies a personalized response such as a generic or administrator signature. The response is added to the end of the message text.

  Note: The administrator must set up a personalized response before you can use this option. For more information about personalized responses, see Personalized Response (see page 2316)

5. You can send documents or URLs to the selected recipients, if you have selected the **Email** method and if you have installed the **mail_allow_attmnts** option.

   Note: This feature will only be available if you apply a patch for CA Service Management Release 14.1.01. Find the patch and the download details from CA Support Online.

   Ensure that you read the following considerations before using this feature:

   - Attachment repository used for storing manual notification attachments should be configured to match the sender and receiver email server restrictions in terms of file size and extensions. There is no separate repository to store the attachments. As an Administrator, you may need to add extra validations to match Exchange limitations.
   - Mailer daemon needs to be explicitly configured to use SSL (use the options manager) if encryption is needed.
   - The SOAP web services method **notifyContact** does not support this functionality.
   - Based on the size of the attachments, emails with many attachments may slightly degrade the performance of sending emails.

- No changes are made to the mobile interface as Manual Notify is not supported from the mobile interface.
- CA SDM does not handle bounce emails and emails failed to be delivered by the mail server.
- Email attachments are not encrypted.
- CA SDM is not responsible for language differences in the email content. An email in Portuguese can be sent to the English supported device.
- CA SDM does not have the mechanism to detect if huge (number/size) emails are sent. Ensure that you check the email size at the firewall level.
- The attachments can be sent to CA SDM contacts, and to the contacts that are not created in CA SDM (using email addresses directly). CA SDM will not take responsibility of the following:
  - attachments being forwarded to other contacts.
  - attachments may contain virus or malware content in the files.
  - attachments may contain sensitive information (such as personal information)
- If an Analyst sends the same attachment as part of two different manual notify activities, then, there would be duplicate attachments created and linked to the cr object. Ensure that you check before uploading any attachment.

To upload the documents or URLs, click **Attach Documents** or **Attach URLs** from the **Attachments** tab and follow the on-screen instructions. After you upload, the URL or the document is listed on the tab.

6. Click Notify.
   The notification is sent and the activity is recorded on the Activities tab.

How to Set Up Notification for an Activity

You can define a notification that is sent for a specific activity. An activity is an action that someone performs, such as resolving a ticket, sending a managed survey, running the Knowledge Report Card. Even daily activities such as returning a call, canceling or closing a record, increasing priority, or updating status are activities that can result in a notification being sent.

Follow these steps:

1. Open the CA SDM Web UI (see page).
2. Verify the Prerequisites (see page 846).
3. If you do not want to use a predefined message template, Create a Message Template (see page 848).
4. If you do not want to use a predefined notification rule, Create a Notification Rule (see page 849).

5. If you do not want to use a predefined activity association, Create an Activity Association (see page 851).

6. If you do not want to use a predefined activity notification, Create an Activity Notification (see page 852).

Open CA SDM Web UI

Log in to the web UI from the following servers, depending on your CA SDM configuration:

- Conventional: Primary or secondary servers
- Advanced availability: Application or background servers

Verify the Prerequisites

Verify the following prerequisites, before you being the setup:

- Installed the option to add URL in the notification (see page 846).
- Verified the notification method for the recipient (see page 846).
- If you want to send a manual notification to an email address that is not associated with a contact, allow temporary email address (see page 847).

Install the Option to Add URL Hyperlinks to Notifications

The web_url field in the Change_Request and Workflow_Task tables holds a URL value that allows a user to access a particular change order or workflow task through the web interface. When used in email notifications, a user can click the URL and can go to the web interface without any further querying.

Before you can implement the URL hyperlinks in notifications, configure the system as follows:

1. Install and configure the CA SDM web interface.

2. Using the Options Manager, configure and install the web_cgi_url option to specify the location of the CA SDM web engine. For example, http://hostname/scripts/pdmcgi.exe. For advanced availability, the host name should point to the application server or the load balancer.

Verify the Notification Method for the Recipient

Ensure that the contact to whom you want to send the notification, is assigned to that particular notification method.

Follow these steps:

1. Select Security and Role Management, Contacts on the Administration tab.
   The Contact Search page opens.

2. Search for the contact using the filter and select the contact that you want to notify from the search result.
   The contact detail page opens.

3. Select Notification on the Contact Details tab.

4. Verify the notification method. Based on your notification priority, choose the required option. For example, you want to send an email notification for any emergency notification. Select the Email option in the Emergency field.

5. To change the notification method, click Edit, change the option, and click Save.
   The notification method for the contact is verified.

Allow Temporary Email Addresses

A temporary email address is an address that is not associated with a contact in the system. Temporary email addresses are useful in circumstances such as the following one:

- An end user is out of the office or is having difficulty accessing their standard email account.
- The analyst wants to use email to track interactions with the user.
- The analyst sends a manual notification to a *temporary* email address for the user.
- The analyst can view the activity log, which is updated with the manual notification.

Recipients cannot reply to temporary addresses when their email address is not associated with a contact record or does not have permission to update the ticket.

Note: Temporary email addresses are always SMTP email addresses, and are supported only when the Preferred Method supports SMTP. For information about how to set up temporary email addresses, see the *Online Help*.

Follow these steps:

1. Select Options Manager, Notifications on the Administration tab.
   The Option List page opens.

2. Click notification_allow_temp_address.
   The notification_allow_temp_address Options Detail page opens.

3. Click Edit.

4. Click Install.
   The notification_allow_temp_address Options Detail page opens.

5. Click Close Window.

6. Restart the CA SDM servers. See How to Restart the CA SDM Servers (see page 913).
   Temporary email addresses are now allowed for manual notifications.

Create Message Templates

Create a message template that contains the values to use for the notification message. When you send multiple notification messages, you can use the message templates to simplify your workload.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. Select Notifications, Message Templates from the Administration tab.
   The Message Template List page opens.

2. Click Create New.
   The Create New Message Template page opens.

3. Complete the fields as appropriate.

   - **Symbol**
     Defines a unique identifier for this message template.

   - **Object Type**
     Specifies the object type associated with this template. For example, select Request/ Incident/ Problem for any notification related to a ticket.

   - **Record Status**
     Specifies the status of the template as either active or inactive. Set the status to Active to use the message template.

   - **Auto Notification**
     Specifies to send the notification associated with this template automatically, when the activity occurs. For example, you set up an initial notification, set up the objects to notify, and set up the message template, but you are not ready to turn on the notifications. In this case, you do not select Auto Notification. When you are ready to start automatic notifications, you select the check box. The notification becomes active and occurs as defined.

   - **Notify Level**
     Indicates the relative importance of sending this notification. For example, select Emergency if you want to send the email notification to the contact immediately when the associated activity occurs.

   - **Notification Message Title**
     Specifies the summary title of the message. You can use variables to insert the incident number in the message title. For example, @{call_req_id.type.sym} @{call_req_id. ref_num} @{type.sym}.

- **Notification Message Body**
  Specifies the content of the message. You can use variables to insert the analyst name, end-user name, and description into the message. For example,

```
@{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}.

Assigned to: @{call_req_id.assignee.combo_name}

Customer: @{call_req_id.customer.combo_name}

Description: @{call_req_id.description}


Click on the following URL to view:

@{call_req_id.web_url}
```

  You can use the ARTIFACT keyword to specify how artifacts are handled in outbound messages, message templates, notifications, and auto-replies. The ARTIFACT keyword uses the following values:

  - **NONE** -- Specifies no validation of artifacts. This value is the same as not using the keyword.
  - **PROTECTED** -- Validates a ticket against the hash for confirmation. If confirmation fails, the artifact is considered invalid and filtering fails when filtering searching for an artifact ({{object_id}}).
  - **SECURE** -- Decrypts the ticket number. If the value is not a valid password, the artifact is considered invalid and filtering fails when filtering is searching for an artifact ({{object_id}}).

- **HTML Message**
  Specifies the HTML message that is displayed to the recipient. If the recipient receives the message on an external device, such as a cell phone or PDA, the message displays in plain text only. Click Edit HTML Message to open the HTML Editor.
- **Quick View**
  Displays the message as it appears to the recipient.
- **HTML Source**
  Displays the message in the HTML source code.

4. Click Save.
   The message template is created.

Create a Notification Rule

Create the notification rule to specify the contacts to be notified and under what circumstances.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Note: The "Document about to expire" activity notification is activated seven days before the actual expiration date that displays in the knowledge document.

Follow these steps:

1. Select Notifications, Notification Rules from the Administration tab.
   The Notification Rule List page opens.

2. Click Create New.
   The Create New Notification Rule page opens.

3. Complete the following fields:

   - **Symbol**
     Defines a unique identifier for this notification rule. For example, enter Ticket Description Update.

   - **Object Type**
     Defines the object to which the rule applies. For example, select Request/ Incident/ Problem for an activity related to a ticket.

4. Click Save & Continue.

5. Click Condition to select the macro you can use to define a condition for this rule. Do one of the following actions to define the condition:

   Note: A notification rule without a condition notifies all contacts every time the activity occurs.

   - Search for the macro from the list and select it.

   - Click Create New to create a macro.

6. Click Message Template to add a message template that you have created for this rule. Do one of the following:

   - Search for the template from the list and select it.

   - Click Create New to create a message template.

7. Choose the appropriate contacts to notify from the following tabs:

   Note: Use the Update Contacts button that appears on each tab to search for and select more contacts to notify.

- **Object Contacts**
  Displays the available organizations, vendors, and configuration items for the selected Object type that receive notification about tickets. For example, you can select Affected End User or Affected End User's Admin Org to notify.

- **Contacts**
  Displays the individuals who are added to the notification rule, regardless of their association with the ticket.

- **Contact Types**
  Displays the users who are defined within the notification rule with the same classification, such as analyst or customer.

8. Click Save.
   The notification rule is created.

Create an Activity Association

Associate an activity with the object attribute to track the changes to the related object attribute. For example, associate Field Update activity with the object attribute of the Description field of an incident record. This enables you to send a notification whenever the description of the incident is updated. An object attribute can have only one activity notification.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. Select Notifications, Activity Associations on the Administration tab.
   The Activity Association List page opens.

2. Click Create New.
   The Create New Activity Association Type page opens.

3. Complete the following fields:

   - **Symbol**
     Defines a unique identifier for this association.

   - **Code**
     Defines an internal code for the activity association.

   - **Object Type**
     Specifies the name of the object to which the attribute applies. For example, select Request/ Incident/ Problem.

- **Object Type Attribute**
  Defines the object attribute to which the activity type is associated. For example, enter the object attribute of the Description field of an incident record.

- **Activity Type**
  Indicates the type of activity. For example, select Field Update to check when the selected object attribute is updated.

- **Log Me**
  Determines if this activity association creates a log entry in the Audit Log.

4. Click Save.
   The Activity Association Type Detail page opens.

5. Click Close window.
   The activity association is created.

Create an Activity Notification

Associate the activity with a notification. When the activity takes place, the associated notification is sent to the selected contacts.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants. You cannot maintain different Manual Notify activity notifications per tenant, or copy a Manual Notify activity notification.

Follow these steps:

1. Select Notifications, Activity Notifications from the Administration tab.
   The Activity Notification List page opens.

2. Click Create New.
   The Create New Activity Notification page opens.

3. Complete the following fields:

   - **Symbol**
     Defines a unique identifier for this activity notification.

   - **Code**
     Defines an internal code for the activity notification.

   - **Activity Valid for**
     Specifies the object to which this activity applies.

4. Click Save & Continue.
   The Update Activity Notification page opens.

5. Complete the following fields:

   - **Internal**
     Specifies if the activity notification is available only to internal employees or visible to end users.

   - **Record Status**
     Defines if the activity notification is active or inactive. Set the status to active to use the activity association.

   - **Related Ticket Activity**
     Specifies if the activity log on a ticket is propagated to all related tickets. The activity log propagation is only valid for related incidents, problems, and change orders. If you use multi-tenancy, perform the following actions:

     - Specify the appropriate tenant type from the Related Ticket Activity drop-down list.

     - Enter the name of the tenant in the tenant field, or click the search icon to search for a tenant.

   - **Object Type**
     Specifies the name of the object to which the activity applies.

6. Select the Notification Rules tab and click Update Notification Rules. Do one of the following actions:

   - Enter the search criteria, click Search, and select the notification rule from the search result.

   - Click Create New to create a notification rule.

7. (If you want to send a survey to the recipient of the notification) Select the Survey tab and define a survey notification (see page 854). Surveys let you collect and analyze the customer feedback. An activity log is generated when a survey notification is sent and when one is received back from a customer.

   Note: The Survey tab applies to all object types except Knowledge Documents, Knowledge Document Comments, and Knowledge Report Card. When specified from the Object Type list, the Emails tab appears instead of the Survey tab on the Update Activity Notification page. From the Emails tab, you can search for one or more email messages to associate with this notification or define a new one.

8. (If you want to trigger an event after the notification is sent) Select the Events tab. Events are procedures that an issue management system follows after a certain amount of time has elapsed. When the activity notification is triggered, the selected events occur. For example, update the status of the incident to Close. Search for the event and click Update Events button to add the event to an activity notification.

9. Click Save.
   The Activity Notification Detail page opens.

10. Click Close Window.
    The activity notification is created. If an error occurs on the outgoing mail server, email notifications are not sent and queue in the $NX_ROOT/site/mail_queue directory. When the mail server becomes active again, after an interval it processes and sends email. You can set the email retry interval variable (see page 854) to recycle the email that was queued when the mail server was busy.
    Notification email messages that the outgoing mail server fails to send are resubmitted until you do one of the following actions:

    - Stop the Mail Daemon (pdm_mail_nxd) that handles outbound email notifications.
    - Manually delete the messages from the $NX_ROOT/site/mail_queue directory.

Define Survey Notifications

Complete the following fields, as appropriate:

- **Send Survey**
  Indicates whether to activate or deactivate the survey. If selected, the survey is sent to the contact when the selected activity notification is triggered.
- **Default Survey**
  Specify a default survey using the search icon or specify your own in the text box.
- **Survey Message Title**
  Enter the title for the survey.
- **Survey Message Body**
  Enter a message for the contact. When a contact receives notification of a survey, the message includes a URL that they can access from their web browser to find and fill out the survey form.

Set the Email Retry Interval Variable

You can define the time interval (in seconds) to retry failed attempts to send outgoing email to the mail server.

Note: CA SDM does not retry sending messages that the outgoing mail server accepts, but cannot be delivered. For these messages, the outgoing mail server retry capabilities and policies, if any, are in effect.

Retries are on a per-message basis. If the mail server is unavailable for a period, each message is retried when its own timer expires, rather than all the messages being sent at once. However, if you restart the outgoing mail daemon, all unsent messages attempt to be sent at that time, and if they all fail to be sent, their retry timers are all reset at the same time.

The setting (NX_EMAIL_RETRY_INTERVAL) in the NX.env file controls the retry interval. You can change the default retry interval setting on one or more servers.

Follow these steps:

1. Log in to the following server, depending on your CA SDM configuration:
   - Conventional: Primary server
   - Advanced availability: Background server.
2. Navigate to the $NX_ROOT directory
3. Use a text editor such as WordPad to open the NX.env file.
4. Modify the value of to the NX_EMAIL_RETRY_INTERVAL interval you want as follows:

   ```
   NX_EMAIL_RETRY_INTERVAL=number_of_seconds
   ```

   - **NX_EMAIL_RETRY_INTERVAL**
     Defines the time interval (in seconds) to retry failed email attempts.
   - ***number_of_seconds***
     Specifies the number of seconds for each email retry interval. The default time is 600 seconds (10 minutes). The minimum value that you can use is 20 seconds. If you set a value that is less than the minimum of 20 seconds or more than 2000000 seconds, the default value of 10 minutes is used.
5. Save and close the file.
   Restart the CA SDM servers. For more information about how to start the CA SDM server, depending on your CA SDM configuration, see How to Restart the CA SDM Servers (see page 913) .
   The change takes effect.

Service Management Overview

This article contains the following topics:

Service Management Processes and Best Practices

Implementing standardized processes and best practices directly impacts the effectiveness, productivity, and cost of the Service Support environment. CA provides a library of recommended processes and best practices for Service Management that aligns with industry standards and recognized best-practice frameworks including ITIL, CobIT, BS15000, and more. The processes described for CA SDM include the following:

- Incident Management
- Problem Management
- Change Management

- Request Management
- Configuration Management
- Release Management
- Knowledge Management
- Support Automation

Note: Information about the Best Practices library is available online. You can learn about the Service Management Best Practices of CA, including white papers and other collateral at . The strategic process expert partners of CA can help personalize the best-practice library for your organization.

ITIL Configuration

Information Technology Infrastructure Library (ITIL) is a collection of best practices in computer data center management. In addition to defining recommended processes, a major benefit of the ITIL framework is its precise definitions of commonly used data center terminology. Often in the IT world, the same word is used to mean different things; or different people use a particular word with a meaning that is individually nuanced. ITIL helps to avoid this problem.

The following ticket types are available:

- Request
- Change Order
- Issue
- Incident
- Problem

Important! CA SDM only supports an ITIL interface. The ITIL interface supports data objects that were not used in previous non-ITIL versions of the product, for example, problem and incident tickets.

ITIL does the following:

- Produces an ITIL interface for your CA SDM installation.
- Allows your CA SDM database, forms, and fields to differ from a standard installation, and to conform to ITIL conventions instead.

Important! When upgrading your existing system, clear the "Load default data" check box to retain the database tables and data; otherwise, all existing data is lost.

ITIL Service Disciplines

ITIL describes best practices for several disciplines. The Service Support and Service Delivery disciplines combine to provide the Service Management capability of an organization. Complex interrelationships among all ten of the Service Management disciplines interact to help ensure that IT infrastructure delivers a high level of service to businesses.

Service Support includes the following disciplines:

- Incident Management
- Problem Management
- Change Management
- Release Management
- Configuration Management

CA SDM specifically addresses Incident, Problem, Change, and Configuration Management.

Service Delivery includes the following disciplines:

- Service Management
- Availability Management
- Capacity Management
- Financial Management for IT Services
- IT Service Continuity Management

CA SDM specifically addresses Service Management.

Configure the CA SDM Components

This article contains the following topics:

Components in CA SDM

CA SDM components include CMDB, Visualizer, Web Screen Painter, and Support Automation.

Configuration Management Database (CMDB)
CMDB consolidates and reconciles disparate sources of IT-related data in the context of business services. It lets you view the configuration item (CI) information such as resource attributes, relationships, and dependencies. You can use CMDB to display the relationships associated with a contemplated change, and thereby to understand the impact associated with such a change from a business service perspective (impact analysis). CMDB is installed automatically when you install CA SDM.

Visualizer
Visualizer provides a graphical depiction of a CI and its related CIs including the types of the relationships. You can double-click a CI in the Visualizer to follow relationship trails and understand the impact that one CI has on the other CIs. You can configure Visualizer on the Primary Server or a Secondary Server when you install CA SDM on that server. However, if you want to configure Visualizer after installing CA SDM, you launch CA SDM and then use the Configuration Wizard Visualizer.

Web Screen Painter
You can use Web Screen Painter to modify the database schema of CA SDM to meet your needs. Web Screen Painter also allows you to test your schema changes on your own web forms before updating the physical DBMS schema or affecting other users. In the conventional configuration, you can install Web Screen Painter on the Primary Server or any Secondary Server. However, in the advanced availability configuration, you must install Web Screen Painter only on the Background Server. If you install it on a standby server or an application server, you get an error message upon launching it.

Support Automation

Support Automation is a set of tools, processes, and technology. It enables the automated diagnosis, repair, and prevention of computer problems with minimal interaction required by the end user. Support Automation helps IT Analysts access end-user computers remotely and fix issues. You can configure Support Automation when you install CA SDM.

Configure the CA SDM Components

CA SDM is used to configure the primary and secondary servers as well as the database and web interface.

To install and configure CA SDM and its components on SQL server, enable TCP/IP on a system.

CA SDM Release 12.9 does not provide tools.jar and javac for AIX. Install tools.jar on AIX before you run the product configuration. Configuring REST Web Services and Support Automation requires the tools.jar file. To use the REST sample files, install javac on AIX. You can download the Java SDK for AIX from the IBM website in the IBM Developer kits section for Linux. Download the 32-bit binaries of Java SE and install JDK 1.6 SR10 on the AIX computer at any location. Copy tools.jar from the installed JDK location to <Shared Component>\JRE\1.6.0_10\lib and copy javac to \JRE\1.6.0_10\bin. You can also find the JRE location in the NX_JRE_INSTALL_DIR variable.

Note: If Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) coexist on the network, verify that appropriate tools and mechanisms to support these technologies are in place before you start the server configuration.

Follow these steps:

1. Select Start, Programs, CA, Service Desk, Configuration.
   The Configuration Wizard appears.

2. Complete the required fields. For information about the fields that appear in the wizard, see Server Configuration Utility (see page 869).

3. To complete the configuration, follow the on-screen prompts.

The default value for the TCP service number is displayed the first time that you configure the product. To determine the TCP service number on your installation, open a telnet session from your Windows workstation to the server:

- If your network is using NIS, enter the following command:

  ```
  ypcat services | grep slump.
  ```

  The output includes a line similar to the following line:

  ```
  slump nnnn/tcp   #This is required for slump to work!
  ```

- If your network is not using NIS, enter the following command:

  ```
  grep slump /etc/services.
  ```

  The output includes a line similar to the following line:

  ```
  #slump nnnn/tcp
  ```

  Enter the number *nnnn* in the TCP Service Number field.

Note: If configuration fails during the Validate Extension Tables step, database connectivity can be an issue. Run the configuration again, and verify that you provided the correct database connectivity information.

Product Configuration

After you install CA SDM and any additional products you select, complete the following steps:

- Configure the CA SDM components (servers, the database, the web interface).
- Configure the web interface if the web server and primary server are on different computers.
- Configure Support Automation.
- Implement Knowledge Document Life Cycle Reports for Automated Policies.
- Configure CA Business Intelligence.
- Implement multi-tenancy

For configuring servers for advanced availability configuration, see the scenario How to Configure Servers for Advanced Availability (see page 508).

Set Up the CMDB Audit Log

The object and trigger definitions, attributes, and HTML forms that are used by CMDB audit has changed. Set the CMDB Release 12.9 audit log by performing the following steps:

Follow these steps:

1. Remove the *cmdb_write_audit_log_site* trigger if you have created site/mods/*extension*.mod (*extension* specifies the extension name).
   In this release of the product, auditing is automatically created and enabled.
2. Add 'UI_INFO("AUDIT_LOG")' to each attribute that you want to log.
3. To migrate your existing HTML forms, use the new CA SDM templates.

CMDB Visualizer Configuration on AIX

Valid on IBM AIX

CA SDM installs CMDB Visualizer by default on all operating environments. You can configure the CMDB Visualizer, if necessary. IBM AIX requires additional security policy files.

Follow these steps:

1. Verify that CMDB Visualizer is configured.
2. Download unrestricted policy files (version 1.4.2 or later) from the Unrestricted JCE policy files page at the IBM website.

   Note: Register on the IBM website to download the policy files.
3. Replace the local_policy.jar and US_export_policy.jar files in your Shared Components JRE directory (default location: /opt/CA/SC/JRE/1.6.0_10/lib/security) with the policy files that you downloaded from the IBM website.

4. Stop and start Visualizer using the following commands:

```
pdm_tomcat_nxd -c STOP -t VIZ
pdm_tomcat_nxd -c START -t VIZ
```

   CMDB Visualizer is configured on IBM AIX.

Modify Third-Party Scripts for CMDB Compatibility

For scripts in the current product release, the ext_asset attribute is renamed to ID. To CMDB extension tables, modify the third-party scripts that use CA SDM web services. Perform the following steps:

Follow these steps:

1. Open the third-party script that you want to modify.

2. Replace all SQL references of ext_asset with ID.
   The script is compatible with the current product release.

How to Switch the Target Server for CMDB Reports

To create CMDB reports, a CA Cohesion ACM system exports CI data to a CMDB server. To export CI data, switch the target CMDB server by completing the following steps:

1. Use a CMDB server as the target for exporting CI data, and run CMDB Reports.

2. Restart the CA Cohesion ACM Server service.

3. Switch to a different target CMDB server for exporting CI data, and run CMDB Reports.

4. (Optional) Repeat Steps 2 and 3.

Configure Single Point of Entry

CA SDM and CA Service Management are integrated, single point of entry can permit Single Sign-On (SSO) to CA Service Catalog. To configure Single Point of Entry, follow these steps:

Follow these steps:

1. Install the catalog_server General option.

2. Restart CA SDM.

3. Navigate to the CA SDM Employee Self-Service page.

4. Click Browse Catalog Services.
   The CA Service Management logon page appears.

When CA EEM is configured for both CA SDM and CA Service Management, Single Point of Entry can permit single sign-on to CA Service Catalog. When single sign-on is configured, the CA Service Management logon page is not displayed.

Note: Single sign-on is not available if you enter CA SDM Employee Self-Service as a guest.

Follow these steps:

1. Verify that CA EEM Security options eiam_hostname and use_eiam_authentication are installed.
2. Set up your users in CA EEM and verify that these users are also CA Service Management users.
3. Click the Administration tab.
4. Open the Security and Role management folder.
5. Click Access Types.
6. Select the Employee role.
7. Verify that the validation type under the Web Authentication tab is set to CA EEM-Use CA Embedded Entitlements Manager.
8. Log in as the defined CA EEM user and navigate to the Employee Self-Service page.
9. Click Browse Catalog Services.
   The CA Service Management main page appears.

How to Modify the System Environment

CA SDM uses environment variables that are specified in the environment template file (NX.env.tpl) to determine certain behaviors. You can use environment variables to modify some system behaviors. You typically use the Options Manager to control system behavior, but at times CA Technical Support instructs you to modify a particular environment variable directly.

Consider the following when editing the environment template file:

- Environment variables set in this file can be overridden by setting the environment variable in the process space in which a process runs. Although convenient in some limited cases, this setup is not wanted. Preceding a variable setting with an at symbol (@) prevents variables in the process space overriding the variable. Unless there is a specific reason for allowing an override, the @ symbol always precedes the variable name in the template file.
- The comment characters for this file are pound (#) and exclamation point (!). The exclamation point character is also used to disable an option.

Important! Modify the template file (NX.env.tpl) and allow the configuration process to apply the changes to the environment file. Never modify the environment file (NX.env) directly.

Follow these steps:

1. Back up the environment template file (.tpl) that corresponds to your system environment:
   - UNIX -- $NX_ROOT/pdmconf/NX.env.tpl.
   - Windows -- installation-directory\pdmconf\NX.env_nt.tpl.
2. Edit the environment template file on the following server, depending on your CA SDM configuration:
   - Conventional: Primary server
   - Advanced availability: One of the standby servers

   Note: You can view and modify this file using any text editor (Windows users use WordPad).
3. Make the changes as instructed by your support technician, and save the changes.
4. To apply the changes you made to the environment template file to the actual environment file, run the configuration utility on the primary or standby server installation.
5. Depending on your CA SDM configuration, complete one of the following actions:
   - Conventional: For the changes that are made to the environment file to take effect, restart the primary server.
   - Advanced availability: Restart all the CA SDM servers (see page 866).

   Note: To avoid shutting down your system, your support technician can instruct you to restart only certain processes rather than recycling your entire CA SDM server.

Options Manager Usage

The CA SDM web client lets you use the Options Manager from the Administrative tab to do the following actions:

- Obtain a list of all the available options.
- View a summary of each option such as the application with which it is associated, a brief description, and its status.

- View the details of any specific option.
  When you view the detailed information for any option, you can get a comprehensive description of its functionality from the *Online Help*. The *Online Help* description includes any special actions that you are required to take when changing the option. For example, after installing or uninstalling some options, ensure that you restart the CA SDM server for the option to take effect. The *Online Help* description also indicates it.

- Review the status of all options at the summary level.

- Uninstall any of the available options (applicable only on the background server).
  Many of the options are preconfigured and installed during the CA SDM installation. Using the Options Manager to install or uninstall options can alter some or all of the default settings.

- Install any defined option (applicable only on the background server).

How to Move the Authentication Module to an External Server

This article contains the following topics:

The authentication module in CA SDM is a singleton daemon that is responsible for the user authentication. The authentication module runs on the primary server for the conventional configuration and on the background server for the advanced availability configuration. You can move the authentication module to an external server for the following scenarios:

- **Conventional configuration:**

  - The primary server is on UNIX or a Linux platform and you require a Windows authentication, you move the authentication module to a Windows secondary server.

  - The primary server is on a Solaris platform and you require the CA EEM authentication, you move the authentication module to the secondary server as CA SDM does not support the CA EEM integration on Solaris.

- **Advanced availability configuration:**

  - The background server is on UNIX or a Linux platform and you require a Windows authentication, you move the authentication module to a Windows application server.

- The background server is on a Solaris platform and you require the CA EEM integration, you move authentication module to an application server as CA SDM does not support the EEM integration on Solaris.

The following diagram illustrates how to move the authentication module:

Note: The selected external server must have CA SDM installed. If you move the authentication module to an external server such as an application server, it becomes a single point of failure. If the application server is down, users cannot log in.

Verify the Prerequisites

The analysis of the CA SDM server platforms helps you to decide how to move the authentication module to an external server.

Follow these steps:

- Identify the operating system of the following server, which is based on the configuration type:
  - **Conventional:** Primary server.
  - **Advanced Availability**: Application server.
- Identify the type of required authentication from the following models:
  - Windows authentication for the CA SDM implementation on UNIX or Linux.
  - CA EEM authentication for the CA SDM implementation on Solaris.
- Make sure that CA SDM is installed on the selected external server.

Configure CA SDM for Using External Authentication

To redirect the authentication requests to an external server, specify the hostname of the target server where the authentication module is present. The process of configuring CA SDM for moving the authentication module is different for the conventional and advanced availability configuration of CA SDM.

Conventional Configuration

Follow these steps:

1. Log in to the primary server as an administrator.
2. From the command prompt, change the directory to samples\pdmconf under NX_ROOT and run pdm_perlpdm_edit.pl.
3. From the pdm_edit.pl top menu select U, and press Enter.
   The User Validation server submenu appears.

4. Enter E to specify the hostname of the external server, and press Enter.
5. Enter primary for the primary server or the hostname of the secondary server, and press Enter.

You have configured the redirection of authentication requests to an external server.

Advanced Availability Configuration

Follow these steps:

1. Log in to the background server web interface as an administrator.
2. Select the Administration tab.
3. Expand Options Manager, Security.
4. Click the bopauth_nxd_host entry in the Option List.
   The bopauth_nxd_host Options Details page is displayed.
5. Click Edit.
6. Select the hostname of the target server from the Option Value drop-down list.
7. Click Save.

Note: By default, the authentication module runs on the background server.

You have configured the redirection of authentication requests to an external server.

How to Restart the CA SDM Servers

Depending on your CA SDM configuration, perform the following processes:

- Restart the CA SDM servers in conventional configuration.
- Restart the CA SDM servers in advanced availability configuration.

Restart the CA SDM Servers in Conventional Configuration

For the conventional configuration, you restart the servers in the following order:

Note: To restart a server click Start, Settings, Control Panel, Administrative Tools, Services. Right-click the CA SDM Server and select Start.

1. Restart the secondary server.

2. Restart the primary server.

Restart the CA SDM Servers in Advanced Availability Configuration

For the advanced availability configuration, we recommend that you restart the CA SDM servers in the following order:

Note: To restart a server click Start, Settings, Control Panel, Administrative Tools, Services. Right-click the CA SDM Server and select Start.

1. Restart all Standby Servers.
2. Promote the Standby Server as the New Background Server (see page 867).
3. Start the Old Background Server.
   When you start the background server, it becomes a standby server.
4. Choose the Less Active Application Server (see page 868).
5. Restart the Less Active Application Server.
6. Stop the Other Application Server (see page 868).
7. Start the Application Server.
8. Perform the steps 6 and 7 for the other application servers.

Promote the Standby Server as the New Background Server

Before you stop the background server, promote the standby server (that you have upgraded) as the new background server. If Support Automation is installed with CA SDM, notify the active Support Automation users about the background server shutdown.

Follow these steps:

1. Execute the following command on the background server to notify all active users using Support Automation to save their work:

   ```
   sa_server_notifier [-h] | [-q seconds] | [-c]
   ```

   - **-h**
     Displays the help page.
   - **-q seconds**
     This option notifies a local server (background) to quiesce in a specified time interval. This interval is the number of seconds before the server goes offline. This option cannot be used for a standby server or application server.

- **-c**
  This option cancels a previously sent quiesce request.

A pop-up message is displayed to all the active users using Support Automation. This message notifies the users about the server shutdown and the time that is left for the shutdown. The users must save their work and logout within that scheduled time.

2. Execute the following command on the standby server that you wish to promote as the new background server:

```
pdm_server_control  -b
```

- **-b**
  Notifies a local standby server to become the background server. The standby server must already be running. If the server is not running, it is started but no failover is performed; to start a failover, run the command again.

The background server shuts down automatically and the standby server is promoted as the new background server. This change does not affect the end-user sessions. The in-progress updates (if any) are stored and delayed, until the new background server comes online.

Choose the Less Active Application Server

You choose an application server with the least user activity. Run the following command on each application server to choose the one with no or minimal active sessions:

```
pdm_webstat
```

Note: This command does not capture the SOAP or REST Web Service sessions.

Stop the Other Application Server

You inform all the active users on an application server to move to the less active application server before you stop it. Ensure that you have restarted the less active application server before moving all the users to it.

Follow these steps:

1. (Recommended) Inform all active Support Automation analysts on the application server which you want to stop, to create a ticket in CA SDM with their session information. This process ensures that the session information is not lost. For example, the Support Automation analyst is in a session with a customer to resolve a hardware issue. In such a case, the Support Automation analyst can create an issue in CA SDM with the session information before the application server shuts down.

2. Send a notification (for example, an email notification) to all the active users on the application server to move to the less active application server that you just restarted. This notification can include the details of the updated application server.

3. Execute the following command on the application server:

   ```
   pdm_server_control [-h] -q interval -s server_name
   ```

   - **-h**
     Displays the help page.

   - **-q interval -s server_name**
     Notifies a local or remote application server to quiesce in a specified time interval. This interval is the number of seconds before the server goes offline. When using this option without a server_name, the local server is notified to quiesce. This option cannot be used for a background or a standby server.

   A pop-up message is displayed to all the active users on the application server to notify them about the server shutdown and the time left for the shutdown. The users must save their work and logout within that time. The application server stops after the specified time. The users log on to the other application server to resume their work. The Support Automation analyst can refer to the ticket and resume their work.
   The application server is stopped successfully.

Verify the Authentication

Verify the authentication with a user ID that has a corresponding contact record in Windows or CA EEM, based on the authentication type. A successful login indicates that you have successfully moved the authentication module.

Follow these steps:

1. Launch the browser and enter the CA SDM URL.

2. Log in to CA SDM with a user name having a corresponding contact record in Windows or CA EEM, based on the authentication type.

If the module has been moved successfully, the Service Desk Home Page opens.

Server Configuration Utility

The CA Service Desk Manager Server Configuration utility (pdm_configure) initializes and configures the CA Service Desk Manager server, database, and web environment. Configuration runs automatically during CA Service Desk Manager installation. The system administrator also can run Configuration on demand. The system administrator can configure the Administrative Client on Linux.

Follow these steps

- Select Server Configuration (see page 870)
- General Settings (see page 870)
- System Accounts (see page 871)
- Load Default Data (see page 872)
- Select Database (see page 872)
  - MS SQL Database Configuration (see page 873)

Select Server Configuration

You can select the CA Service Desk Manager installation configuration type and the type of database to configure.

Select Server Configuration

Specifies the configuration type for your CA Service Desk Manager installation. The options in the subsequent screens automatically updates to correspond to the configuration type you select. You can select the Advanced Availability option or Conventional option.

General Settings

Configure the General Settings page with the following options:

- **Configuration Type**
  The server type to configure.
  - Advanced Availability: If you are executing the Server Configuration utility for the first time, background server is automatically selected. Configure the background server and then add the application or stand-by servers to support advanced availability and failover.
  - Conventional: If you are executing the Server Configuration for the first time, primary server is automatically selected. After the primary server is configured, you can add secondary servers to manage high traffic volume and improve performance.
    For example, you can add more Object Managers and web engines to another server. There can be zero or more secondary servers in a CA Service Desk Manager enterprise system.
- **Slump Host Name**
  Available only for the Advanced Availability configuration. Slump host name specifies the system on which the server is installed.
- **Server Id**
  Available only for the Advanced Availability configuration. This field is automatically populated.
- **Primary Server Node**
  Available only for the Conventional configuration.
  Specifies the host name of the primary server. This field is case-sensitive. The Primary Server Node value is the same for both primary and secondary servers in the CA Service Desk Manager installation.

- **Object Manager Display Name**
  Specifies the server connecting to the server object managers (domsrvr). All object managers that start on this computer use this name for display purposes only. You can change this value when the object manager is started.

- **Object Manager Name**
  Specifies the names or aliases of the object managers to which you want to establish a connection. You can enter a single name or a list of names. The default of ANY connects to any running object manager, and is acceptable in most situations.

  Important! Verify the names of the object manager or group of object managers with your system administrator.

- **Local Host Name**
  Specifies the name of the server. This field is case-sensitive.

  - Conventional: You can enter the value only for secondary servers. This field is case-sensitive.
  - Advanced Availability: The value is automatically populated from your background server configuration details.

- **Configure /etc/services (UNIX only)**
  Adds the new socket ports to the /etc/services file. Valid only if you are the root user.

- **Slump Socket Port**
  Specifies the name of the main communications socket port. CA Service Desk Manager uses this port for all servers that are configured in your environment. The default value is 2100. The primary server always opens a listen port on the slump socket port. Every daemon (service) that communicates across the slump port connects to the primary server using this port.

- **Proctor Socket Port**
  Available only for the Conventional configuration. Applies only to systems that use secondary servers (proctors). Each secondary server listens on this port for messages from the primary server. The secondary servers open this port only when they cannot connect to the slump port on the primary server. For example, the port opens when the primary server is not running.
  Default: 2300

System Accounts

Configure the System Accounts page with the following options:

- **Privileged User Name**
  Identifies an operating system user ID with administration privileges. On Windows, if the name you specify does not exist, the system creates a local use with domain rights to different places, depending on how your local computer is defined:

  - If the local computer is not defined as a primary or backup domain controller, the privilegeduser is added to the local computer as a local user.

- If the local computer is defined as a primary domain controller, the privilegeduser is added as a domain user.
- If the local computer is defined as a backup domain controller, the privilegeduser is added to the primary domain controller as a domain user.

Important! If you have modified the user and domain user rights, contact the system administrator to set up the privileged user.

- **Privileged User Password (Windows)**
  Specifies a password for the privileged user account. If the privileged user name exists on the local computer, and the local computer is not defined as a primary or backup domain controller, the local user is checked. If the local computer is defined as a primary domain controller or a backup domain controller, the domain user is checked.
- **Privileged User Password (Linux)**
  Specifies a privileged user password for integrations with AMS and Workflow.
- **Restricted User Name (Windows only)**
  Specifies an operating system user ID that is used on behalf of clients as they access functions. The user name is restricted because it has limited user rights. The default is rhd. The rhd user is added in the same manner as the privileged user.
- **Restricted User Password (Windows only)**
  Specifies a required password for the restricted user name is added. The configuration stores the value.
- **Default User Name (UNIX)**
  Appears only for client installations. The default user name can be the privileged user, but it is typically a separate user ID for client users.

Load Default Data

Load default data is available only for the Advanced Availability configuration.

- **Load default data**
  Specifies whether to load the CA Service Desk Manager default system data into the database. If you have modified any system default values, selecting this option replaces the data values.

Note: You can select the option only during the background server configuration.

Select Database

Specifies the type of database to configure for your CA Service Desk Manager installation. The available options on the left automatically update to correspond the database type you select. For example, if the Database Type is SQL, the options update with MS SQL Database Config.

- Advanced Availability: The database type that you select must match the background server database.
- Conventional: The database type that you select must match the primary server database.

MS SQL Database Configuration

If you are using MS SQL Database, specify the following details:

- **Load Default Data**
  Applicable only for Conventional configuration.
  Load Default Data whether to load the CA Service Desk Manager default system data into the database. If you have modified any system default values, selecting this option replaces the data values.

- **Database Server Node**
  The name of the MS SQL instance that CA Service Desk Manager uses for configuration. The service instance is in the format hostname\instance_name. If the default instance is used, you only have to specify the hostname.

  - Advanced Availability: The database server node must match the background server database node.
  - Conventional: The database server node must match the primary server database node.

- **Database Name**
  Indicates the name of the database.

  - Advanced Availability: The database name must match the background server database.
  - Conventional: The database name must match the primary server database.

- **Database Admin User**

  Specifies the admin user who has permission to create user and schema.

- **Database Admin Password**

  Specifies the database password of user specified by database admin user.

- **Database Userid**
  The database user ID and password. The SQL user ID is added while creating the database.

  Note: The special at-sign character (@) cannot be used in database IDs or passwords.

- **Database Password**
  The password for the SQL database.

- **SQL Listening Port (Optional)**
  (Optional). The listening port of the defined SQL server instance.
  Default: 1433

Oracle Database Configuration

If you using the Oracle database, specify the following details:

CA Service Desk Manager requires a Net Service Name specifying the Oracle database where the MDB resides. CA Service Desk Manager also requires a system identifier (SID) for the database. CA Service Desk Manager requires the Net Service name and SID information to access the database with both Oracle client technology and JDBC technology. For information about Service Names and SIDs, refer to Oracle documentation.

- **Load Default Data**
  Applicable only for Conventional configuration and indicates the CA Service Desk Manager default system data into the database. If you have modified any system default values, selecting this option replaces the data values.

- **Remote Database**
  To indicate whether the Oracle MDB is on a remote server (selected) or the local server. If the Oracle server is local, the MDB is created during the configuration. If it is remote, the MDB must already be configured with the remote installer.

  Note: For Advanced Availability configuration, we recommend that you configure the Oracle MDB on a remote server.

- **Create Tablespaces**
  Specifies whether to create tablespaces for the MDB database or use existing tablespaces.

  - If this check box is selected, the script creates tablespaces with the default names MDB_DATA and MDB_INDEX.

    Note: The Data Tablespace Name and Index Tablespace Name fields are disabled.

  - If this check box is not selected, provide names of the existing tablespaces in the Data Tablespace Name and Index Tablespace Name.

    Important! To use the existing tablespaces, configure the database to use at least 500 MB of tablespace, and an index tablespace of at least 150 MB.

- **Net Service Name**
  Identifies the Net Service Name of the Oracle database where the MDB resides. If the database is remote, provide the Net Service Name that is defined within the Oracle client on the local computer.

- **mdbadmin User Password**
  Specifies the password of the mdbadmin user for accessing the mdb.

- **DBA User Name**
  Identifies the name of an Oracle user with DBA access.

- **DBA Password**
  Identifies the password for the DBA user.

  Note: The special at-sign character (@) cannot be used in database IDs or passwords.

- **Data Tablespace Name**
  Specifies the name for the MDB data tablespace you want to create. Used only if the Oracle server is on the local computer.

- **Index Tablespace Name**
  Specifies the name for the MDB index tablespace you want to create. Used only if the Oracle server is on the local computer.

- **Tablespace Path in DB Server**
  Specifies the directory path to the physical tablespace location.

- **Oracle Home Path**
  Specifies the Oracle Home path.

- **JDBC Connectivity**
  Specifies whether to use JDBC Connectivity. Several components of CA Service Desk Manager use JDBC technology to access the database and require specific information about the Oracle server.

  - **Database Host Name**
    Identifies the name of the computer where the Oracle server is installed.

  - **SID**
    Specifies the system identifier (SID) for the database as defined on the Oracle server computer. The SID value must be the SID for the MDB, and is not the same as the Net Service Name.

  - **Listener Port**
    Specifies the listener port for the database.

Important! For Windows installation, configure the Oracle MDB to use UTF-8 as the database character encoding to support multilingual search.

Web Interface

Configure the Web Interface with the following options:

- **Web Host**
  Specifies the system that hosts the web server. This value is used to build URLs for the system. By default, the web host is your local system.

- Advanced Availability: You can configure web services only on application server.
- Conventional: Available only if you are on a primary server, and defaults to the primary server name. You can change this value if your default web server is on another computer. For example, if you move your web server to a secondary server, you can change this value to the name of your secondary server. This value is used to build URLs for the system.

- **Config Type**
  Specifies the web server for your installation:

  Note: The Tomcat port is always used to access upload, the Asset Maintenance System, and pdmgraph, regardless of this setting.
  Note: Select the Manual option only when using an alternate http or servlet server.

  - On Windows, you can select Tomcat or IIS.
  - On UNIX, you can select Tomcat or Apache.

- **Web Site**
  NT only. Identifies the web site for the CA Service Desk Manager Server. The names appearing identify the available web sites. The IIS port is used to specify the port that is associated with the site.

  Note: You can install any mail system client on your server that complies with Microsoft MAPI 1.0 standard.

- **Tomcat Port**
  Specifies the Tomcat port number. Defaults to 8080, but you can set this port value. This value appears in the URL that is constructed to access the web site, for example, http://bobcat:8080/CAisd/UploadServlet.

- **Tomcat Shutdown Port**
  Specifies the socket port for Tomcat to monitor for shutdown requests.

- **Apache Config File (UNIX)**
  Specifies the complete path to the Apache configuration file. An include file is added to this configuration file when integrating with an existing Apache installation.

- **IIS/Apache Port**
  Specifies the IIS or Apache server port number. If you configure with IIS or Apache, and are not using port 80, enter an alternate port number. If you are using port 80, leave this field blank.

- Deploy SOAP Web Services
  - Advanced Availability: Applicable only for the application server. Enabling this option notifies the active users on the application server about the server shutdown details. For example, during rolling maintenance of the application server, a form is displayed to the active users stating that the application server shuts down within a specified time.

- Conventional: This check box is only available if you are configuring a secondary server. This option lets you deploy the web services on the secondary server. By default, web services are installed on the primary server.

REST Web Services

Configure the REST Web Services page with the following options:

- **REST Tomcat Port**
  Specifies the REST Tomcat Port.
  Default: 8050

- **Tomcat Shutdown Port**
  Specifies the REST Tomcat Shutdown Port.
  Default: 8055

Note: For Advanced Availability configuration, this option is available only for application servers.

Federated Search

Configure the Federated Search Tomcat with the following options:

- **Configure Federated Search**
  Specifies the option to select Federated Search. The Tomcat options are available only after selecting this option.

- **Tomcat Port**
  Specifies the Federated Search Tomcat Port.
  Default: 8040

- **Tomcat Shutdown Port**
  Specifies the Federated Search Tomcat Shutdown Port.
  Default: 8045

Visualizer

Configure the Visualizer page with the following options:

- Service Desk Manager Web Services
  - **Web Host**
    Displays the web host address.
  - **Web Host Port**
    Displays the Visualizer web host port.
- Visualizer Tomcat

- **Tomcat Port**
  Specifies the Visualizer Tomcat Port.
  Default: 9080

- **Tomcat Shutdown Port**
  Specifies the Visualizer Tomcat Shutdown Port.
  Default: 9085

Note: For Advanced Availability configuration, this option is available only for application servers.

Support Automation

On the Support Automation page, select the appropriate Configuration Type:

- **None**
  Configures CA Service Desk Manager without Support Automation functionality.

Important! If you want to configure Support Automation in a multi-tenancy environment, we recommend that you separately migrate the CA Support Automation r6.0 SR1 eFix5 divisions to Release 12.9 tenants before enabling Support Automation on a CA Service Desk Manager server.

- **Main Server**
  Configures the Support Automation server in main server (standalone) mode.
  Note: If you select the Main Server option, and are planning to configure one or more socket proxy servers, set the Socket Server host name and external port to the socket proxy host. For multiple socket proxies, you set the Socket Server to the host and external port of the load balancer server.

Note: For Advanced Availability, the main server resides on background and stand-by servers.

  - HTTP
    - **Host Name or IP** -- Specifies the address of your server.
    - **External Port** -- Specifies the external port of your server.
      Default: 8070
  - Socket Server
    - **Host Name or IP** -- Specifies the address of your socket server.

- **External Port** -- Specifies the external port of your socket server.
  Default: 10443
- **Internal Port** -- Specifies the internal port of your socket server.
  Default: 7005
- **Bind to IP** -- Specifies the IP where you want to bind the server.

- **Socket Proxy Server**
  Configures the Support Automation server in socket proxy mode. Use a Socket Proxy Server to off-load some of the CPU-intensive operations of Support Automation, such as encryption/decryption from the main server.
  Advanced Availability: This option is available only for the application server.
  Conventional: This option is available only for the secondary server.
  - Socket Configuration
    - **Main Server Host Name or IP** -- Specifies the address of the main server.
    - **Main Server Internal Port** -- Specifies the internal port of the main server.
      Default: 7005
    - **Main Server HTTP Port** -- Specifies the HTTP port of the main server. This field is available only for conventional configuration.
    - **External Port** -- Specifies the external port of the server.
      Default: 10444
    - **Bind to IP** -- Specifies the IP where you want to bind the server.

- **Message Routing Server**
  Configures the Support Automation server in message routing server mode. Use Message Routing Servers (MRS) to manage multiple Remote Control sessions that are based on the geographical location of the local server. Using MRS helps improve performance during assistance sessions.
  Advanced Availability: This option is available only for the application server.
  Conventional: This option is available only for the secondary server.
  - Socket Configuration
    - **External Port** -- Specifies the external port of the socket.
      Default: 10444
    - **Bind to IP** -- Specifies the IP where you want to bind the server.

- Tomcat Configuration
  1. **Tomcat Port**
     - Specifies the Support Automation Tomcat port.
       Default: 8070
  2. **Tomcat Shutdown Port**

- Specifies the Support Automation Tomcat Shutdown port.
  Default: 8075

> **Note:** When you change the main server Tomcat port, also change the port references in the server.properties file with tomcat server.xml.

Configuration Options

Configure the Config Options page with the following options:

- **Server Configuration**
  Select the configuration that you want to apply for this server from the drop-down list. Select Default to apply default CA Service Desk Manager configurations.

- Windows

  - **Start service when completed**
    Select this check box for the server to start when the configuration is complete.

    > **Note:** The UNIX users must be at the root user level for these options to be enabled.

  - **Start service when completed**
    Select this check box if you want the server to start when the configuration is complete.

  - **Put CA Service Desk Manager links in /usr/bin**
    This option only works if you are at root. Selecting this option puts important CA Service Desk Manager links into /usr/bin.

  - **Start Event converter daemons**
    Select this option to enable the event converter daemons. This option allows you to create the CA Service Desk Manager tickets from either CA NSM World View or CA NSM Event Monitor.

Character Encoding (UNIX/Linux)

The ICU converter provides the character encoding mapping that CA Service Desk Manager uses when transcoding character data between Unicode and the operating system character encoding.

> **Note:** This configuration page is only available on UNIX and Linux systems.

Configure the Character Encoding page with the following options:

- **Use detected converter**
  Auto-detection has determined the converter available for your UNIX/Linux system. Leave selected if you want to use this converter.

- **Specify a converter**
  The ICU converter name field provides feedback of the converter CA Service Desk Manager has determined best matches the operating environment. The converter also provides a means of overriding the auto-detected converter by specifying a converter name. The converter names are not case-sensitive.
  You can find a list of ICU converter names and aliases that are grouped by industry standards using the ICU Converter Explorer tool at the following web site:
  http://ibm.com/software/globalization/icu/demo/converters
  Give special attention to two converter names, if these converters appear as auto-detected:

  - **US-ASCII**
    Appears when the following conditions occur:

    - The auto-detection could not determine a matching converter and defaulted to US-ASCII. In this case, the ICU Converter Explorer or an equivalent tool must be used to determine a converter best matching the character encoding of the operating system locale. Enter its name into the ICU converter name field.

    - The character set of the operating system locale only supports a limited 7-bit character encoding such as C, POSIX, US-ASCII, ISO646-US. In this case, we recommend that you select a different operating system locale which utilizes a character set encoding that supports a wider selection of characters. See your operating system documentation for details for changing the locale environment for the user or shell that is used to invoke the CA Service Desk Manager configuration program. A matching locale environment must be used for all subsequent accounts that are used to launch and operate CA Service Desk Manager.

  - **UTF-8**
    Specifies to encode Unicode as UTF-8.

    Important! CA Service Desk Manager must run on an UTF-8 locale on UNIX platforms.

- **Default HTTP character set**
  Specifies the character set that is used on web pages that are sent from CA Service Desk Manager web servers. This value is specified in the web page HTTP character set declaration as the charset parameter in the HTTP Content-Type header, and is described in RFC 2616 Hypertext Transfer Protocol - HTTP/1.1.
  The configuration application attempts to determine whether this value is an alias of the ICU Unicode converter that is specified in ICU Unicode converter name. If it is not, you can override the value.

Configure the CA SDM Environment

This section contains the following topics:

How to Configure the Employee and Guest Interface

This article contains the following topics:

You can use CA SDM to configure separate interfaces for employees and guests. You configure these separate interfaces through the Options Manager in the Administration tab. The following values control these interfaces:

- **employee_intf_incident_support**

  Displays the following values:

  - Request only
  - Incident only
  - Both Incident and Request

- **guest_intf_incident_support**

  Displays the following values:

  - Request only
  - Incident only
  - Both Incident and Request

Important! For a new installation, ITIL is configured by default value set to *Incident only*. If you are migrating from a previous non-ITIL configuration, though the options are installed, the values are set to *Request only*.

Configure the Employee Interface

You can configure the employee interface to display incidents, requests, or both.

Follow these steps:

1. Click the Administration tab.
   The Administration console appears.

2. Click Options Manager, Request Mgr.
   The Option List appears.

3. Click employee_intf_incident_support.
   The Options Detail page appears.

4. Change the Option Value field to one of the following values:

   - **Incident Only**
     (ITIL Default) Displays only Incident ticket types on the employee interface.

   - **Request Only**
     Displays only Request ticket types on the employee interface.

   - **Both Incident and Request**
     Displays both Incident and Request ticket types on the employee interface.

   Click Save.

5. Click Refresh to confirm your selections.
   The Options Detail is updated.

6. Close the Options Detail.

Configure the Guest Interface

You can configure the guest interface to display incidents, requests, or both.

Follow these steps:

1. Click the Administration tab.

2. Click Options Manager, Request Mgr.

3. Click guest_intf_incident_support.

4. Change the Option Value field to one of the following values:

   - **Incident Only**
     (Default) Displays only Incident ticket types on the guest interface.

   - **Request Only**
     Displays only Request ticket types on the guest interface.

   - **Both Incident and Request**
     Displays both Incident and Request ticket types on the guest interface.

   Click Save.

5. Click Refresh to confirm your selections.
   The Options Detail is updated.

6. Close the Options Detail.

How to Configure the Web Interface

This article contains the following topics:

When you install CA SDM, the *web interface* (commonly referred to as the *browser interface*) is automatically installed.

Select the web server depending on the CA SDM configuration. Consider the following use cases:

- Conventional: No additional action is required when the web server and the primary server are on the same computer. If they are installed on a different computer, install and configure both primary and secondaryserver.

- Advanced Availability: No additional action is required when the web server and the background server are on the same computer. But if they are on a different computer, install and configure both background and application server. The web interface for end usersis never hostedfrom the background server. The web interface must be hosted only on the application servers.

Select the computer on which the web server resides depending on your CA SDM configuration:

- Conventional: Secondary server. Install this server after you install the primary server.

- Advanced Availability: Application server. Install this server after you install the background server.

Important! By default, Tomcat is the default web server. If you want to use IIS as your web server, manually configure the product and select IIS. For information, see the *Server Configuration Online Help*.

To configure the web interface, complete the following steps:

1. (Required) Enable the web engine on the secondary server on Windows or UNIX.

2. (Required) Configure the web interface (see page 887).
   You can then start the web interface (see page 887).

Add Web Engines or Web Directors

Web engines connect to an object manager for processing all requests to CA SDM objects. Web directors are optional, and are used when two or more web engines are installed on a single server. You can configure web directors on any server. Depending on the CA SDM configuration, CA SDM installs a default web engine on the following servers:

- Conventional: Primary server.
- Advanced Availability: All servers.

Follow these steps:

1. Select Systems, Configurations on the Administration tab.
   The Configurations List page opens.
2. Select the configuration to which you want to add the web engine or web director.
   The Configuration Detail page opens.

   Note: If you are changing the configuration for the first time, then create a configuration first. When you want to make a configuration change, always create or copy an existing one. This process allows you to revert to the previous configuration, if needed.

3. Select the Web Engines/Web Directors tab.
   The Web Engine/Web Directors Listpageopensdisplays the web engines and web directors that are configured for the server.
   - Conventional: A web engine exists by default on the primary server. You can add web directors to any server.
   - Advanced availability: A web engine exists by default on all servers. You can add more web directors on any CA SDM server.
4. Click Add Web Engine/Web Director.
   The Create New Web Engine/Web Director page opens.
5. Complete the following fields:

   Important! Enter only English characters for all the input fields for any localized language.

- **Host Name**
  Specifies the host name for the web engine or web director. You can click Search to look up for the servers.
  For an advanced availability configuration type, the host name is read-only and is automatically populated based on the host name you specified while creating the configuration.

- **Type**
  Specifies if you are configuring a webengineorwebdirector. Based on the option that is selected, the relevant fields are automatically populated.

  - Select Web Engine if you want to configure a web engine.
  - Select Web Director if you want to configureawebdirector.

  Note: Ensure that you have selected the appropriate option. You cannot edit the process type after you have saved the configuration.

- **Web Director**
  Specifiesthewebdirector that is assigned to the web engine. You can click Search to look up for the web directors added to the server.

  Note: When implementing any web engine load-balancing scheme, SSL-Login, or both, at least two web engines must be assigned to the same web director.

- **CGI Name**
  Specifies the unique CGI name for the web engine. It is the name of an actual CGI executable when IIS or Apache is used as the HTTP server; it is a servlet parameter when Tomcat is used as the HTTP server.
  Examples: (web engines) pdmweb1, pdmweb2, (web directors) pdmweb_d1, and pdmweb_d2.
  Default: pdmweb.exe (The CGI name must be unique).

- **CGI Port Number**
  Specifies the port on which CA SDM web clients can connect. The CGI port number is the same port on which the tomcat server is running.
  Default: 8080

- **Protocol**
  Specifies the protocol for accessing the web engine.

  - Select HTTPS if the web engine is configured to handle all CA SDM web-client user authentication requests.
  - Select HTTP if the web engine is configured to handle all web client non-user authentication requests (afteruserisauthenticatedthrough the secure login web engine).

- **Record Status**
  Specifies whether the web engineorwebdirector is active or inactive.

Note: Before setting the record status of a web director to inactive, remove the link between the web director and the associated web engines.

- **Object Manager**
  Specifies the object manager that you want to assign to the web engine.

  - **Default**
    Specifies that the default object manager is assigned to the web engine.

  - **ANY**
    Specifies that the web engine can connect to any available object manager with more willingness value. Willingness value is the availability of the server to accept new clients. A willingness value of zero means that the web engine does not accept any sessions.

  - **Choose**
    Allows you to specify an object manager for the web engine. Selecting this option provides you the option to add multiple object managers or aliases to the configuration.

Click Save.

The web engineorwebdirectorthatyouadded appears in the Web Engines/Web Directors List.

Configure the Web Interface

If the default web interface configuration specified does not meet the CA SDM installation requirements, modify the *web.cfg* file. The *web.cfg* is located in the *installation-directory* \bopcfg\www. Edit the file using a text editor, such as Notepad or WordPad.

Each entry in the file consists of a single line containing a property name, optionally followed by a value. Lines beginning with a pound sign (#) are treated as comments and are ignored.

Start the Web Interface

Verify that the Daemon Server services and the database server are started before starting the web interface. If the secondary server is configured, the Remote Daemon Proctor service must be started before starting the primary server service. To start the services on Windows and Linux OS, perform the following steps:

- (Windows): Select Start, Control Panel, Administrative Tools, Services). Right-click the CA SDM Remote Proctor and select Start.

- (Linux): Run the *pdm_init* command to start the primary server and *pdm_proctor_init* to start the secondary server.

Verify that the services are started and then start the web interface. You can also start the web interfacefroman internal web site. If you are on the primary or secondary server system and are using the Internet Information Services (IIS), perform the following steps:

- Select Start, All Programs, CA, Service Desk Manager, Service Desk Manager Web Client.

- On a system that is not a primary or a secondary server, open a web browser and enter the following URL address:

```
http://servername:8080/CAisd/pdmweb.exe
```

  In this URL, *servername* is the name of the computer that is hosting the CA SDM web server.

- On a System that is not a primary or secondary server with IIS as the web server, open a web browser and enter the following URL address:

```
http://servername/CAisd/pdmweb.exe
```

- To start the web interface from an internal website, add */pdmweb.exe* to the URL for your web pages. Use the following sample HTML code as a guide:

```
A HREF=http://<server-name>:<port-no>/CAisd/pdmweb.exe
```

  In this URL, *server-name* identifies your computer and *port-no* is the port on which your web server is listening.

  Note: If the Internet Explorer browser security is set to high, a warning message appears after starting the web interface. To avoid this message, add the website to your trusted sites or lower your security settings. In advance availability, the default web interface is readily available with the default installation and configuration.

Record Locking Behavior in the Web Interface

Editing a database record using the web interface, the user is given an exclusive lock of two minutes. You can change the default time by using the ExclLockSeconds property in the web.cfg file.

The following conditions apply when a database record is updated:

- If a user *can* edit and submit changes within an allotted time, the changes are included the database.
  When the database record is locked, other users (both web and non-web users) can view the record, but cannot edit the record. If they try to edit the record when it is locked, an error message appears.

- If a user *cannot* edit and submit changes within an allotted time, the record lock automatically drops and other users can edit the record.
  When the user submits the updates, time stamps are checked to ensure that nobody else has changed the record:

  - If the record has not been changed since the exclusive lock was dropped, the user updates are saved to the database.

  - If another user has edited the record after the lock expires, the user receives an error response and the changes are not saved. The user must restart the edit process and must reapply the changes.

Enabling the CAPA Help

CA Productivity Accelerator (CAPA) provides context-sensitive in-application performance support for the CA SDM analyst web forms. The CAPA player package directly integrates with the Context Help menus of CA SDM analyst web pages. The integration of CAPA Help content with CA SDM is achieved through the help menu scripts. These scripts launch the CAPA recorded Help content from the CA SDM Help menu drop-downs and right-click context help.

Note: This section does not include information about the CAPA recording tool, obtaining and configuring the CAPA Help content, and installing the Smart Help.

CA SDM provides a unique identifier to recognize each web form uniquely. If an identification element is present in the top frame of the CA SDM, the CAPA recording tool recognizes the web application form. Once the top frame is recognized, all sub frames are considered to be part of this application. The sub frames that are loaded from a different domain must also be identified. Otherwise, these sub frames are not considered a part of CA SDM. To enable CAPA help, prepare the help content and configure the options to launch the CAPA help.

Note: To modify the HTML files, use the invoke methods from the ias_helper.js files for the CAPA recorder to recognize the html forms.

CAPA Help is not supported on the CA SDM Employee, Customer, or PDA interfaces.

Follow these steps:

1. Open the capa.properties file from the following CA SDM directory:

   ```
   %NX_ROOT/bopcfg/www/wwwroot
   ```

2. Change the following values in the file:

   - **Enable_Alerts** = 0. This option verifies and displays the javascript alert messages in a browser console when the CA SDM web page loads.

3. Save the file.

4. Go to the web.cfg file in the CA SDM directory, add DebugScript=1, and restart the web engine.
   The recorded content is prepared, published, and deployed on the CAPA server.

5. Open the capa.properties file and change the following values:

   - **Enable_For_Recording** = 0

   - **Show_Learn_Links** = 1. This value displays the CAPA Help option in the CA SDM Help Menu and in the right-click Help context menu.

- **Server_Name** = name of the server where CAPA published content is deployed.
- **Server_Port =** CAPA server port where the CAPA published content is deployed. For example, the TOMCAT port.
- **Virtual_Dir** = virtual directory where the CAPA published content is deployed on the CAPA server.
- **Namespace** = application context namespace. For example, app.SDM.Project123;en.
- **Enable_Alerts** = 0

6. Save the file.
   You are ready to launch the CAPA Help from the CA SDM analyst web forms.

How to Configure Integrated Windows Authentication for CA SDM

As a system administrator, you can authenticate CA SDM users through an existing external authentication method. The following scenario describes configuring Integrated Windows Authentication (IWA) to authenticate CA SDM users through Microsoft Active Directory (AD). Configure CA SDM access types like administrators to use IWA. The users of the selected access types are directly authenticated through Active Directory.

Follow these steps:

1. Verify the Prerequisites (see page 890)
2. Configure Internet Information Services (IIS) for IWA. (see page 891)
3. Configure CA SDM for IWA. (see page 891)
4. Test IWA (see page 892)

Verify the Prerequisites

Verify the following requirements before you configure the external authentication for CA SDM:

- You have configured servers for CA SDM.
- You have installed IIS 7.0 on the following server depending on your configuration:
  - Conventional configuration: primary server.
  - Advanced Availability: application server.
- You have configured CA SDM to use IIS 7.0.
- You have the list of access types for which the external authentication is required. For example, CMDB Administrator, Employee, and CMDB User.

Configure IIS for IWA

You configure the IIS server to enable IWA. The configuration changes the authentication mode of IIS from Anonymous to Windows Authentication. After the configuration, the server starts redirecting authentication requests to the external source.

Follow these steps:

1. Log in as administrator to the following server depending on your configuration:
   - Conventional: Primary or secondary server.
   - Advanced Availability: Background server.
2. Open the Administrative Tools, Internet Information Services Manager.
3. Expand the Server Name node, where Server Name is the name of the CA SDM server.
4. Expand Sites, Default Web Site, CAisd node.
   The CAisd Home page opens.
5. Double-click the Authentication icon.
   The Authentication Settings page opens.
6. Disable the Anonymous Authentication by clicking the existing Status value.
7. Enable the Windows Authentication by clicking the existing Status value.
8. Restart IIS to apply the changes.

You have configured IIS for IWA.

Configure CA SDM for IWA

You configure the IWA for each of the selected access types. After an access type is configured for the external authentication, CA SDM externally authenticates the contacts of that access type.

Follow these steps:

1. Log in to CA SDM as a system administrator.
2. Select the Administration tab, Security and Role Management, Access Types.
   The Access Type List page opens.
3. Click the access type for which the external authentication is required.
   The Update Access Type form opens.
4. Select the Web Authentication tab and select the Allow External Authentication check box.
5. Select an appropriate value from the Validation Type drop-down list. The following values require description:

- **No Access**
  Specifies that the selected access type is not allowed to access.

- **Open**
  Specifies that the access is open to all.

- **OS**
  Specifies that the CA SDM server operating system credentials are required to access CA SDM. If you have configured EEM, the login request would be redirected to the EEM server.

- **PIN**
  Specifies that the value of selected CA SDM contact record field is required for the authentication. For example, if you select Pin as Validation Type and select Contact_Number from the PIN Field drop-down, the contact number of the user is required for authentication.

Note: The Validation Type is not used for the IWA validation, but it is used when the user logs in through the CA SDM login form. The CA SDM Login page appears only when the user clicks the Logout link or when the credentials do not match with IIS credentials.

6. Click Save.
   To configure the external authentication for other access types, repeat steps 1 through 6.

Test IWA

You test the IWA with a user id having the corresponding contact record in CA SDM. A successful login indicates that you have configured the IWA successfully.

Follow these steps:

1. Log in to the following server depending on your configuration, with a user id having the corresponding contact record in CA SDM:

   - Conventional: Primary or secondary server.

   - Advanced Availability: Application server.

Note: If the LDAP options have been installed in the Options Manager, you can also create new contact in CA SDM from any Active Directory contact.

2. Launch the browser and enter the CA SDM URL.
   The Service Desk Home page opens.

Search Engine Configuration

This article contains the following topics:

The EBR Search Engine installs with CA SDM by default.

Note: For more information about the search engine options, see the *Online Help*.

Knowledge Reindex Utility

The Knowledge reindex utility, pdm_k_reindex.exe, is located under the Knowledge Management installation directory.

Note: Reindexing the documents in the knowledge base can be a time-consuming operation based on your database size. It is recommended that you run the Knowledge Reindex utility after all the changes have been added. For advanced availability configuration, you cannot execute the knowledge reindex utility during the failover process.

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use pdm_task to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

Follow these steps:

1. Open the command prompt.
2. To run the knowledge reindex, enter the following command:

For example:

```
pdm_k_reindex
```

The following options are available with this command.

- **-D**
  Defines the debug mode, such as printing to the command window.
- **-v**
  Defines the verbose mode, such as printing to the stdlog file.
- **-i**
  Does not create table indexes in the reindex table after reindexing.

Note: Parameters with a dash as a prefix, such as " - D", must precede other parameters that do not have this prefix.

The other option is as follow:

- ***File*:reindex.txt**
  Documents are reindexed to the specified file.

- **+i**
  Creates the indexes of the reindexed table only, which is the search table after reindexing. The old indexes are dropped before reindexing.

- **+t**
  Switches the names of search and reindex tables only.

Note: A “+” prefix denotes only this parameter applies.

- **sdtout**
  Defines the frequency of statistic appearing in the command window. By default the knowledge reindex utility provides statistics into the command window for every 1000 documents processed. However, sometimes statistics are required to be provided more often. Use the following parameter:

  ```
  pdm_k_reindex -i sdtout:10
  ```

  In this case, statistics display in the command window for every ten documents.

The documents are reindexed in the knowledge base.

New Tags to Configure a Domserver for the Crawler Surface

You must have a dedicated server for the Crawler Surface depending on your CA SDM configuration and data size for indexing. The dedicated server minimizes the impact on the production environment:

- Conventional: Primary or secondary server

- Advanced Availability: Application server
  Note: For more information on how to configure CA SDM server, see Server Configuration Utility (see page 869).

The following two new tags are introduced in the crawler_surface_config.xml file to take care of the indexing:

- A new tag has been introduced in crawler_surface_config.xml file root\general_configuration\sdm_domsrvr_name to let the customer mention the name of a dedicated domserver instance for the Crawler Surface.
  Default: domsrvr
  This value is a default domserver (object manager) instance name.

- Another new tag has been introduced in the crawler_surface_config.xml file *sharepoint_properties_file* at the *root\general_configuration*.
  Default: sharepoint
  This value is the name of *sharepoint.properties* file available by default at NX_ROOT\CATALINA_BASE_FS\lib.

How to Enable Auto-Failover

Server health monitoring observes how a server reacts to the operating load and tracks its responsiveness to the client requests. The purpose of this monitoring is to prevent server failures by ensuring that the server always retains sufficient capacity to conduct the required tasks. Most of the standard health monitoring tools support remote server monitoring through the HTTP and HTTPS protocols.

CA SDM automatic failover feature exposes the following HTTP-based standard interfaces:

- Health Monitoring Interface: HTTP(S) interface to monitor the background server health. It also makes reliable failover decisions to initiate the failover on a chosen standby server in case of any disruptions to the background server's availability or ability to conduct required tasks.

- Failover Initiating Interface: HTTP(S) interface to promote the chosen standby server as the new background server without causing any service disruption.

Follow these steps:

1. Install Apache Tomcat on the background and all standby servers.

   Note: Ensure that Tomcat is using JRE 1.7 and ensure that the Tomcat is not using the port number that is configured for the CA SDM components.

2. (Optional) Configure SSL on the Tomcat servers that you have installed. For more information about configuring SSL, see How to Configure SSL Authentication (see page 935).

3. Log in to the background server.

4. Deploy the health servlet. Complete the following steps:

   a. Copy the HealthServlet.war file from the $NX_ROOT/samples/HealthServlet folder to the *TOMCAT_HOME*/webapps folder.

   b. Restart Tomcat.

The HealthServlet.war file is deployed in the webapps folder. To confirm the deployment, verify that the HealthServlet folder is created in the same webapps folder.
After the successful deployment, the health servlet is ready to perform the health checks. It includes checking the status of the SLUMP and health of the CA SDM processes that are defined in the health.xml file. Find the health.xml file in the following location:

```
TOMCAT_HOME/webapps/HealthServlet/WEB-INF/classes
```

5. (Optional) Customize the health.xml based on your organization needs. For example, you want to monitor the webengine process. Add the process in the health.xml file with the correct tagname, as defined in CA SDM. Complete the following steps to find the tagname:

    a. Open the pdm_startup.i and pdm_startup files from the $NX_ROOT/pdmconf directory.

    b. Look for the process that you want to monitor in both the files.

    c. Find the corresponding tagname by matching the variables in both the files.
    For example, webengine process is defined in the pdm_startup.i file as follows:

    ```
    #define WEBENGINE(_TAG,_HOST,_SLUMP_NAME,_DOMSRVR, _CFG, _WEBDIRECTOR,
    _RPC_NAME)
    ```

    The webengine process is defined in the pdm_startup file as follows:

    ```
    WEBENGINE(webengine, $NX_LOCAL_HOST, web:local, domsrvr, $NX_ROOT/bopcfg
    /www/web.cfg, "", "rpc_srvr:%h")
    ```

    From the example, we can find out that the tagname for webengine process is webengine.

    Important! For creating a new process, the existing process is commented out in the pdm_startup file and new entries are added. Ensure that you look for the tagname in the new process entries.

    Important! If you modify health.xml, ensure that the XML does not have any errors and that you restart Tomcat to reflect the changes that are made to the XML.

6. Perform steps 4 and 5 for all standby servers.

7. Configure the chosen third-party tool to monitor the health of the background server at regular intervals. To monitor the health, use the following HTTP URL:

    ```
    http(s)://Background_server_name:port_number/HealthServlet/GetHealth
    ```

8. Configure the chosen third-party tool to initiate a failover logic when the background server health degrades. We recommend that you to configure the failover logic so as to promote the standby server as the new background server. Use the following failover servlet in the failover logic:

   Important! We recommended you to configure the failover servlet on SSL with the access privileges given only to predefined users. Follow this recommendation for configuring third-party tools to initiate failover.

   ```
   http(s)://Standby_server_name:port_number/HealthServlet/FailoverServlet
   ```

   You have enabled auto-failover.

9. After the successful configuration, the third-party tool starts monitoring the background server health using the health servlet URL.

   - Each server type has its own set of processes. If the SLUMP and all the CA SDM processes are working properly, the third-party tool receives an HTTP 200 response from the background server with a predefined payload:

     ```
     AA-Server-Status: All OK!

     AA-Server-Role: BG
     ```

   - If a SLUMP or any of the CA SDM processes (listed in health.xml) stop working and cannot resume, the third-party tool receives an HTTP 503 response from the background server with a predefined payload as:

     ```
     AA-Server-Status: NOT OK!

     AA-Server-Role: BG
     ```

10. If the HTTP 503 response is received, the third-party tool automatically initiates the failover logic.

Screen Reader Usage

You can modify system behavior for optimal use with a screen reader for visually impaired users.

To enable screen reader usage:

1. Enable screen reader usage on the main menu from View, Preferences, and select the Using Screen Reader option.

   Important! You must log off and log back on for this change to take effect.

2. From the Help menu, select Screen Reader Usage for an overview of using CA SDM with a screen reader.

Deploy the Health Servlet on the Application Server

Server health monitoring prevents server failures and downtimes by ensuring that the server always retains sufficient capacity to conduct the required tasks.

Note: Ensure that your health servlet is installed on a separate instance of Tomcat server than CA SDM.

To deploy health servlet on the CA SDM Application Server, complete the following:

Follow these steps:

1. Install Apache Tomcat on the CA SDM Application Servers.

   Note: Ensure that Tomcat is using JRE 1.7 and ensure that the Tomcat is not using the port number that is configured for the CA SDM components.

2. (Optional) Configure SSL on the Tomcat servers that you have installed.
   For more information about configuring SSL, see How to Configure SSL Authentication (see page 935).

3. Log in to the application server and deploy the health servlet by completing the following steps:

   a. Copy the HealthServlet.war file from the $NX_ROOT\samples\HealthServlet\HealthServlet.WAR to the *Apache Tomcat Webapps directory (TOMCAT_HOME*/webapps).

   b. Restart Tomcat.

      The HealthServlet.war file is deployed in the webapps folder. To confirm the deployment, verify that the HealthServlet folder is created in the same webapps folder. After the successful deployment, the health servlet is ready to perform the health checks. It includes checking the status of the SLUMP and health of the CA SDM processes that are defined in the health.xml file. Find the health.xml file in the following location:

      `TOMCAT_HOME/webapps/HealthServlet/WEB-INF/classes`

4. (Optional) Customize the health.xml based on your organization needs. For example, you want to monitor the webengine process. Add the process in the health.xml file with the correct tag name, as defined in CA SDM. Complete the following steps to find the tag name:

a. Open the pdm_startup.i and pdm_startup files from the $NX_ROOT/pdmconf directory.

b. Look for the process that you want to monitor in both the files.

c. Find the corresponding tag name by matching the variables in both the files.
For example, webengine process is defined in the **pdm_startup.i** file as follows:

```
#define WEBENGINE(_TAG,_HOST,_SLUMP_NAME,_DOMSRVR, _CFG, _WEBDIRECTOR,
_RPC_NAME)
```

d. The webengine process is defined in the **pdm_startup** file as follows:

```
WEBENGINE(webengine, $NX_LOCAL_HOST, web:local, domsrvr, $NX_ROOT/bopcfg
/www/web.cfg, "", "rpc_srvr:%h")
```

Important!: For creating a new process, the existing process is commented out in the pdm_startup file and new entries are added. Ensure that you look for the tag name in the new process entries.

Important!: If you modify health.xml, ensure that the XML does not have any errors and that you restart Tomcat to reflect the changes that are made to the XML.

5. Configure the chosen third-party tool to monitor the health of the application server at regular intervals. To monitor the health of the server, use the following HTTP URL:

   ```
   http(s)://application_server_name:port_number/HealthServlet/GetHealth
   ```

6. After the successful configuration, the third-party tool starts monitoring the CA SDM application server health using the health servlet URL.
   For more information on how to deploy health servlet on the background and standby servers, see How to Enable Auto-Failover (see page 895).

7. Each server type has its own set of processes. If the SLUMP and all the CA SDM processes are working properly, the third-party tool will receive an HTTP 200 response from the Application server with a predefined payload, as follows:

   ```
   AA-Server-Status: All OK!
   AA-Server-Role: AP
   ```

   If a SLUMP or any of the CA SDM process (listed in health.xml) stops working and cannot resume, the third-party tool receives an HTTP 503 response from the application server with a predefined payload, as follows:

   ```
   AA-Server-Status: NOT OK!
   AA-Server-Role: AP
   ```

   You have successfully deployed the health servlet for the CA SDM Application Server.

Managing Servers

This article contains the following topics:

The CA SDM installation consists of one or more server components that an administrator can manage. The number of servers depends on the CA SDM configuration:

- Conventional: One primary server and one or more secondary servers.
- Advanced Availability: One background server, one or more standby servers, and one or more application servers.

After you install CA SDM, configure each computer that runs the CA SDM components. You can run the server configuration as part of the installation process, or you can run it later. The CA SDM services must be restarted after you change the server configuration.

How to Change a Server Configuration

As an administrator, you can configure the servers for CA SDM installation. The number and type of servers depend on the CA SDM configuration. The initial configuration occurs as part of the CA SDM installation process.

Note: A change in the system environment can require changes to the server configuration. For example, the database management system or integration changes with a web server (EEM server or Tomcat)

Follow these steps:

1. Log in to the server you want to configure again.
2. From the Windows Start menu, select Programs, CA, CA SDM, Configuration.
   The CA SDM Configuration utility opens.

3. Complete the utility fields, and click Next.
   The right panel changes to show the appropriate fields for the link that is highlighted in the navigation pane on the left.

4. Continue following the on-screen instructions and click Finish.
   The server configuration is changed.

How to Configure TCP/IP

You can change the default TCP Internet Protocol (TCP/IP) setting on one or more servers. This setting cannot be forced on the client if it is not supported on the server.

The TCP/IP setting is controlled by using the NX.env file, which is found in the $NX_ROOT directory. Use a text editor such as WordPad for editing this file. The following option controls the TCP/IP setting:

```
NX_PROTOCOL_ONLY=mode
```

where *mode* can be one of the following values:

- **IPv4**
  In IPv4 mode, the system opens up sockets for slump processes that listen to IPv4 traffic.

- **IPv6**
  In IPv6 mode, the system opens up sockets for slump processes that listen to IPv6 traffic.

- **Mixed**
  In mixed mode, the system opens up sockets for slump processes that listen to both IPv4 and IPv6 traffic. Depending upon your CA SDM configuration, you can configure mixed mode in the following circumstances:

  - Conventional: The Secondary servers that use a different Internet Protocol from the primary server or each other.

  - Advanced Availability: The Application servers that use a different Internet Protocol from the background server or each other.

Note: If IPv4 and IPv6 hosts coexist on the network, ensure that the appropriate transition strategies, tools, and mechanisms to support these technologies are in place before you change the server configuration.

Example

```
NX_PROTOCOL_ONLY=ipv4
```

Activity Log Security

The Activity Log security option prevents end users from updating fields on an activity log. You can select the internal option to prevent a customer from seeing the log.

Activity Log security affects activity logs from the following ticket types:

- Request
- Change order
- Issue
- Incident
- Problem

Enable Activity Log Security

You can enable Activity Log Security from the Options Manager in the Administration tab.

Follow these steps:

1. Click the Administration tab.
2. Click Options Manager, Request-Change-Issue.
3. Click activity_log_security.
4. Click Edit, and select one of the following Option Values:

   - **Editable**
     (Default) Allows all fields on the activity log to be editable through the web interface or web services.
   - **Write Protected**
     Displays the activity log as read-only. If you select the internal option, only internal users can edit the log which cannot be viewed by the customer.

   Note: If the security option is enabled and you try to edit the log using the web interface or external web services, an error message displays that the activity log is read-only

   Click Save.

5. Click Refresh to confirm your selections. Close Window.
   Activity log security is enabled.

Important! The activity_log_security option cannot be uninstalled. You can only change the value of the option to Editable or Write Protected in Options Manager, Request-Change-Issue.

Impact on Web Screen Painter

The Activity Log Security feature, $NX_ACTIVITY_LOG_ SECURITY, includes the following attributes (time_spent, time_stamp, and description) for the alg, chgalg, issalg objects in majic.

Example: $NX_ACTIVITY_LOG_SECURITY for Object alg in cm.maj

In this example, for object alg in cm.maj, $NX_ACTIVITY_LOG_SECURITY appears on the three attributes:

```
time_spent DURATION $NX_ACTIVITY_LOG_SECURITY {ON_POST_VAL update_cr_timespent
( call_req_id ) 50 ;
 } ;
time_stamp DATE $NX_ACTIVITY_LOG_SECURITYÂ Â Â { ON_NEW DEFAULT NOW ; } ;
descriptionÂ Â Â Â  STRING Â Â Â $NX_ACTIVITY_LOG_SECURITY;
```

In Web Screen Painter, *Updatable only for new record* field is disabled when the value of the keyword evaluates to WRITE_NEW.

Improve Performance With Browser Caching

The CA SDM web interface uses many JavaScript, style sheets, and image files, which can be fairly large and can affect performance.

To improve performance of the web interface, set up your HTTP server so that the user browser caches these files and loads only once a day.

The web interface performance improves.

Note: The default installation automatically configures caching for Apache and IIS; however, you can configure it manually.

Configure the Microsoft Internet Information Server

You can configure Microsoft Internet Information Server (IIS) to notify the browser that files loaded from the CA SDM directory expire one day after loading. The browser queries the server for these files only once a day, regardless of how many times they are used.

Follow these steps:

1. Launch the Internet Services Manager application (for Windows 2000 and XP, select Programs, Administrative Tools, Internet Services Manager).

2. Navigate to the CA SDM file folder, which is typically CAisd:

    a. Click the plus sign that is adjacent to the server running the CA SDM web interface.

    b. Click the plus sign that is adjacent to Default Web Site.

    c. Scroll down to CAisd.

3. Right-click the CAisd folder, and select Properties.
   The Properties page appears.

4. Click the HTTP Headers tab.

5. Select the Enable Content Expiration check box.

6. Select the Expire After option, enter 1 into the text field, and select a day from the drop-down list.

7. Click OK.
   The properties are saved and the changes take effect immediately.

Configure Apache

You can configure Apache to notify the browser that files loaded from the CA SDM directory expire one day after loading. This configuration means that the browser queries the server about these files only once per day, regardless of how many times they are used.

You configure Apache by updating a text configuration file. The default installation modifies your active configuration file in the apache conf directory (typically httpd.conf) to contain the statement:

```
Include installation-directory/bopcfg/www/CAisd_apache.conf
```

Installation-directory must be replaced with a full path. On Windows, this path is typically c:\Program Files\CA\CA SDM. On UNIX, replace *installation-directory* with the value of $NX_ROOT.

The file CAisd_apache.conf, which is referenced by the Include statement, contains the following text. Again, *installation-directory* is replaced with the full path as it was in the Include statement.

```
<IfModule mod_alias.c>
    Alias /CAisd installation-directory/bopcfg/www/wwwroot/
    <IfModule mod_expires.c>
           <Directory installation-directory/bopcfg/www/wwwroot>
              ExpiresActive   On
              ExpiresDefault  "access plus 1 day"
           </Directory>
    </IfModule>
</IfModule>
```

To configure Apache manually for browser caching of the CA SDM files, include statements similar to those in CAisd_apache.conf in your Apache configuration file. You can either add them directly to the file, or add an Include statement referencing a separate file, like the default installation.

Changes to Apache configuration files take effect only after you recycle Apache.

Clear the Cache

If you change a JavaScript, image, style sheet, HTML, or help file loaded by the HTTP server itself, you must instruct the users to clear their browser cache.

Note: For changes to HTMPL files to take effect, you must either recycle the web engine or use the pdm_webcache utility. In a development environment, you can avoid this task by specifying the configuration file property SuppressHtmplCache.

To clear the browser cache for Internet Explorer, perform the following:

Follow these steps:

1. Select Tools, Internet Options.
   An Internet Options dialog appears.

2. Click Delete Files.
   A confirmation window appears.

3. Click OK.
   The browser cache is cleared

To clear the browser cache for Firefox, perform the following:

1. Select Tools, Clear Private Area.

2. Click the Clear Private Data Now button.
   The browser cache is cleared.

Add a CA SDM Server

If you want to install a new server in your CA SDM deployment, you must first add the corresponding server record before you configure it.

Follow these steps:

1. Log in to the following server, depending on your CA SDM configuration:
   - Conventional: Primary server
   - Advanced availability: Background server
2. Select System, Servers from the Administration tab.
3. Click Create New to add a server record for the following server, depending on CA SDM configuration:
   - Conventional: Secondary server
   - Advanced availability: Application or standby server

4. Complete the fields as appropriate for the server.

5. Click Save to add the server detail.

Create Server Fields

The following fields appear when you create or update a server:

- **Host Name**
  Specifies the local host name of the server. The local host name is stored in the usp_servers table in local_host column.

  Important! Ensure that host name is entered as case-sensitive in the usp_servers table.

- **Attachment Servlet Path**
  You must specify the fully qualified domain name of a server using this field:
  http://<host>:<port>/CAisd/UploadServlet
  Where <host> is the fully qualified domain name of a server.
  We recommend that you configure this field.

- **Time Zone**
  Specifies the time zone where the server is located. This time zone value is used to trigger events in the application. This value is used only if the Use End User Time Zone option is not selected, or if no time zone is specified for the service type.

- **Record Status**
  Indicates the state of the server. Active status indicates that the server is a part of the CA SDM deployment.

  Important! If you have inactivated any server, it is recommended not to start CA SDM services on that server. This action may result in unexpected behaviour.

- **Server Type**
  Specifies the type of server that you want to configure. Following server types can be selected, depending on your CA SDM configuration:

  - Advanced Availability: Application or standby server
  - Conventional: Secondary server

- **Configured**
  Available only for advanced availability configuration. This field indicates the state of the configured server. The default value of this field is No. The value is updated to Yes after you successfully run pdm_configure on that server. If you edit any of the automatically entered field values of a server record, the Configured field turns to No.

How to Start the CA SDM Servers

This article contains the following topics:

Depending on your CA SDM configuration, complete the following actions:

- Start the CA SDM servers in conventional configuration (see page)
- Start the CA SDM servers in advanced availability configuration (see page).

The following table describes the processes that start automatically after you start the CA SDM servers:

Note: In this table, the Notification Manager process applies only to the Windows environment and the Default DB process applies only to the UNIX environment.

Process	Description
Daemon Agent (pdm_proctor_nxd)	The daemon agent responsible for starting the managed daemons
Daemon Monitor (pdm_d_mgr)	Monitors daemon processes
BOP Virtual DB (bpvirtdb_srvr)	BOP virtual database server
Data Dictionary (ddictbuild)	Rebuilds data dictionary each time the system is started -- this runs and then goes away
KPI Daemon (kpi_daemon)	Manages the collection, organization, and storage of KPI data.
Oracle agent (orcl_agent)	Agent for Oracle database -- many instances, depending upon load
Oracle DB (orcl_prov_nxd)	Oracle database provider
SQL agent (sql_agent) (runs only if you are using MS SQL)	Agent for SQL Server database -- many instances, depending upon load
SQL DB (sql_prov_nxd) (runs only if you are using MS SQL)	Microsoft SQL Server database provider
Event Manager (ehm_nxd)	Event manager
Message Dispatcher (sslump_nxd)	Dispatches messages
Notification Manager (bpnotify_nxd)	Manages notifications
Object Engine (domsrvr)	CA SDM Object Manager

Process	Description
Report Manager (pcrpt_nxd)	PC reporting
Software Version Control (pdm_ver_nxd)	Manages versions of specified system components
Method Engine (spel_srvr)	Spell code interpretation server
Text API (pdm_text_nxd)	Text API daemon for email and CA NSM interfaces
Timed Events/Notifications (animator_nxd)	Timed events and notifications
User Validation (boplgin)	User account validation
User Authentication (bopauth)	User account authentication
Web Engine (webengine)	Runs the engine for the web client
Archive Purge Daemon (arcpur_srvr)	Manages the background Archive and Purge processing
BU Daemon (bu_daemon)	Handles FAQ Rating calculation for Knowledge Documents
DB Monitor (dbmonitor_nxd)	Monitors CA common tables for changes
EBR Daemon (bpebr_nxd)	Handles knowledge search requests
EBR Idx Daemon (bpeid_nxd)	Handles EBR keyword indexing/re-indexing
KRC Daemon (krc_daemon)	Manages statistical calculations and notifications for the Knowledge Report Card
KT Daemon (kt_daemon)	Manages Knowledge Documents (KD approval process, permissions, notifications, and so on)
LDAP virtdb (ldap_virtdb)	Agent for communication with LDAP Servers
Mail Daemon (pdm_mail_nxd)	Handles outbound email notifications
Mail Eater (pdm_maileater_nxd)	Handles inbound email notifications
MDB Registration Server (mdb_registration_nxd)	Agent for handling MDB registration requests
PDM RPC (PDM_RPC)	Manages the Web Services requests
Repository Daemon (rep_daemon)	Handles attachment repositories
Spell checker (lexagent_nxd)	Handles spell checking requests
Time-to-Violation (ttv_nxd)	SLA Violation forecaster
tomcat controller (pdm_tomcat_nxd)	Manages Tomcat services

Start the CA SDM Servers in Conventional Configuration

Start the servers in the following order:

1. Start the secondary server (see page 909).
2. Start the primary server (see page 909).

Start the Secondary Server

If your installation includes one or more secondary servers, you must start the secondary servers prior to starting the primary server.

Follow these steps:

- (Windows) Select Services from the Control Panel, select the CA SDM Remote Proctor service and click Start.
- (UNIX) Use pdm_init from the command line.

Start the Primary Server

Every CA SDM installation has one primary server that handles basic product functionality.

Important! If your installation includes one or more secondary servers, you must start the secondary servers (see page 909) before starting the primary server.

Follow these steps:

- (Windows) Select Control Panel, CA SDM Server service and click Start. You can start the service manually each time you need it, or you can configure it to start automatically like any other Windows service.
- (UNIX) Use pdm_init from the command line.

Start the CA SDM Servers in Advanced Availability Configuration

Start the servers in the following order:

Note: (Windows) Select Control Panel, CA SDM Server service and click Start. You can start the service manually each time you need it, or you can configure it to start automatically like any other Windows service. (UNIX) Use pdm_init from the command line.

1. Start the background server.
2. Start the standby and application servers (in any order).

How to Stop the CA SDM Servers

This article contains the following topics:

Depending on your CA SDM configuration, do one of the following actions:

- Stop the CA SDM servers in conventional configuration (see page).
- Stop the CA SDM servers in advanced availability configuration (see page).

Stop the CA SDM Servers in Conventional Configuration

You stop the following servers:

- Stop the primary server (see page 910).
- Stop the secondary server (see page 910).

(Conventional Configuration) Stop the Primary Server

You can stop the primary server in the Windows or UNIX environment.

(Windows), follow these steps:

1. Select Services from the Control Panel.
2. Select the CA Service Desk Manager Server service and click Stop.
   The primary server is stopped. The processes or daemons on the secondary servers are also stopped.

(UNIX), follow these steps:

- Enter the following command in the command prompt:

  ```
  pdm_halt
  ```

  The primary server is stopped. The processes or daemons on the secondary servers are also stopped.

(Conventional Configuration) Stop the Secondary Server

You can stop the secondary server in the Windows or UNIX environment.

(Windows), follow these steps:

1. Select Services from the Control Panel.
2. Select the CA Service Desk Manager Remote Proctor service and click Stop.
   The secondary server is stopped.

(UNIX), follow these steps:

- Enter the following command in the command prompt:

```
pdm_halt
```

The secondary server is stopped.

Stop the CA SDM Servers in Advanced Availability Configuration

You stop the following servers:

- Stop the standby server (see page 911).
- Stop the background server (see page 911).
- Stop the application server (see page 912).

(Advanced Availability Configuration) Stop the Standby Server

You can stop the standby server in the Windows or UNIX environment.

(Windows), follow these steps:

1. Select Services from the Control Panel.
2. Select the CA Service Desk Manager Server service and click Stop.
   The standby server is stopped.

(UNIX), follow these steps:

- Enter the following command in the command prompt:

```
pdm_halt
```

The standby server is stopped.

(Advanced Availability Configuration) Stop the Background Server

Before you stop the background server, promote the standby server (that you have upgraded) as the new background server. If Support Automation is installed with CA SDM, notify the active Support Automation users about the background server shutdown.

Follow these steps:

1. Execute the following command on the background server to notify all active users using Support Automation to save their work:

   ```
   sa_server_notifier [-h] | [-q seconds] | [-c]
   ```

   - **-h**
     Displays the help page.

- **-q seconds**
  This option notifies a local server (background) to quiesce in a specified time interval. This interval is the number of seconds before the server goes offline. This option cannot be used for a standby server or application server.

- **-c**
  This option cancels a previously sent quiesce request.

A pop-up message is displayed to all the active users using Support Automation. This message notifies the users about the server shutdown and the time that is left for the shutdown. The users must save their work and logout within that scheduled time.

2. Execute the following command on the standby server that you wish to promote as the new background server:

```
pdm_server_control  -b
```

- **-b**
  Notifies a local standby server to become the background server. The standby server must already be running. If the server is not running, it is started but no failover is performed; to start a failover, run the command again.

The background server shuts down automatically and the standby server is promoted as the new background server. This change does not affect the end-user sessions. The in-progress updates (if any) are stored and delayed, until the new background server comes online.

(Advanced Availability Configuration) Stop the Application Server

Before you stop an application server, notify all active users to move to another application server.

Follow these steps:

1. Send a notification to all the active users on the application server for stopping servers. This notification can include the details of other application servers.

2. Execute the following command on the application server that you want to stop:

```
pdm_server_control -q interval -s server_name
```

- **-q interval -s server_name**
  Notifies a local or remote application server to quiesce in a specified time interval. This interval is the number of seconds before the server goes offline. When using this option without a server_name, the local server is notified to quiesce. This option cannot be used for a background or a standby server.

A pop-up message is displayed to all the active users on the application server. This message notifies the users about the server shutdown and the time left for the shutdown. The users must save their work and logout within that time. The application server stops after the specified time. The users log on to the other application server to resume their work. (Recommended) The active Support Automation analysts can create a ticket related to their session to save their work. They can log in to the other application server and refer to this ticket to resume their work.

How to Restart the CA SDM Servers

This article contains the following topics:

Depending on your CA SDM configuration,

- Restart the CA SDM servers in conventional configuration (see page).
- Restart the CA SDM servers in advanced availability configuration (see page).

Restart the CA SDM Servers in Conventional Configuration

For the conventional configuration, you restart the servers in the following order:

Note: To restart a server click Start, Settings, Control Panel, Administrative Tools, Services. Right-click the CA SDM Server and select Start.

1. Restart the secondary server.
2. Restart the primary server.

Restart the CA SDM Servers in Advanced Availability Configuration

For the advanced availability configuration, we recommend that you restart the CA SDM servers in the following order:

Note: To restart a server click Start, Settings, Control Panel, Administrative Tools, Services. Right-click the CA SDM Server and select Start.

1. Restart all Standby Servers.
2. Promote the Standby Server as the New Background Server (see page 867).
3. Start the Old Background Server.
   When you start the background server, it becomes a standby server.
4. Choose the Less Active Application Server (see page 868).
5. Restart the Less Active Application Server.

6. Stop the Other Application Server (see page 868).
7. Start the Application Server.
8. Perform the steps 6 and 7 for the other application servers.

Promote the Standby Server as the New Background Server

Before you stop the background server, promote the standby server (that you have upgraded) as the new background server. If Support Automation is installed with CA SDM, notify the active Support Automation users about the background server shutdown.

Follow these steps:

1. Execute the following command on the background server to notify all active users using Support Automation to save their work:

   ```
   sa_server_notifier [-h] | [-q seconds] | [-c]
   ```

   - **-h**
     Displays the help page.
   - **-q seconds**
     This option notifies a local server (background) to quiesce in a specified time interval. This interval is the number of seconds before the server goes offline. This option cannot be used for a standby server or application server.
   - **-c**
     This option cancels a previously sent quiesce request.

   A pop-up message is displayed to all the active users using Support Automation. This message notifies the users about the server shutdown and the time that is left for the shutdown. The users must save their work and logout within that scheduled time.

2. Execute the following command on the standby server that you wish to promote as the new background server:

   ```
   pdm_server_control  -b
   ```

   - **-b**
     Notifies a local standby server to become the background server. The standby server must already be running. If the server is not running, it is started but no failover is performed; to start a failover, run the command again.

   The background server shuts down automatically and the standby server is promoted as the new background server. This change does not affect the end-user sessions. The in-progress updates (if any) are stored and delayed, until the new background server comes online.

Choose the Less Active Application Server

You choose an application server with the least user activity. Run the following command on each application server to choose the one with no or minimal active sessions.

```
pdm_webstat
```

Note: This command does not capture the SOAP or REST Web Service sessions.

Stop the Other Application Server

You inform all the active users on an application server to move to the less active application server before you stop it. Ensure that you have restarted the less active application server before moving all the users to it.

Follow these steps:

1. (Recommended) Inform all active Support Automation analysts on the application server which you want to stop, to create a ticket in CA SDM with their session information. This process ensures that the session information is not lost. For example, the Support Automation analyst is in a session with a customer to resolve a hardware issue. In such a case, the Support Automation analyst can create an issue in CA SDM with the session information before the application server shuts down.

2. Send a notification (for example, an email notification) to all the active users on the application server to move to the less active application server that you just restarted. This notification can include the details of the updated application server.

3. Execute the following command on the application server:

   ```
   pdm_server_control [-h] -q interval -s server_name
   ```

   - **-h**
     Displays the help page.

   - **-q interval -s server_name**
     Notifies a local or remote application server to quiesce in a specified time interval. This interval is the number of seconds before the server goes offline. When using this option without a server_name, the local server is notified to quiesce. This option cannot be used for a background or a standby server.

   A pop-up message is displayed to all the active users on the application server to notify them about the server shutdown and the time left for the shutdown. The users must save their work and logout within that time. The application server stops after the specified time. The users log on to the other application server to resume their work. The Support Automation analyst can refer to the ticket and resume their work.
   The application server is stopped successfully.

How to Configure Processes for CA SDM Servers

As an administrator, you can add or modify processes and daemons to enhance the performance of the CA SDM servers. You can configure object managers, web engines, web directors, and other processes for the CA SDM servers in your environment. You can add the processes across several servers to increase volume, performance, and enhance security.

Follow these steps:

1. Add a Server (see page)
2. Create a Process Configuration (see page 917)
3. Add CA SDM Server Processes (see page 919)
4. Configure the Server (see page 930)
5. Verify the Configuration (see page 930)

Add a Server

If you want to install a new server in your CA SDM deployment, you must first add the corresponding server record before you configure it.

Follow these steps:

1. Log in to the following server, depending on your CA SDM configuration:
   - Conventional: Primary server
   - Advanced availability: Background server
2. Select System, Servers from the Administration tab.
3. Click Create New to add a server record for the following server, depending on CA SDM configuration:
   - Conventional: Secondary server
   - Advanced availability: Application or standby server
4. Complete the server fields (see page) as appropriate.
5. Click Save to add the server detail.

Server Fields

The following fields appear when you create or update a server:

- **Host Name**
  Specifies the local host name of the server. The local host name is stored in the usp_servers table in local_host column.

  Important! Ensure that host name is entered as case-sensitive in the usp_servers table.

- **Attachment Servlet Path**
  You must specify the fully qualified domain name of a server using this field:
  http://<host>:<port>/CAisd/Upload/Servlet
  Where <host> is the fully qualified domain name of a server.
  We recommend that you configure this field.

- **Time Zone**
  Specifies the time zone where the server is located. This time zone value is used to trigger events in the application. This value is used only if the Use End User Time Zone option is not selected, or if no time zone is specified for the service type.

- **Record Status**
  Indicates the state of the server. Active status indicates that the server is a part of the CA SDM deployment.

  Important! If you have inactivated any server, it is recommended not to start CA SDM services on that server. This action may result in unexpected behaviour.

- **Server Type**
  Specifies the type of server that you want to configure. Following server types can be selected, depending on your CA SDM configuration:

  - Advanced Availability: Application or standby server
  - Conventional: Secondary server

- **Configured**
  Available only for advanced availability configuration. This field indicates the state of the configured server. The default value of this field is No. The value is updated to Yes after you successfully run pdm_configure on that server. If you edit any of the automatically entered field values of a server record, the Configured field turns to No.

Create a Process Configuration

Important! (Recommended) Ensure that both background server and all other standby servers have similar configuration. The standby server becomes the new background after fail over and function likes the old background server.

You can create a process configuration for your CA SDM installation, or can modify an existing configuration to suit your requirement.

Consider the following points while creating or modifying a process configuration:

- If you want to modify a process configuration, we recommend you to create a new one or copy the existing configuration and then modify it. This process allows you to revert to the previous configuration, if necessary.

- In conventional configuration, you create configuration only for a primary server and not for secondary servers. All secondary server configuration details must be included within the configuration created for the primary server. For example, to add a webengine with the secondary server hostname details, open the configuration for the primary server and add the necessary details.

- For an advanced availability configuration type, you can create configurations only for the specific server. Make sure that you create the same configuration for the background server and standby server.

Follow these steps:

1. Select Systems, Configurations on the Administration tab.

2. Click Create New to add a server configuration.

3. Complete the following fields and click Save:

> **Important!** Enter only English characters for all the input fields for any localized language.

- **Configuration Name**
  Specifies the name that you want to assign to the configuration you create.

- **Advanced Availability**
  Indicates whether the configuration is created for conventional configuration or for the advanced availability configuration type. Select Yes if the configuration is valid for advanced availability configuration type.

> **Note:** Configurations that are created for one configuration type (advanced availability or conventional) cannot be implemented for the other configuration type.

Host Name
Specifies the host name for the configuration. The host name is taken from the servers records configured under the Servers page. You can click the Search button to look up for the servers added to your CA SDM installation.

- **Record Status**
  Specifies if the server configuration record is active.

- **Current Configuration**
  Indicates that the configuration is applied on the selected CA SDM server. This field is read-only and is updated based on the configuration you select while executing server configuration utility (pdm_configure).

The configuration is saved. New tabs are enabled on the page to add object managers, web engines, web directors, and other processes.

Note: The host name and the advanced availability fields become read-only once you have saved the configuration.

Click Edit in List on the Configuration List page to modify the record status of a process configuration.

Note: You cannot modify the record status if the current configuration of a selected server is in use.

Add CA SDM Server Processes

You can configure object managers, web engines, web directors, and other processes for the CA SDM servers in your environment. We recommend that you become familiar with the following information before configuring the CA SDM processes:

Important: Reconfigure the specific server by running the pdm_configure utility on the server after adding the CA SDM processes.

- **Object Manager**
  Object managers manage all the CA SDM objects. Each object manager has an associated name, which it uses to communicate with other objects. Enterprise systems with multiprocessor servers can add object managers to spread out the processing load. Depending on your configuration type, CA SDM installs a default object manager on the following servers:
  - Conventional: Primary server
  - Advanced Availability: All servers

  Note: You cannot modify the default object manager, but can add extra object managers to any server.

- **Web Engines**
  Web engines help prepare web pages for the web client. All systems have one or more web engines. Each web engine connects to an object manager for processing all requests to CA SDM objects. Each web engine can run and be accessed directly. In direct access, every web browser enters the specific CGI interface for a specific web engine. With this approach, all clients can connect to one web engine and can overburden the web engine, while the other web engines go unused. To handle such heavy traffic, you can assign two or more web engines to a single web

director. All requests that go to web engines are directed to the web director. The web director then redirects the client to the most available web engine.
Depending on your configuration type, CA SDM installs a default web engine on the following servers:

- Conventional: Primary server
- Advanced Availability: All servers

- **Web Directors**
  Web directors are optional, and are used when two or more web engines are installed on a single server. Web Director receives connection requests from users, selects a web engine to handle the request, and redirects the request to that web engine. This process is transparent to the end user who always accesses CA SDM with the same URL, regardless of the number of web engines configured. Web directors can be used for the following purposes:

  - To configure CA SDM for efficient use of secure sockets (SSL).
    The HTTPS protocol allows web transactions to be encrypted, providing maximum security for sensitive data, especially passwords. However, pages using SSL are ineligible for browser caching, which can have a negative impact on the performance.
  - To direct logins to a specific web engine (or web engines).
    After a user is authenticated, Web Director can move the session to a different web engine, which can be on a different HTTP server. This setup lets you configure SSL for a web engine, providing protection for your passwords while using HTTP protocol for transactions.
  - To have multiple Web Directors, each handling a different group of web engines.
    This setup can be useful in geographically dispersed organizations that want to locate groups of web engines physically closer to their end users.

- **Aliases**
  Aliases are easily identifiable names you can create for object manager Slump names. You can create aliases for a specific object manager or a group of object managers. These aliases can be used in place of an object manager name while configuring CA SDM processes. Aliases are optional in CA SDM.

- **Knowledge Daemons**

  Applicable only to a conventional configuration type. Knowledge daemons provide the knowledge base for CA SDM (knowledge documents, approval process, permissions, notifications, and so on). CA SDM configures the knowledge daemon by default on the primary server. You can move the daemon to a secondary server by changing the host name.

- **Login User Authentication**

  Applicable only to a conventional configuration type. CA SDM configures the login user authentication daemon by default on the primary server. You can move the daemon to a secondary server by changing the host name.

- **LDAP Virtual DB**

Applicable only to a conventional configuration type. CA SDM configures the LDAP virtual database daemon by default on the primary server. You can move the daemon to a secondary server by changing the host name.

- **Repository Daemons**

  Applicable only to a conventional configuration type. The Repository daemon enables you to locate the attachment records saved in the repository directory. Using the CA SDM web UI, you can add the processes only for secondary servers. After you have added the process through the web UI, enable the specific option during the CA SDM configuration. For more information about enabling the processes, see the Visualizer (see page 869) options. .

- **Visualizer**

  Applicable only to a conventional configuration type. You can configure visualizer on a CA SDM server to use web services. Using the CA SDM web UI, you can add the processes only for secondary servers. After you have added the process through the web UI, enable the specific option during the CA SDM configuration. For more information about enabling the processes, see the *Server Configuration Online Help*.

- **REST Web Services for Tomcat Server**

  Applicable only to a conventional configuration type. REST Web Services enables you to configure the web UI for CA SDM to be able to communicate with external world. Using the CA SDM web UI, you can add the processes only for secondary servers. After you have added the process through the web UI, enable the specific option during the CA SDM configuration. For more information about enabling the processes, see the *Server Configuration Online Help*.

- **Support Automation**

  Applicable only to a conventional configuration type. Using the CA SDM web UI, you can add the processes only for secondary servers. After you have added the process through the web UI, enable the specific option during CA SDM configuration. For more information about enabling the processes, see the *Server Configuration Online Help*. You can only add one support automation process for each secondary server. You can configure the following support automation servers:

  - **SA Main Server**
    Specifies the server on which support automation is installed. You can add the SA main server only to a secondary server.

  - **SA Dedicated Object Manager Server**
    The server on which the object manager for the support automation configuration resides. You can configure the dedicated object manager server on a secondary server.

    Note: You can add a dedicated object manager server only if the SA Main Server is configured.

  - **SA Message Routing Server**
    You can configure the message routing server on a secondary server to manage multiple Remote Control sessions and help improve the performance during assistance sessions.

- **SA Socket Proxy Server**
  You can configure the socket proxy server on a secondary server to take load off the main server during CPU-intensive operations of Support Automation, such as encryption /decryption.

- **UNI Converter**
  You can add UNI Converter to any one of the servers running on the UNIX platform. You can add the UNI converter to the following servers:

  - Conventional: Primary server, secondary server
  - Advanced Availability: Application server

- **TNG Converter**
  You can add a TNG converter to any one of the servers running on the Windows platform. You can add the TNG converter to the following servers:

  - Conventional: Primary server, secondary server
  - Advanced Availability: Application server

  Note: If the Daemon Manager manages the TNG converter, it starts and stops with the other daemons. If you need the TNG converter to catch events after the CA SDM daemons are shut down, start and stop the TNG converter as a service.

Add Object Managers

Adding object managers to CA SDM servers improves the overall system performance. CA SDM installs a default object manager on all servers. You cannot modify the default object manager, but you can add more object managers on any CA SDM server to increase the server performance. Depending on your configuration type, CA SDM installs a default object manager on the following servers:

- Conventional: Primary server.
- Advanced Availability: All servers.

Note: You cannot modify the default object manager, but can add additional object managers to any server.

Follow these steps:

1. Select **Systems**, **Configurations** under the **Administration** tab.
   The **Configurations List** page opens.
2. Select the configuration to which you want to add the object manager.
   The **Configuration Detail** page opens.

3. Select the **Object Managers** tab.
   The **Object Manager List** page opens displaying the object managers that are configured for the server. The default object manager (if any) is also displayed in the list.

4. Click **Add Object Manager**.
   The **Create New Object Manager** page opens.

5. Complete the following fields and click **Save**.

> **Important!** Enter only English characters for all the input fields for any localized language.

Host Name

Specifies the host name to which you want to add the object manager. You can click the Search button to look up for the servers added to your CA SDM installation.

For an advanced availability configuration type, the host name is read-only and is automatically populated based on the host name you specified while creating the configuration.

- **Display Name**
  Specifies a display name for the object manager. The display name appears on the clients to indicate which object manager it is connected to.

- **Object Manager Group**
  Specifies the group name to which the object manager is added.

  > **Important!** Enter only English characters for the object group name for any localized language.

- You can group object managers so that the groups can be assigned to provide service to specific groups of web engines. Users that require this feature often have web engines that are geographically separated from the primary server and want to collocate an object manager and the webengine. The users group the object managers that are assigned to the local webengines, and then assign the webengines to this group of object managers.

- **Accept Mask**
  Specifies the mask for the object manager. The Accept mask feature tells the object manager from which clients it accepts connections.
  For example, a web engine attempts to connect to an object manager with names such as web:seattle:1 (http://webseattle:1/), web:seattle:2 (http://webseattle:2/) or web:texas:1 (http://webtexas:1/). You can specify an Accept mask like web:seattle.* (http://webseattle.%2A/) to accept all seattle connections and reject others. You also specify a mask like web:.* to accept connections from web engines and reject connections from clients.

- **Record Status**
  Specifies whether the object manager is active or inactive.

  Note: Before setting the record status of an object manager to inactive, you must remove the link between the object manager and associated web engines.

The object manager that you added appears in the **Object Managers** list.

Add Web Engines or Web Directors

Web directors are optional, and are used when two or more web engines are installed on a single server. The Web Director receives connection requests from users and selects a web engine to handle the request. The request is then redirected to that web engine.

Web engines connect to an object manager for processing all requests to CA SDM objects. Web directors are optional, and are used when two or more web engines are installed on a single server. You can configure web directors on any server. Depending on the CA SDM configuration, CA SDM installs a default web engine on the following servers:

- Conventional: Primary server.
- Advanced Availability: All servers.

Follow these steps:

1. Select **Systems**, **Configurations** on the **Administration** tab.
   The **Configurations List** page opens.
2. Select the configuration to which you want to add the web engine or web director.
   The **Configuration Detail** page opens.

   Note: If you are changing the configuration for the first time, then create a configuration first. When you want to make a configuration change, always create or copy an existing one. This process allows you to revert to the previous configuration, if needed.

3. Select the **Web Engines/Web Directors** tab.
   The **Web Engine/Web Directors List** page opens displays the web engines and web directors that are configured for the server.
   - Conventional: A web engine exists by default on the primary server. You can add web directors to any server.
   - Advanced availability: A web engine exists by default on all servers. You can add more web directors on any CA SDM server.

4. Click **Add Web Engine/Web Director**.
   The **Create New Web Engine/Web Director** page opens.

5. Complete the following fields and click **Save**.

> **Important!** Enter only English characters for all the input fields for any localized language.

- **Host Name**
  Specifies the host name for the web engine or web director. You can click Search to look up for the servers.
  For an advanced availability configuration type, the host name is read-only and is automatically populated based on the host name you specified while creating the configuration.

- **Type**
  Specifies if you are configuring a web engine or web director. Based on the option that is selected, the relevant fields are automatically populated.

  - Select Web Engine if you want to configure a web engine.
  - Select Web Director if you want to configure a web director.

> **Note:** Ensure that you have selected the appropriate option. You cannot edit the process type after you have saved the configuration.

- **Web Director**
  Specifies the web director that is assigned to the web engine. You can click Search to look up for the web directors added to the server.

> **Note:** When implementing any web engine load-balancing scheme, SSL-Login, or both, at least two web engines must be assigned to the same web director.

- **CGI Name**
  Specifies the unique CGI name for the web engine. It is the name of an actual CGI executable when IIS or Apache is used as the HTTP server; it is a servlet parameter when Tomcat is used as the HTTP server.
  Examples: (web engines) pdmweb1, pdmweb2, (web directors) pdmweb_d1, and pdmweb_d2.
  Default: pdmweb.exe (The CGI name must be unique).

- **CGI Port Number**
  Specifies the port on which CA SDM web clients can connect. The CGI port number is the same port on which the tomcat server is running.
  Default: 8080

- **Protocol**
  Specifies the protocol for accessing the web engine.
  - Select HTTPS if the web engine is configured to handle all CA SDM web-client user authentication requests.
  - Select HTTP if the web engine is configured to handle all web client non-user authentication requests (after user is authenticated through the secure login web engine).
- **Record Status**
  Specifies whether the web engine or web director is active or inactive.

  Note: Before setting the record status of a web director to inactive, remove the link between the web director and the associated web engines.
- **Object Manager**
  Specifies the object manager that you want to assign to the web engine.
  - **Default**
    Specifies that the default object manager is assigned to the web engine.
  - **ANY**
    Specifies that the web engine can connect to any available object manager with more willingness value. Willingness value is the availability of the server to accept new clients. A willingness value of zero means that the web engine does not accept any sessions.
  - **Choose**
    Allows you to specify an object manager for the web engine. Selecting this option provides you the option to add multiple object managers or aliases to the configuration.

The web engine or web director that you added appears in the Web Engines/Web Directors List.

Add Aliases

Clients and other daemons can be connected to a specific Object Server using aliases. Aliases are easily identifiable names you can create for object manager Slump names. You can create aliases for a specific object manager or a group of object managers. These aliases can be used in place of an object manager name while configuring the CA SDM processes. Aliases are optional in CA SDM. Before you create aliases, perform the following activities:

- Define object managers and add some to groups.
  For example, domsrvr:group1:11, domsrvr:seattle:12, domsrvr:seattle:13, domsrvr:Tacoma:11.
- Enter a regular expression that matches a group of object managers.
  For example, you want the Java clients that are located in Washington to connect to object managers located in Seattle. You connect them to /domsrvr:seattle.*. Or, you can define an alias named SEATTLE and can assign it the value /domsrvr:seattle.*.
- Define web engines and assign aliases to the web engines.

Important! If you have created aliases for an object manager group, ensure that you modify the respective aliases after modifying the object manager group.

Follow these steps:

1. Select **Systems**, **Configurations** under the **Administration** tab.
2. Select the configuration to which you want to add the alias.
3. Select the **Aliases** tab.
4. Click **Add Alias**.
5. Complete the following fields and click Save:

Important! Enter only English characters for all the input fields for any localized language.

- **Name:** Specifies the name for the alias you created.
- **Definition:** Specifies the regular expression that is associated with the alias. The following format is used for an alias definition:

```
domsrvr:[[set the product group or family]:][<host_id><id>][.*]
```

Default: /domsrvr:.*

- **Record Status:** Specifies whether the alias is active or inactive.

The alias that you added appears in the Aliases List.

Add Additional Processes

CA SDM enables you to configure support automation servers, visualizer, LDAP, KT, TNG/UNI, BopLogin repository daemons, and REST web services process to a server. For more information about the processes, see System Configurations (see page 942).

Follow these steps:

1. Select **Systems**, **Configurations** on the **Administration** tab.
2. Select the configuration to which you want to add the additional processes.
3. Select the **Additional Processes** tab.
   The **Additional Process List** displays the list of processes that are configured for the server along with the default processes, if any.

4. Click **Add Process**.

5. Complete the following fields as appropriate and click **Save**:

> **Important!** Enter only English characters for all the input fields for any localized language.

- **Process**
  Indicates the CA SDM server process that you want to add.

- **Repository Daemon**
  Specifies the repository daemon that is configured for the server. Repository daemons support attachment repositories. CA SDM configures a repository daemon by default on the primary server. You can move the daemon to a secondary server by changing the host name.

- **SA Main Server**

  Applicable only to a conventional configuration type.

  Specifies the SA main server that is configured for the server. You can only configure one SA Main server.

- **SA Dedicated Object Server**
  Specifies the dedicated object manager for the support automation configuration. You can specify only one Dedicated Object Server either on primary or secondary server.

> **Note:** You can add a dedicated object manager server only if the SA Main Server is configured.

- **SA Message Routing Server**
  Specifies the message routing server that is configured for the server. You can configure the message routing server on a secondary server to manage multiple Remote Control sessions and help improve the performance during assistance sessions.

  Applicable only to a conventional configuration type.

- **SA Socket Proxy Server**

  Applicable only to a conventional configuration type.

  Specifies the socket proxy server that is configured for the server. You can configure the socket proxy server on a secondary server to take load off the main server during CPU-intensive operations such as encryption/decryption.

- **REST Web Services for Tomcat Server**

  Applicable only to a conventional configuration type.

Specifies the REST Web Services configures for the server. REST Web Services enables you to configure the web UI for CA SDM to be able to communicate with external world. Using the CA SDM web UI, you can add the processes only for secondary servers. After you have added the process through the web UI, enable the specific option during the CA SDM configuration. For more information about enabling the processes, see the *Server Configuration Online Help*.

- **TNG Converter**

  You can add a TNG converter to any one of the servers running on the Windows platform. You can add the TNG converter to the following servers:

- **Conventional:** Primary server, secondary server.

- **Advanced Availability:** Application server.

  Note: If the Daemon Manager manages the TNG converter, it is started and stopped with the other daemons. If you want the TNG converter to catch events after the CA SDM daemons are shut down, start and stop the TNG converter service.

- **UNI Converter**
  Specifies the UNI converter that is configured to respond to UNIX events. These events can be filtered and configured to create tickets and trigger other work in the Service Desk. You can add UNI Converter to any one of the servers running on the UNIX platform. You can add the UNI converter to the following servers:
  Conventional: Primary server, secondary server.
  Advanced Availability: Application server.

- **Visualizer Tomcat Server**

  Applicable only to a conventional configuration type. Specifies the visualizer that is configured for the server.

  You can configure visualizer on a CA SDM server to use web services. Using the CA SDM web UI, you can add the processes only for secondary servers. After you have added the process through the web UI, enable the specific option during the CA SDM configuration. For more information about enabling the processes, see the *Server Configuration Online Help*.

  Note: You can configure only one Visualizer Tomcat Server on a Secondary Server.

- **Hostname**
  Specifies the server that hosts the process you added. You can click the Search button to look up for the servers.

- **Record Status**
  Specifies whether the process you added is active or inactive.

The process that you added are displayed in the Additional Process List page.

Configure the Server

Use the Server Configuration utility (pdm_configure) to initialize and configure the CA Service Desk Manager server, database, and web environment. For more information, see Server Configuration Utility (see page 869)

Verify the Configuration

1. After the configuration is completed and the services are properly started, execute the pdm_status or task manager command to verify that the new daemons added.

2. Verify that the current configuration is updated with the configuration you selected during pdm_configure.

How to Perform Rolling Maintenance on CA SDM Servers

Important! Migration from an advanced availability environment is not possible using rolling maintenance. You must shutdown the CA SDM services in all the application and standby servers before starting the migration activity. For more information, see How to Upgrade CA SDM (see page 399).

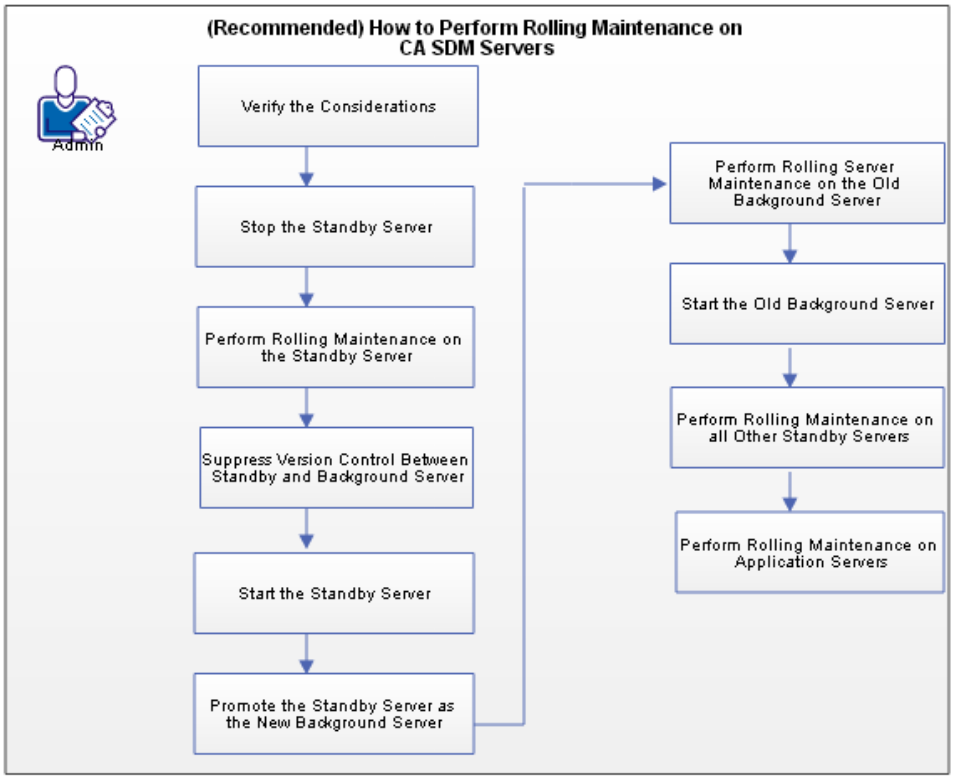
This article contains the following topics:

As a system administrator, you perform the rolling server maintenance on the CA SDM servers. This maintenance can be performed to apply patches or to perform a general maintenance on the servers. We recommend you to perform the maintenance on all the servers in a specific order. This process ensures all the servers are updated with the similar changes causing minimal or no disruption to end users. For any server-specific changes, you do not need to update all the other servers.

Important! Before applying a common MDB patch or an OS or security patch, shut down all the CA SDM servers. In such cases, the user task is disrupted with no access to CA SDM until all servers are up and running. We recommend the system administrator to plan the patch application accordingly.

The following diagram shows the recommended process to perform a rolling maintenance on the CA SDM servers:

Note: Depending upon your organization standards, the rolling maintenance process in your organization may differ from the recommended process.



Follow these steps:

1. Verify the Considerations (see page 932).
2. Stop the Standby Server (that you wish to promote as the new background).
3. Perform Rolling Maintenance on the Standby Server.
4. Suppress Version Control between the Standby and Background Server (see page 932).
5. Start the Standby Server.
6. Promote the Standby Server as the New Background Server (see page 867).
7. Perform Rolling Maintenance on the Old Background Server.
8. Start the Old Background Server.
   When you start the background server, it becomes a standby server.
9. Perform Rolling Maintenance on all Standby Servers.

Note: Stop the standby server, perform a rolling maintenance, and start the server.

10. Perform Rolling Maintenance on Application Servers (see page 933).

Verify the Considerations

During a failover of the background server to the standby server, consider the following points:

- The new users cannot log in.
- For the users that are already connected, some actions do not work during the failover. The users must try the actions after the failover. The following actions do not work:
  - Creating the tickets with attachments
  - Downloading the attachments
  - Searching Knowledge documents
  - Indexing the new knowledge documents
  - Inbound email
  - The SLA events that are not triggered until the failover has completed

Important! If you have configured your third-party tool to enable the auto-failover of the CA SDM servers, you must disable it before starting the rolling maintenance.

Suppress Version Control between the Standby and Background Server

CA SDM version control helps you to manage the system modifications across all CA SDM servers. Ensure that you suppress the version control on the standby server before starting it. This process ensures, that the standby server is not upgraded to the system modifications of the background server. To suppress the version control, run the following command on the standby server that you just upgraded:

```
pdm_server_control  -v
```

Promote the Standby Server as the New Background Server

Before you stop the background server, promote the standby server (that you have upgraded) as the new background server. If Support Automation is installed with CA SDM, notify the active Support Automation users about the background server shutdown.

Follow these steps:

1. Execute the following command on the background server to notify all active users using Support Automation to save their work:

   ```
   sa_server_notifier [-h] | [-q seconds] | [-c]
   ```

   - **-h**
     Displays the help page.

   - **-q seconds**
     This option notifies a local server (background) to quiesce in a specified time interval. This interval is the number of seconds before the server goes offline. This option cannot be used for a standby server or application server.

   - **-c**
     This option cancels a previously sent quiesce request.

   A pop-up message is displayed to all the active users using Support Automation. This message notifies the users about the server shutdown and the time that is left for the shutdown. The users must save their work and logout within that scheduled time.

2. Execute the following command on the standby server that you wish to promote as the new background server:

   ```
   pdm_server_control  -b
   ```

   - **-b**
     Notifies a local standby server to become the background server. The standby server must already be running. If the server is not running, it is started but no failover is performed; to start a failover, run the command again.

   The background server shuts down automatically and the standby server is promoted as the new background server. This change does not affect the end-user sessions. The in-progress updates (if any) are stored and delayed, until the new background server comes online.

Perform Rolling Maintenance on Application Servers

As a best practice, you can first perform the rolling maintenance on an application server that has the minimal or no users connected to it. Then, inform all users active on other application servers to log in to the updated server. Finally, you can perform the maintenance on the other application servers. This process ensures that the users are not moved between application servers multiple times.

Follow these steps:

1. Choose the less active application server (see page 868).

2. Stop the less active application server, perform the rolling maintenance, and start it.
   The application server is updated with all the changes.

3. Stop the other application server (see page 868).

4. Perform the rolling maintenance on the application server and start it.
   The application server is updated with all the changes.

5. Perform steps 3 and 4 for the other application servers.
   All the application servers are updated with all the changes.

Choose the Less Active Application Server

You choose an application server with the least user activity. Run the following command on each application server to choose the one with no or minimal active sessions.

```
pdm_webstat
```

Note: This command does not capture the SOAP or REST Web Service sessions.

Stop the Other Application Server

You inform all the active users on an application server to move to the less active application server before you stop it. Ensure that you have restarted the less active application server before moving all the users to it.

Follow these steps:

1. (Recommended) Inform all active Support Automation analysts on the application server which you want to stop, to create a ticket in CA SDM with their session information. This process ensures that the session information is not lost. For example, the Support Automation analyst is in a session with a customer to resolve a hardware issue. In such a case, the Support Automation analyst can create an issue in CA SDM with the session information before the application server shuts down.

2. Send a notification (for example, an email notification) to all the active users on the application server to move to the less active application server that you just restarted. This notification can include the details of the updated application server.

3. Execute the following command on the application server:

   ```
   pdm_server_control [-h] -q interval -s server_name
   ```

   - **-h**
     Displays the help page.

   - **-q interval -s server_name**
     Notifies a local or remote application server to quiesce in a specified time interval. This interval is the number of seconds before the server goes offline. When using this option without a server_name, the local server is notified to quiesce. This option cannot be used for a background or a standby server.

   A pop-up message is displayed to all the active users on the application server to notify them about the server shutdown and the time left for the shutdown. The users must save their work and logout within that time. The application server stops after the specified time. The users log on to the other application server to resume their work. The Support Automation analyst can refer to the ticket and resume their work.
   The application server is stopped successfully.

How to Configure SSL Authentication

As a system administrator, you can configure the web director to direct login requests to a specific web engine using the Secure Socket Layer (SSL) protocol. Configuring the SSL authentication provides enhanced login security while allowing users to access a higher performance connection.

Follow these steps:

1. Verify the Prerequisites (Setting up SSL) (see page 935)
2. Set the Web Engine Capability by Web Director Parameters (see page 935)
3. Choose the SSL Login Environment (see page 935)
4. Set Up SSL Login Environment (see page 937)

Verify the Prerequisites

Verify the following prerequisites before you begin the SSL configuration:

- Installed and configured CA SDM on the server where you want to implement SSL.
- Configured and assigned at least two web engines configured and assigned to a web director. For more information about how to configure web engines and web directors, see the How to Configure Processes for CA SDM Servers (see page 915).

Set the Web Engine Capability by Web Director Parameters

After you configure the web engine to use a web director, the web engine can handle the web client requests. The web engine can service login requests (redirect nonlogins elsewhere) or nonlogin requests (redirect logins elsewhere) or both (‘general purpose’ web engine). The WebDirector parameter found in the <Host_Name>-web[#].cfg file determines how webengine can service login requests.

The following table shows the relationship between the web engine role and web director parameter setting:

Web Engine Capability	‘<Host_Name>-web[#].cfg’ ‘webdirector’ Parameter Settings
Service login requests	‘UseDirector AfterLogin’; ‘Willingness 0’
Service non-login activity	‘UseDirector BeforeLogin’; ‘Willingness [1 thru 10]’
General purpose	‘UseDirector Yes’; Willingness [1-10]’

Choose the SSL Login Environment

You can use the web director for a targeted SSL login in a mixed SSL/non-SSL web environment to redirect every web-login request to the specific SSL web engines. All other requests can be redirected to and serviced by the non-SSL web engines.

Choose from the following SSL Login environment:

Non-SSL Environment with Basic Load-Balancing

You can use web director in a non-SSL environment with basic load-balancing. Web director balances load across all web engines according to each web engine willingness value. Each web engine can service login requests and nonlogin requests. The HTTP protocol is used for communication between the web client and the web server.

For each web engine under web director control, set the web director parameters in the web engine '<*Host_Name*>-web[*#*].cfg' as follows:

- UseDirector: Yes
- WebDirectorSlumpName: (do not change this value)
- WillingnessValue: [1 through 10]
- RedirectingURL: (the preappended protocol value can be either missing or 'http')

Global SSL Environment with Basic Load-Balancing

You can use web director in a global SSL environment with basic load-balancing. Web director balances load across all web engines according to each web engine willingness value. Each web engine can service login and nonlogin requests. The HTTPS protocol must be used for all communications between web clients and the web server.

For each web engine under web director control, set the web director parameters in the web engine '<*Host_Name*>-web[*#*].cfg' as follows:

- UseDirector: Yes
- WebDirectorSlumpName: (do not change this value)
- WillingnessValue: [1 through 10]
- RedirectingURL: (the preappended protocol value must be 'https')

Targeted Login in a Non-SSL Environment with Optional Load-Balancing

You can use web director for a targeted login in a non-SSL environment with optional load-balancing. The login-only web engine services only the login requests. The remaining web engines under web director control, service all other requests. This configuration puts the entire burden of servicing login requests on the specified login-only web engines. The HTTP protocol is used for communications between the web client and the web server.

For the login-only web engines, set the web director parameters in the web engine '<*Host_Name*>-web[*#*].cfg' as follows:

- UseDirector: AfterLogin
- WebDirectorSlumpName: (do not change this value)
- WillingnessValue: 0

- RedirectingURL: (the preappended protocol value can either be missing or ‘http’)

For the nonlogin web engines, set the web director parameters in the web engine ‘<*Host_Name*>-web [#].cfg’ as follows:

- UseDirector: Before Login
- WebDirectorSlumpName: (do not change this value)
- WillingnessValue: [1 through 10]
- RedirectingURL: (the preappended protocol value can be either missing or ‘http’)

Targeted SSL Login in a Mixed Environment with Optional Load-Balancing

You can use web director for a targeted SSL login in a mixed SSL/non-SSL web environment with optional load-balancing. Every web-login request is redirected and serviced by the SSL web engines, while other requests being serviced by the non-SSL web engines. The HTTPS protocol must be used for all communications between the web client and the SSL web engines.

Set Up SSL Login Environment

Setting up SSL allows web transactions to be encrypted, providing maximum security for sensitive data, especially passwords. Depending on your configuration type, you can implement an SSL login environment on the configured CA SDM servers.

Follow these steps:

1. Log in to the following server, depending on your CA SDM configuration:
   - Advanced Availability: Application server
   - Conventional: Primary or secondary server
2. Verify that the server has successfully imported an SSL certificate.
3. Create a copy (including subdirectories) of the directory ‘$NX_ROOT/bopcfg/www/wwwroot’, and assign it the following name:
   ‘$NX_ROOT/bopcfg/www/wwwrootsec’
4. Add a new virtual directory for the web server named CAisdsec.
5. Point this virtual directory to the following physical directory:
   ‘$NX_ROOT/bopcfg/www/wwwrootsec’
6. Verify that the virtual directory permissions for CAisdsec match the CAisd virtual directory permissions for the script execution. Enforce SSL for the CAisdsec virtual directory.

   Note: In this example, CAisdsec is user-defined and can be renamed.

7. Save the changes.

> **Note:** Webdirectors do not use a '<Host_Name>-web[#].cfg' file. However, web engines require a unique '<Host_Name>-web[#].cfg' file. Sample web.cfg files are automatically generated while running the configuration. You can import the modifications in the original web.cfg to the new web configuration files by specifying the original web.cfg as the template file you want to use.

8. Copy and save the following files, because a backup of these files is useful whenever you decide to restore the original environment:
   - $NX_ROOT/pdmconf/pdm_startup.tpl
   - $NX_ROOT/pdmconf/pdm_startup
   - $NX_ROOT/bopcfg/www/web.cfg file
   - Any existing primary-web[#].cfg files
   - $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml and web.xml.tpl
   - For a secondary server configuration, save backup copies of any existing $NX_ROOT/bopcfg/www/web.cfg or <Secondary_Server_Host_Name>-web[#].cfg files and $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml*
9. For each web engine assigned to a webdirector, ensure that the parameters (<Host_Name>-web[#].cfg 'webdirector') of the web engine are set correctly by examining the file in a text editor. If necessary, modify the 'webdirector' parameter values to reflect the web engine role you want. Then copy them to the directory: $NX_ROOT/bopcfg/www.
10. Move all $NX_ROOT/samples/pdmconf/primary-web[#].cfg files to the $NX_ROOT/bopcfg/www directory.
    For the secondary server configuration, Move all $NX_ROOT/samples/pdmconf/' secondary_server_name-web[#].cfg' from the primary server to the secondary server $NX_ROOT/bopcfg/www directory
11. For the servlet server like Tomcat, CA SDM creates web.xml files that can replace the web.xml file on each server hosting a webengine. These files are name primary-web.xml. Rename the files and copy them to the directory: $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF directory.
    For the HTTP server like IIS or Apache, create copies of 'pdmweb.exe' in the $NX_ROOT/bopcfg/www/wwwroot directory, a 'pdmweb[#].exe' for each web engine, and a 'pdmweb_d[#].exe' for each webdirector that has been configured. Verify that the 'pdmweb[#].exe' and 'pdmweb_d[#].exe' are named according to the correct CGI I/F values (for example: 'pdmweb1.exe', 'pdmweb2.exe', pdmweb_d1.exe', and so on).
12. If you are using IIS and want to add Server Extensions for each CGI interface, you can take the file primary-site.dat file and copy it to your $NX_ROOT/bopcfg/www directory as site.dat. When the system is reconfigured these sites is added to IIS.

13. Reconfigure the primary server without reinitializing the database and start services.

14. After reconfiguring verify that the current settings are valid. Start the CA SDM daemons. Verify that there are no errors in the stdlog files. Use pdm_status to view the daemons and their status. Use http://localhost:8080/CAisd/pdmweb.exe to access the system.

15. For Knowledge Management to CA SDM integration, if SSL has been enforced for CA SDM, the CA SDM URL protocol value must be changed.

    a. From the Knowledge Management Tool Settings Manager, General, Integration, change the CA SDM URL protocol value from http to https.

    b. Save and exit.

16. Open a web browser to the CA SDM login page and verify that a user can log in and that the expected redirect/login behavior is observed.

Implement SSL Login Environment

To implement the SSL login you have set up, make changes to the web director parameter values.

Follow these steps:

1. For Secure Login Web engines, edit the <Host_Name>-web[#].cfg as follows:

    a. Change the CAisd parameter value from /CAisd to /CAisdsec.

    b. Change the UseDirector parameter value from Yes to AfterLogin if the web director uses pass through an authentication.

    c. Change the Willingness parameter value from 5 to 0.

    d. Verify that the RedirectingURL value protocol is listed as https.

    e. Change the Redirecting URL <cgi directory> value from CAisd to CAisdsec.

    f. Save the changes.

2. For non-secure web engines handling all other activity, edit the <Host_Name>-web[#].cfg files as follows:

    a. Verify that the CAisd parameter value is /CAisd.

    b. Change the UseDirector parameter value from Yes to BeforeLogin.

    c. Maintain the Willingness value of 5 or set it to any integer value from 1 to 10, depending on the particular loading weight desired.

    d. Verify that the RedirectingURL value protocol is listed as http.

    e. Verify that the RedirectingURL <cgi directory> value is CAisd.

f. Save the changes.
After the configuration, restart Service Desk. After the service restarts, test the login by accessing the non-ssl web engine using HTTP. Verify if it automatically redirects you to the HTTPS secure webengine for the login. Once you are logged in, it automatically redirects you back to the non-ssl HTTP webengine for the normal Service Desk activity.

Verify SSL Login Environment

You can verify the SSL login environment for web engines.

Follow these steps:

- The secure-login web engines must reside in the physical directory that is mapped to the SSL-enforced virtual directory (CAisdsec in this example).
For secure-login web engines, create instances of pdmweb.exe in the $NX_ROOT/bopcfg/www/wwwrootsec directory with the name of pdmweb[#].exe. The executable name must match the CGI I/F value for each secure-login web engine.
Example: If you have assigned the CGI I/F value of the secure-login web engine to pdmweb2, create a physical copy of pdmweb.exe, and rename it pdmweb2.exe.

- The non-secure web engines and web directors must reside in the physical directory that is mapped to the non-SSL virtual directory CAisd.
For non-secure web engines and web directors, create instances of pdmweb.exe in the $NX_ROOT/bopcfg/www/wwwroot directory. A copy of pdmweb.exe must exist for each non-secure web engine and webdirector configured. Rename the copies so that the new names of the executables match the CGI I/F values that have been defined for the web engines and web directors.
Example: If you have assigned the CGI I/F value of pdmweb3 to the non-secure web engine and the value of pdmweb_d1 to the web director, then create two copies of pdmweb.exe. Rename the first copy to pdmweb3.exe, and then rename the second copy to pdmweb_d1.exe.

Set Up SSL Login for Tomcat Server

Configure SSL on Tomcat Servers in your CA SDM environment.

Follow these steps:

1. To create a key store on each CA SDM server that requires an SSL certificate, perform the following steps:

> **Note:** A keystore is a store or storage unit for certificates, in which the certificates are imported to, and then Tomcat points to use that keystore and certificates for SSL.

a. Create a directory under the C: drive (or the local drive you want) with the name, certificates.

b. Using the command line, navigate to the JRE bin directory (for the JRE installed with Service Desk - usually /SC/JRE)

c. Run the command "keytool -genkey -alias tomcat -keyalg RSA -keystore c:/certificates /keystore.jks".

d. Fill in the fields as appropriate (make sure to note what you filled in each filed as you may need this information later).
A keystore.jks file is created in the C:\certificates\ directory.

2. Generate the Certificate Request for each server. Perform the following steps to generate the certificate request:

a. Using the command line, navigate to the JRE bin directory (for the JRE installed with Service Desk - usually /SC/JRE)

b. Run the command "keytool -certreq -alias tomcat -keystore c:/certificates/keystore.jks -file servername-certreq.csr"
A .csr file is created in the c:/certificates directory on each server where you generated the certificate request.

c. Send the .csr files to the vendor of your choice who will then generate the appropriate certificates you need based on the certificate request, for each server.

Note: The certificate you receive from each is different. Some vendors will send you multiple certificated possibly including a root certificate, an intermediate certificate, and a certificate of authority. Each vendor has different instructions on which certificates they provide need to be imported into the keystore. So the key here is to ask the specific vendor that you used to generate the certificates for you, for specific instructions on how to import their certificates into a tomcat keystore.

Once you received the specific instructions from the vendor, you can follow those to import the appropriate certificates into the keystore on each server. Once that is complete, you can now configure Tomcat on the Service Desk side of things to point it to that keystore where the certificates have been imported.

3. Open the \bopcfg\www\CATALINA_BASE\conf\server.xml file using a text editor and locate the following:

```
<-- <Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="C:\Documents and Settings\user\.keystore"
keystorePass="password"/> -->
```

4. Change the code to the following:

```
<Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
```

```
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="C:\certs\keystore.jks"
keystorePass="password"/>
```

Note: Be sure to remove the <-- and --> tags that currently comment out the HTTPS /SSL connector for Tomcat, and set the appropriate path and password for your keystore that you generated in the beginning.

5. Save the server.xml file.

6. Restart Tomcat by using the following commands:

```
pdm_tomcat_nxd  - c stop
pdm_tomcat_nxd  - c start
```

Note: We recommend you to restart all the CA SDM servers to ensure that the Tomcat is restarted.

7. Test your tomcat SSL connection by opening a browser and navigating to the Service Desk URL, using the HTTPS protocol, and the tomcat port. For example, use the following URL:

```
https://servername:8080/CAisd/pdmweb.exe
```

The Service Desk Login Screen should open. You have successfully configured SSL on Tomcat.

System Configurations

Contents

To enhance the performance of CA SDM Servers, add or modify the processes and daemons. Configure object managers, web engines, web directors, and other processes for the CA SDM servers in your environment. You can add the processes across several servers to increase volume, performance, and enhance security.

Additional Processes

Depending on your configuration type, you can configure the following extra processes for the CA SDM servers:

Processes	Configuration details
Knowledge Daemons Login User Authentication LDAP Virtual DB	Applicable only to the conventional configuration. CA SDM configures these daemons by default on the primary server. You cannot delete the daemons but can move the daemons to a secondary server by changing the host name.
Repository daemons REST Web Services for Tomcat Server Visualizer	Applicable only to the conventional configuration. Using the CA SDM web UI, you can add these processes only for secondary servers. After you have added the process through the web UI, enable the specific option during the CA SDM configuration. For more information about enabling the processes, see the *Server Configuration Online Help*.
SA Main Server SA Dedicated Object Server SA Message Routing Server SA Socket Proxy Server	Applicable only to the conventional configuration. Using the CA SDM web UI, you can add the processes only for secondary servers. After you have added the process through the web UI, enable the specific option during the CA SDM configuration. For more information about enabling the processes, see the *Server Configuration Online Help*. You can only add one support automation process for each secondary server.
TNG converter UNI Converter	Depending on the operating system, you can add the processes to the following servers: Conventional: Primary server, secondary server. Advanced Availability: Application server.

Current Locks

Current Locks let you view and release locks on any object. During normal operations, the system locks objects while users work with data. If there is a system failure, you can free objects for future updates. Because the initial locks default to 5 (five) minutes, you unlock the objects when another user needs the same data.

View Current Object Locks

You can view a snapshot of currently locked objects.

Follow these steps:

1. On the Administration tab, select System, Current Locks.
   The Current Locks page lists the following information about object locks:

   - **Lock**
     Process that requested the lock.
   - **Name**
     The lock name. If the lock is related to a ticket, the lock name can reflect the ticket number.
   - **Table Name**
     Location of the locked object.
   - **Object Name**
     The Majic object.
   - **Lock Owner**
     The table user.
   - **Locked Since**
     Date and time of the object lock.
   - **Process**
     Process that initiated the lock.

2. Refresh the browser.
   The Current Locks page shows the most recent object locks.

Unlock Objects

You can review and release object locks to allow other users to access the object.

Follow these steps:

1. On the Administration tab, select System, Current Locks.

   The Current Locks page shows a list of object locks.

2. Refresh the browser.

The Current Locks page shows the most recent object locks.

3. Right click the row.

   A Delete Lock menu appears.

4. Click Delete Lock.

   A confirmation message appears.

5. Click OK.

   The Current Locks page updates and a message notifies you that the object is free.

Managing Your Database

This article contains the following topics:

You can run utilities to manage your database while CA SDM is shut down. If you are running database management utilities and using a database other than the CA SDM default repository, the database environment variables must be set.

Note: For information about setting environment variables, see the database documentation you are using.

Database Backup

You can back up the contents of a single database table, multiple database tables, or your entire CA SDM database, using the database backup utility, pdm_backup. The output of the backup utility is an ASCII file that the pdm_restore utility can use.

As part of its processing, pdm_backup first shuts down the daemons (UNIX) or services (Windows). pdm_backup stops CA SDM and then writes one or more tables from a CA SDM database to an ASCII file. You can use this output file as the input file to pdm_restore. In addition to the contents of the database, pdm_backup backs up application configuration files.

If you have operating environment-specific backup tools, we recommend that you use them instead of pdm_backup. Because pdm_backup is a generic tool, it can be slow on some operating environment combinations.

Note: As part of its processing, pdm_backup first shuts down the daemons (UNIX) or services (Windows).

Syntax

This command has the following format:

```
pdm_backup [-d] [-g] [-v] -f filename [ALL | table1...tableN]
```

-d

Specifies to back up the database data only.

-g

Specifies that only non-database data be backed up. This means only windows (forms) and other non-database data is backed up.

-v

Specifies verbose mode, which writes comments about command progress to stdout.

-f *filename*

Specifies an output file.

ALL|table1...tableN

Specifies ALL files or the table or tables to write. If more than one table is specified, separate each with spaces.

- You can find table names in the CA SDM database schema file, ddict.sch, located in $NX_ROOT /site (UNIX) or *installation-directory*\site (Windows). $NX_ROOT or *installation-directory* is the directory where you installed CA SDM.
- If no table is specified, the entire CA SDM database is written, including window groups and menu registration files.

Restrictions

pdm_backup cannot be run while CA SDM is active.

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

Database Restore

The database restore utility, pdm_restore, loads an output file from pdm_backup to the CA SDM database. The pdm_restore utility first shuts down the daemons (UNIX) or services (Windows). Then it restores, clears, and replaces all existing database records. Use the formatted ASCII file created by pdm_backup as input for the pdm_restore utility.

You can also use the pdm_restore and pdm_userload utilities to gain access to the CA SDM application in case of a catastrophic database corruption. If your database is damaged to the point where you cannot gain any access to the application and if all other measures have failed, rerun configuration and reinitialize the database to rebuild your database and populate reference data and system tables.

This procedure initializes your database in the same way that you did during the original installation. You can now access CA SDM. The pdm_restore utility can be used to restore the last backed up copy of your database.

For more information, see pdm_restore--Restore a Database (see page 947).

pdm_restore--Restore a Database

pdm_restore stops CA SDM and then deletes all records from a CA SDM database and replaces them with records from a file you specify with the -f option. The data from the input file is the only data that will be in the CA SDM database after running pdm_restore.

The input file must be created using pdm_extract or pdm_backup, or otherwise formatted for pdm_restore. pdm_backup can back up non-database data, and pdm_restore can restore this data also. pdm_backup and pdm_restore are not recommended when other backup and restoration tools are available.

Note: As part of its processing, pdm_restore first shuts down the daemons (UNIX) or services (Windows).

Syntax

This command has the following format:

```
pdm_restore [-d] [-g] [-n] [-w] [-v]  -f filename
```

Restrictions

pdm_restore can be run only on a CA SDM server. Only the privileged user or root can run pdm_restore. The following restrictions are applicable if you are using the advanced availability configuration:

- If you are restoring the database, run the pdm_restore command only on the background server.
- Ensure that you have stopped all servers (application, background, and standby) before you run the pdm_restore command.

Important! Use pdm_restore only with a full database backup created by pdm_backup, because your current database is deleted and replaced by the backup file. Do not run pdm_restore when users are logged in to CA SDM.

-d
Specifies that only database data is restored.

-g
Specifies that only non-database data be restored. Only windows (forms) and other non-database data are restored.

-n
Specifies that NX.env is restored if restoring non-database data. By default, NX.env is not restored. We recommend that the NX.env file not be restored unless the restore is to the same server the backup came from. Restoring an incorrect NX.env can affect unintended databases.

-w
Specifies that web.cfg is restored if restoring non-database data. By default, web.cfg is not restored.

-v
Specifies verbose mode.

-f *filename*

Specifies an input file that contains a full backup created by pdm_backup.

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

Database Table Replacement

This article contains the following topics:

The pdm_replace utility is a quick and easy way to replace the entire contents of a CA SDM database table with new information. This utility can be useful for massive revisions of look-up tables.

Note: pdm_replace takes the same input file format as pdm_userload. You can create an input file for pdm_replace using pdm_extract; however, you cannot use the output of pdm_backup as input to pdm_replace.

Note: For more information, see pdm_replace--Replace a Database Table (see page 949) and How to Create and Use an Input File (see page 965).

pdm_replace--Replace a Database Table

pdm_replace deletes a table in a CA SDM database and replaces it with a table from a temporary file you specify with the -f option; the data from the input file is the only data that is in that table after running pdm_replace. Back up your table before running pdm_replace.

Note: As part of its processing, pdm_replace first shuts down the daemons (UNIX) or services (Windows).

pdm_replace accepts a text file as input, which is the same file format used by pdm_userload. You can create an input file for pdm_replace using pdm_extract; however, you cannot use the output of pdm_backup as input to pdm_replace.

Important! Be sure to name your input file with a name different from the table name you are attempting to replace. For example, if you are replacing a table named ca_contacts and you name the input file ca_contacts.dat, after you execute the pdm_replace command to point to the input file (ca_contacts.dat), it deletes the file after execution because it has the same name as the table.

Restrictions

- pdm_replace can be run only on the following servers, depending on your CA SDM configuration:
  - Conventional: Primary server

- Advanced availability: Background server

  Important! Ensure that you have stopped all application and standby servers before running this command on the background server.

- Only the privileged user or root can run pdm_replace.
- Do not run pdm_replace when users are logged in to CA SDM.

Syntax

This command has the following format:

```
pdm_replace [-v] -f filename
```

-v

Specifies verbose mode.

-f *filename*

Specifies an ASCII file with the following format:

```
TABLE table_name
fieldname1fieldname2 . . . . fieldnameN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
.
.
.
{ "valueN1", "valueN2", . . . "valueNN" }
```

This format is the same file format used by pdm_userload. You can create an input file for pdm_replace using pdm_extract; however, you cannot use the output of pdm_backup as input to pdm_replace.

Data Extraction

The pdm_extract utility extracts data from the CA SDM database and produces output in various formats. You can further process this data or enter it into other applications, such as a spreadsheet or another database.

With the pdm_extract utility, you can do the following:

- Dump the entire CA SDM database
- Dump one or more database tables
- Extract specific information from the database and produce output in one of the following three formats:

- Output compatible with pdm_userload
- Comma-separated value (CSV) output
- Informal report-style output

For more information, see pdm_extract--Extract Data from Database (see page 951).

pdm_extract--Extract Data from Database

The pdm_extract command extracts data from specified CA SDM database tables or the entire CA SDM database, and outputs it as ASCII-formatted text.

Syntax

This command has the following format:

```
pdm_extract [-c|-e|-r] [-d] [-h] [-u] [-v] [-C] --B] [-f formatstring| ALL | table1 .
. . TableN]
```

-c

Produces comma-separated value (CSV) output, such as:

```
"field1","field2","field3"
```

The -c, -e, and -r output format options are mutually exclusive.

-e

Produces comma-separated value (CSV) output with embedded double quotes escaped by another double quote. For example:

```
"Text with a "quoted string" in it"
```

The -c, -e, and -r output format options are mutually exclusive.

-r

Produces left-justified output in the formats if the column labels are not supplied in the input file:

```
"label":"value"
```

or

```
"value"
```

This option is intended for use with line printers, for example:

```
Field_Name: Field Value
```

The -c, -e, and -r output format options are mutually exclusive.

-d

Uses the date format found in the file $NX_ROOT/fig/english/cfg/dataent.fmt (UNIX) or *installation-directory*\fig\english\cfg\dataent.fmt (Windows), which you can edit to suit your requirements.

-h

Displays help and usage information.

-u

Produces output without headers.

-v

Specifies verbose mode, which writes comments about command progress to stdout.

-C
Changes encoding from UTF-8 to another charset. The default output is UTF-8.
Example: To convert the output to JIS, you would run "-C iso-2022-jp"
Example: To encode to the operating system's native charset, use "DEFAULT" or "NATIVE".

-B
Suppresses the Byte Order Mark if the variable NX_ADD_UTF8_BYTE_ORDER_MARK is set.
The NX_ADD_UTF8_BYTE_ORDER_MARK option is a signature into a file. It allows editors that support UTF-8 to maintain the UTF-8 integrity of the file.
Note: This is only needed for non-ASCII data. If this is not installed, the default behavior omits the Byte Order Mark (BOM). If installed, set it to "1" or "Yes".

-f *formatstring*

Extracts specific records and fields according to *formatstring*, which is an SQL subset statement.

For a date after a period, use the following syntax:

pdm_extract -v -f "select id, ref_num from Call_Req where open_date >= DATE '2005-02-24'" > daterange1.txt

For a date range, use the following syntax:

pdm_extract -v -f "select id, ref_num from Call_Req where open_date >= DATE '2004-01-20' and open_date < DATE '2004-02-25'" > daterange2.txt

Note: Use single quotes around the date in the YYYY-MM-DD format.

The syntax for DATE is as follows:

```
DATE 'yyyy-mm-dd'
```

yyyy = integer representing year (between 1970 and 2038)

mm = integer representing month

dd = integer representing day

Examples:

```
DATE '2005-01-18'
DATE '1999-12-25'
```

The syntax for TIMESTAMP is:

```
TIMESTAMP 'yyyy-mm-dd hh.mm.ss[.nnnnnn][[+|-][hh.mm]]
```

yyyy = integer representing year (between 1970 and 2038)

mm = integer representing month

dd = integer representing day

hh = integer representing hour

mm = integer representing minutes

ss = integer representing seconds

nnnn = optional integer representing fractions of sec.

[+|-][hh.mm] = optional time zone interval.

Examples:

```
TIMESTAMP '1998-04-28 12:00:00.000000'
TIMESTAMP '2004-10-17 18:30:45'
TIMESTAMP '2005-03-21 12:00:12+08:00'
TIMESTAMP '1999-05-10 09:12:23.005-03:30'
```

Note: The -d option is not needed, as it only affects the format of the output.

A command usage example follows:

```
pdm_extract -f "select * from Call_Req where open_date > TIMESTAMP '2004-01-12 12:00:
00'"
```

In this example, all columns are being extracted from the Call_Req table where the open_date is after midnight 1/12/2004.

ALL

Extracts output from all tables in the database.

```
table1. . . tableN
```

Extracts output from the specified tables. Table names must be separated by spaces.

The default format, if none is specified, is an ASCII file compatible with pdm_userload.

Data Selection for Extraction

To select the data for extraction, the data extractor uses an integral SQL subset with the following rules:

- The following SQL functions are specifically supported in the subset:
  - IS NULL, IS NOT NULL, LIKE
  - SELECT statements and WHERE clauses
- The following SQL functionality is not supported in the subset:
  - Joins
  - Embedded tabs and new-line characters
  - Clauses other than SELECT, FROM, and WHERE
  - Asterisks (*) in SELECT statements
  - Nested SELECTs
  - Aggregate functions
- All SQL reserved words must be in uppercase characters
- Every token in a WHERE clause must be surrounded by white space
- All date/time specifications must be in one of three formats:
  - Elapsed seconds from 12:00:00 a.m. 1/1/1970 Greenwich Mean Time (GMT):

    ```
    start_date< or >174182431500
    ```

  - SQL DATE format:

    ```
    start_date< or >DATE '2001-11-28'
    ```

  - SQL TIMESTAMP format:

    ```
    start_date< or >TIMESTAMP '2001-07-04 15:45:00'
    ```

Note: TIMESTAMP format uses GMT. You can adjust time zones by adding or subtracting the appropriate number of hours, such as: 2001-03-23 14:00:00+02:00 or 2001-06-06 04:45:00-09:00.

Use the Data Extractor on UNIX

Before you use the CA SDM data extractor on UNIX, you must do the following:

1. Set the value of the $NX_ROOT environment variable to the full path name of the CA SDM installation directory that you defined during installation.
2. Append $NX_ROOT/bin to your PATH environment variable.
3. Set umask to 000.

Data Dereferencing

This article contains the following topics:

The pdm_deref utility is a dereferencing tool that converts data from various sources into a format suitable for loading into the CA SDM database. Dereferencing extracts internal IDs for cross-referenced fields. The utility can also be used to calculate down time and SLA down time values.

The pdm_deref utility converts data into one of the following formats:

- Output compatible with pdm_userload, suitable for loading into the CA SDM database
- Comma-separated value (CSV) output
- Informal report-style output

Note: For more information, see pdm_deref--Dereference ASCII Data (see page 955).

pdm_deref--Dereference ASCII Data

pdm_deref processes ASCII-formatted input to exchange data found in one database table for data found in another database table. It can be used to create files compatible with pdm_userload from a non-CA SDM database or spreadsheet. It can also be used to create reports or output files for a non-CA SDM database or spreadsheet.

Important! Do not use pdm_deref if you are unfamiliar with SQL. The directories "export" and "import" in $NX_ROOT/samples (UNIX) or installation-directory\samples (Windows) contain a standard set of specfiles for viewing.

Syntax

This command has the following format:

```
name pdm_deref  - s specfile [-c|-e|-r] [-d] [-h] [-n] [-u] [-v] <filename>
```

-s specfile

(Required) Specifies a file that defines which data is exchanged and the conditions under which it changes.

Specfile contains a list of SQL commands in the following format (note that "att" means attribute and "atts" means attributes):

```
Deref
{
input = <list of "from" atts from input file>
output = <list of "to" atts for output file>
rule = "SELECT <atts used to fill output atts> \
  FROM <table name>  \
  WHERE <att from table name to match input 1> =?\
  AND <att from table name to match input 2> = ? \
  OR <att from table name to match input 3> =?"
}
```

-c

Produces comma-separated value (CSV) output, such as:

```
"field1","field2","field3"
```

The -c, -e, and -r output format options are mutually exclusive.

-e

Produces comma-separated value (CSV) output with embedded double quotes escaped by another double quote. For example:

```
"Text with a "quoted string" in it".
```

The -c, -e, and -r output format options are mutually exclusive.

-r

Produces left-justified output in the formats if the column labels are not supplied in the input file:

```
"label":"value"
```

or

```
"value"
```

This option is intended for use with line printers, for example:

```
Field_Name: Field Value
```

The -c, -e, and -r output format options are mutually exclusive.

-d

Produces diagnostic information.

-h

Displays help and usage information.

-n

Specifies that you do not want to treat 0 valued foreign keys as NULL. This argument should be used only under special circumstances when recovering a damaged database.

-u

Produces output without headers.

-v

Specifies verbose mode.

filename

(Optional) Specifies the ASCII-formatted input file to be processed. If omitted, stdin is used.

Restriction -- **Valid on UNIX only**

Before using pdm_deref on UNIX, the $NX_ROOT environment variable must be set to the path of the CA SDM installation directory, and the PATH environment variable must include $NX_ROOT/bin.

Example: Using pdm_deref to Set Up Data for Input

This example shows how you can use pdm_deref to set up data for input.

Given the following data in the ca_location table:

```
id    location_name_name
86873FA40BA4234A8CF7A418D7C8B2DB    "Boulder NCC"
```

the following statement in the specfile:

```
Deref
{
input = place
output = location_uuid
rule = "SELECT id FROM ca_location WHERE location_name=?"
}
```

would change the following input:

```
last_name, first_name, place
{"Potts", "Elmore", "Boulder NCC"}
```

to the following output, which can be loaded into the ca.contact table with pdm_userload:

```
last_name, first_name, location_uuid
{"Potts", "Elmore", "86873FA40BA4234A8CF7A418D7C8B2DB"}
```

Example: Using pdm_deref to Set Up Data for Output

This example shows how you can use pdm_deref to set up data for output.

Given the following data in the ca_contact table:

```
id  last_name first_name
"69499D5A2424884887E62EC9823F5E47"    "Potts"    "Elmore"
```

the following statement in the specfile:

```
Deref
{
input = primary_contact_uuid
output = firstname, lastname
rule = "SELECT first_name, last_name FROM ca_contact
WHERE id=?"
}
```

would change the following input:

```
location_name, primary_contact_uuid
{"Boulder NCC", "69499D5A2424884887E62EC9823F5E47"}
```

to the following output, which can be printed or sent to a spreadsheet:

```
location_name, firstname, lastname
{"Boulder NCC", "Elmore", "Potts"}
```

Use the Dbadmin Mode

The dbadmin mode is a utility starts or triggers the data manipulation layer of the CA SDM system without starting the object layer. The utility provides the ability to lock the entire database to perform low-level data maintenance and data integrity.

For example, use pdm_extract, pdm_load, pdm_deref, and pdm_replace for performing batch data updates on the system. By using the dbadmin command, the administrator is essentially placing a database lock on the entire system. The backup (pdm_backup) and restore (pdm_restore) utilities, both automatically place the system in dbadmin mode to guarantee a consistent backup and restore.

The dbadmin mode is also useful to configure the system without starting the object layer until the data is modified. For example, an attribute “required” in majic on an existing system can confuse the animator if an update to an object that has the required attribute null. You can put the system into dbadmin mode and update the objects using pdm_load, and then start the system as usual.

Follow these steps:

1. Halt CA SDM either from Windows Service Manager or by running pdm_halt from the command line.

   Note: It is a good practice to send an announcement to alert users and to check for logged in users before halting the system.

2. From the command line, enter the following command using the same case as shown:

   ```
   pdm_d_mgr  - s DBADMIN
   ```

   Note: There is no return message, but a pause occurs before the command prompt returns. If there is no pause, check your spelling to verify that you entered data correctly.

3. Run pdm_status to verify that the system is in dbadmin mode.

   Note: When the system is in dbadmin mode, the system returns the following status, which indicates that it is safe to work on the system:

   ```
   C:\>pdm_status
   The Daemons are not running.
   ```

4. When all work is complete, run pdm_halt to shut down dbadmin mode.

5. Restart the system by following your usual procedures.

How to Use pdm_deref Example

The following example shows how to use the pdm_deref utility in a CA SDM ticket tracking system.

Assume that an existing ticket tracking system that you implemented on a spreadsheet has columns labeled Trouble Description, Technician First and Last Name, and Entry Date. These columns correspond to the description, assignee, and open_date fields in the CA SDM Change_Request table. The Trouble Description field contains the same data type as the description field. But the assignee field is a numeric field, and the Technicianfield on the spreadsheet is in a “last name, first name” format.

Follow these steps:

1. Load the technicians’ names into the Contact table.
2. Prepare a pdm_deref input file with the existing information.
3. Build a specifications file to map the new contact names to assignee values.
4. Prepare a pdm_userload input file to be used to update the Change_Request table.

This process is described in more detail in the following steps:

1. Prepare a pdm_userload input file, location.dat, for the Location table as follows:

```
TABLE ca_location
location_name address_2 address_2
{"Boulder NCC - NQ", "716 Main
    Street","Boulder, CO 84302"}
{"Colorado Springs NCC", "2765 Spring Street",
    "Colorado Springs, CO 84303"}
{"Denver NCC", "3765 Stoneridge Way", "Denver,
    CO 80254"}
```

2. Load the data as follows:

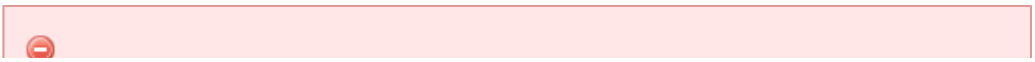
```
pdm_load -f location.dat
```

3. Prepare an input file, contact.dat, with the original information as follows:

```
TABLE ca_contact
last_name first_name middle_name location pri_phone_number
{"Harrison", "Frank," "Harold", "NCC - HQ", "303-555-2333"}
{"Hertzog", "William", "I.", "Colorado Springs NCC", "303-966-1987"}
{"Lyman", "Jeanie", "L.", "Denver NCC", "303-966-5301"}
```

4. Prepare a dereferencing tool specifications file, contact.spec as follows:

```
Deref
{
input = c_location
output = location_uuid
rule = "SELECT id FROM ca_location WHERE location_name=?"
}
```



Important! Do not place a blank space in front of the SELECT keyword. Deref uses the new contacts' first and last names to obtain the appropriate numeric ID fields for loading the Change_Request table. In addition, the "hooks" represented by question marks (?), correspond to the specified input fields. You must have the same number of hooks as input fields, and they must be in the same order.

5. Run pdm_deref as follows:

```
pdm_deref -s contact.spec < contact.dat > contact.out
```

The output file, contact.out, looks like the following:

```
TABLE ca_contact
last_name first_name middle_name location.uuid pri_phone_number
{"Harrison", "Frank", "Harold", "69499D5A2424884887E62EC9823F5E47", "303-555-
2333"}
{"Hertzog", "William", "I.", "86873FA40BA4234A8CF7A418D7C8B2DB", "303-966-1987"}
{"Lyman", "Jeanie", "L.", "58AA42789957734E8BEE146D07F7AD49", "303-966-5301"}
```

6. Load the contact.out file into the CA SDM database as follows:

```
pdm_load -i -f contact.out
```

Note: You must use the pdm_load command to use the - i option.

7. (UNIX only, optional) Write a script, Convert_Ticket, as shown in the following:

```
#!/bin/sh
pdm_load -i $1
cat $2 | pdm_deref -s $3 | pdm_load -i
```

You can run this script, as shown by the following:

```
Convert Ticket location.dat contact.dat contact.spec
```

In this example, pdm_load with the -i flag is used to speed the process. If you are making these updates on a regular basis, you can drop the -i flag so that pdm_load checks for duplicate records.

The following are additional examples of dereferencing tool specification files:

```
Deref
{
    input = first_name, last_name, middle_name
    output = assignee
    rule = " SELECT id from ca_contact \
           WHERE first_name=? \
           AND last_name=? \
           AND middle_name=? "
```

```
}
```

This rule converts three fields labeled first_name, last_name, and middle_name to the appropriate contact UUID. If all three input fields are not present, the rule is not applied. No match produces an error message and processing continues. For multiple matches, the first value is used; an error message is produced, and processing continues.

Database Loader

This article contains the following topic:

The database loader utility, pdm_userload, adds, updates, and deletes CA SDM database records. You create a formatted ASCII input file for the pdm_userload utility and select the tables to load and the optional fields to add.

Important! The pdm_userload utility accesses the CA SDM database and does not directly interact with application software processes. The inventory items added to the database with pdm_userload do not update the helper/selection lists until the application has been halted and restarted.

Although the pdm_userload utility can run with the application active, system performance is degraded. For best results, ensure that the background server is running but that no users are using the client interface before you run pdm_userload.

For more information, see pdm_userload--Add, Update, and Delete Database Records (see page 962).

Note: To add records with cross-referenced fields, use the pdm_deref utility pdm_deref--Dereference ASCII Data (see page 955).

pdm_userload--Add, Update, and Delete Database Records

The pdm_userload utility updates a CA SDM database using an input file you specify.

Important! You should always backup your database before you perform a pdm_userload.

Whenever you upload tickets (such as issues or requests), your ticket number should include a unique prefix or suffix in its string. CA SDM views this number as a string of characters not as a sequential number, and does not guarantee that it assigns a unique number to the uploaded tickets. As long as you assign a unique prefix or suffix using awk or another text processor, however, you can upload tickets without CA SDM writing over previously assigned numbers.

Syntax

This command has the following format:

```
pdm_userload [-a] [-c] [-h] [-r] [-v] [-u] [-m]  - f filename
```

Input File Format

The input file entries follow this format:

```
TABLE table_name
fieldname1fieldname2 . . . . fieldnameN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
.
.
.
{ "valueN1", "valueN2", . . . "valueNN" }
```

table_name is the name of the table to be loaded, as listed in the CA SDM database schema file, which is located in $NX_ROOT/site/sch/schema.sch (UNIX) or *installation-directory*\site\sch\schema.sch (Windows), where $NX_ROOT or *installation-directory* is the directory where you installed CA SDM.

-f filename

Specifies an input ASCII file.

-a

Updates all existing records, regardless of whether more than one existing record matches a single input record. Without this option, input records that match more than one existing record are rejected.

Important! Use this option carefully.

-c

Checks the input file against the database and reports on the updates that would be made, but does not make the updates.

-r

Removes database records that match input records. The -a option can be used with the -r option.

Note: Make a backup copy of the database before running pdm_userload with this option. old database records are removed, you must restore the CA SDM database with this backup copy if you wish to recover any deleted records.

-v

Specifies verbose mode.

-u

Updates existing records, but does not insert new records into the database.

-m

Mass update. Specify when you are using pdm_userload to add or delete a large number of records. This option suppresses all client notifications of updates and sends a cache refresh message for a table when pdm_userload finishes processing the table.

-x
Uses locale sensitive numeric input formats.

-t
Specifies the name or UUID of tenant to associate all loaded data with the specified tenant. This argument is valid only when multi-tenancy is installed.

Pdm_userload supports new arguments on the TABLE statement, "Truncate" and "NoNewID". These arguments are specified in an optional parenthesized option after the table name. For example:

```
TABLE Call_Req (TRUNCATE, NONEWID)
```

- **Truncate**
  Causes pdm_userload to issue a database-specific TRUNCATE command for the table prior to loading any data. In addition, it forces pdm_userload logic to use insert-only logic regardless of command-line arguments, as all records are new.

- **NoNewID**
  Causes pdm_userload to use the id value from its input control file for new rows in the table, rather than generating a new ID for inserted data.

Restrictions

You can run pdm_userload while CA SDM is active, but performance can become very slow. It is best to run pdm_userload when no one is using CA SDM.

Drop and Restore Constraints

Some of the mdb tables that start with ca_ (such as ca_contact_) have referential constraints that may impact mass loading of data using pdm_load, pdm_userload, and pdm_restore tools. If mass loading these tables is required, you may need to drop the referential constraints prior to mass loading of the data.

Two SQL scripts are provided for each DBMS type to drop and restore constraints. Prior to mass loading of data affecting ca_* tables, run the Drop version of the script. After the data load has completed, run the Add version of the script.

For SQL Server the scripts are located in *installation-directory*\samples\views\SQLServer directory. Run the following command to drop constraints:

```
osql -E -e < SQLDropConstraints.sql'
```

Run the following command to add back constraints:

```
osql -E -e < SQLAddConstraints.sql
```

For Oracle, the scripts are located in *installation-directory*\samples\views\Oracle directory.

Run the following command to drop constraints:

```
sqlplus mdbadmin/ <password> < OracleDropConstraints.sql
```

Run the following command to add back constraints:

```
sqlplus mdbadmin/ <password> < OracleAddConstraints.sql
```

How to Create and Use an Input File

You can use an input file and the pdm_userload utility to populate database tables.

The input file format is as follows:

- Surround field values with double quotes (“value”) and separate values with a comma and a space (“value1”, “value2”).
- Precede double quotes with a backslash (\) to embed them in text strings. To set a date/time field to the current date and time, use @NOW@ for the input value.
- Surround each record with curly braces separated by spaces, as follows:

  ```
  ( { record field values } )
  ```

- If properly delimited, input records can span more than one line in the input file as long as individual fields stay on one line. For a multi-line field such as comments, values can include a new line character (\n) to force a new line when the database field is displayed.
- Explicit new line characters are needed only for special formatting. Ordinary running text is automatically displayed with appropriate line breaks, as shown by the following example:

  ```
  "Record status is \"COMPLETE\""
  ```

To create an input file for the pdm_userload utility, perform the following steps:

Follow these steps:

1. Determine which table you want to load, and the fields you want to populate in that table. You must populate the Name or Symbol key field for each record that you load.
2. Make a copy of the appropriate *filename*.dat file for the table that you are loading.

3. Edit your newly created copy of the *filename*.dat file, as follows:

    a. Add an entry for each record to be loaded.

    b. From under the TABLE line (see the following example), remove fields that you do not want to populate.

    ```
    TABLE table_name
    fieldname1 fieldname4 . . . fieldnameN
    ```

4. Save your file and exit from the editor.

5. Run the pdm_userload utility and specify the file, as shown by the following example. In this example, the input file name is myData.dat:

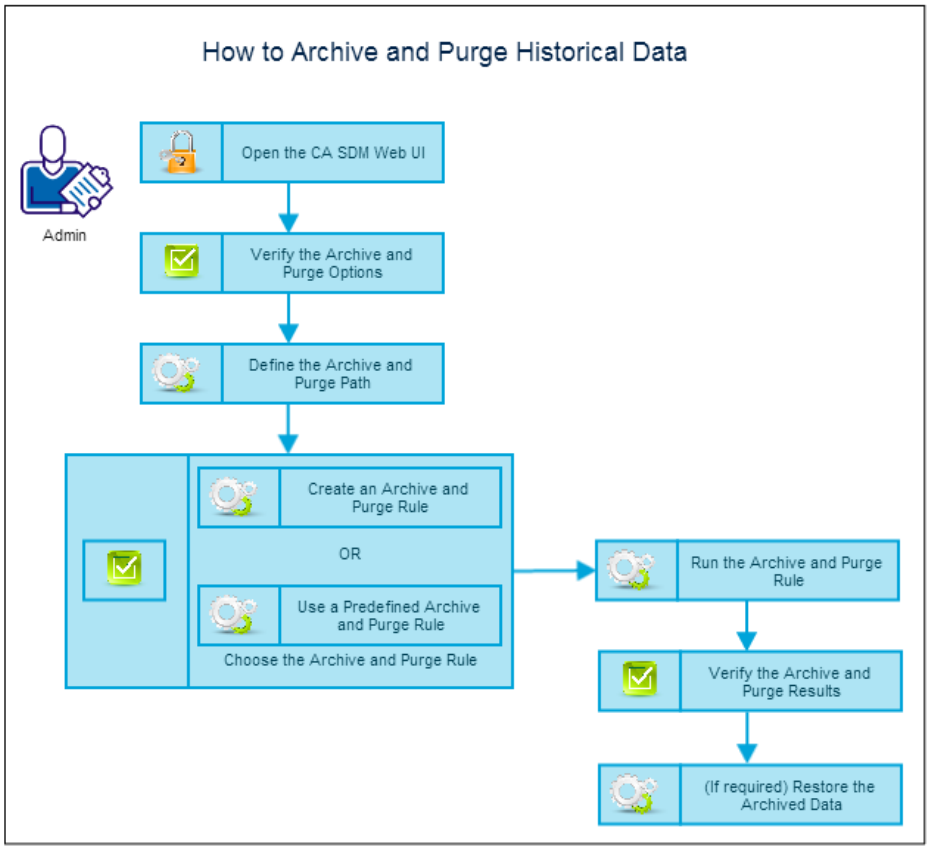
    ```
    pdm_userload -f myData.dat
    ```

    The database table is populated.

How to Archive and Purge Historical Data

Periodically remove the historical records from the system to keep the database at a manageable size for optimum performance. You create rules or activate the predefined rules to archive the historical records and purge them from the database.

The following diagram shows how to archive and purge the historical data:



Follow these steps:

- Open CA SDM Web UI (see page 967)
  - Verify the Archive and Purge Options (see page 968)
  - Define the Archive and Purge Path (see page 968)
- Choose the Archive and Purge Rule (see page 969)
  - Create an Archive and Purge Rule (see page 969)
    - Archive and Purge Rule Fields (see page 971)
  - Use a Predefined Rule (see page 972)
- Verify the Archive and Purge Results (see page 973)
  - View the Archive and Purge History (see page 973)
  - View the Archive and Purge Log File (see page 973)
- (If necessary) Restore the Archived Data (see page 973)

Open CA SDM Web UI

Log in to the web UI from the following servers, depending on your CA SDM configuration:

- Conventional: Primary or secondary servers
- Advanced availability: Application or background servers

Verify the Archive and Purge Options

Before you set up the archive and purge rule, verify the archive and purge options that you may require to install or uninstall, depending on your organization needs. For example, the default_schedule option specifies the default schedule (workshift entry) used by the archive and purge rules. If the option value is set to an invalid workshift entry name or empty string, the rule does not execute the rule with the schedule value. The option value field sets the NX_DEFAULT_SCHEDULE variable, which is located in the NX.env file.

Select Options Manager, Archive and Purge on the Administration tab. Install or uninstall the option that you require.

Define the Archive and Purge Path

You can define the location where you want to store the archived data. This path can be the root directory of a remote server or a UNC path. Depending on your CA SDM configuration, the following servers must run on Windows to access the UNC path:

- Conventional: Primary server
- Advanced Availability: Background server

Follow these steps:

1. Log in to web UI from the following CA SDM servers, depending on your CA SDM configuration:
   - Conventional: Primary or secondary servers
   - Advanced Availability: Application or background servers
2. To archive and purge attachments, complete the following steps:
   a. Select Attachments Library, Repositories on the Administration tab.
   The Repositories page opens.
   b. Right-click on a repository (such as Service Desk) and click Edit.
   The repository details page opens.
   c. Edit the following fields:
      - **Archive Type**
        Specifies the archive and purge action to be taken on the contents of the repository. Following values are valid:
        None: No archive and purge process is performed.
        Archive and Purge:The historic records are written to the file specified in the archive field and purged from the database.
        Purge Only:The historic records are purged from the database, but are not written to the archive file.
      - **Archive Path**
        Specifies the directory path or the UNC path to which files in the repository are moved during the archive process.

- **UNC Credentials**
  Specifies the credentials to access the UNC path. Click UNC Credentials to open the Credentials Search page.

  - If you have already created the credentials to access the specified UNC path, search using the fields and select the credentials.

  - If you want to create the credentials, click Create New. For more information about creating credentials, see the Create UNC Credentials (see page 1096) topic.

d. Click Save.

3. If you want to archive and purge data other than attachments, complete the following steps:

   a. Select Archive and Purge, Archive and Purge Settings on the Administration tab.

   b. Enter the path where you want to store the archived and purged data as the Archive Purge Rule Path.

   c. If you are using a UNC path to store the archived data, click UNC Credentials.
   The Credentials Search page opens.

      - If you have already created the credentials to access the specified UNC path, search using the fields and select the UNC credentials.

      - If you want to create the credentials, click Create New. For more information about creating credentials, see the Create UNC Credentials (see page 1096) topic.

   d. Click Save.

The archive and purge path is defined.

Choose the Archive and Purge Rule

You are required to select the appropriate archive and purge rule. Consider the following possibilities:

- Create an archive and purge rule (see page 969). For example, you create an archive and purge rule for Knowledge Management forums.

- Use a predefined archive and purge rule (see page 972). For example, you use the predefined rules for archiving and purging KPI data.

Create an Archive and Purge Rule

Before you can perform an archive or purge, you create a rule. The rule defines what you want to archive and when.

Example: You create an archive and purge rule to remove deleted forums from the database.

Follow these steps:

1. Select Archive and Purge, Archive and Purge Rules on the Administration tab.
   The Archive and Purge Rule List page opens.

2. Click Create New.
   The Create New Archive and Purge Rule page opens.

3. Complete the archive and purge rule fields (see page 971), as appropriate.

   - Select knowledge document as the Config. Object Name.
   - Add KS_TYPE=20 as the Additional Query.

4. Click Save.
   The new rule is displayed on the Archive and Purge Rule List page.

Example: You create an optional configuration rule inside the arcpur_cfg.xml and itil_arcpur_cfg.xml files to archive and purge the KPI_Ticket_Data node.

Follow these steps:

1. Log in to the following server, depending on your CA SDM configuration:

   - Conventional: Primary server
   - Advanced availability: Background server

2. Find the following files in the $NX_ROOT/site/cfg/ directory:

   - arcpur_cfg.xml
   - itil_arcpur_cfg.xml

3. Edit the files to define the end_time (last_mod_dt) in KPI_Ticket_Data node. It specifies the criteria to select the records for archive and purge.

4. Link the records in the KPI_Ticket_Data table to the records in the Ticket table (such as cr, chg, or iss). This ensures that all ticket-related records in the KPI_Ticket_Data table are archived and purged.

5. KPI_Ticket_Data node does not have a SREL relationship with any Ticket node and it relies on two fields, obj_name, and obj_id, to link with a ticket. The obj_name value can be cr, chg, or iss and the obj_id value is the ticket id. Define a main_obj for each ticket object.
   The following is a sample main_object definition for the ticket object, cr:

```
<!-- KPI Ticket Data -->
<main_obj>
<name>KPI Ticket Data</name>
<internal_name>KPI Ticket Data</internal_name>
<factory>ktd</factory>
<default_query>obj_name='cr'</default_query>
<date_field>end_time</date_field>
<ref_by value="obj_id">cr.id</ref_by>
</main_obj>
```

Note: The configuration rule can only select records for cr. The ref_by tag can match the value of obj_id in KPI Ticket Data to the value of id in cr. If a match is found, it means that a KPI Ticket Data record is referenced by a cr record, so the KPI Ticket Data record is not archived and purged.

6. After adding the configuration rules for all ticket objects, depending on your CA SDM configuration, perform the following steps:

   - Restart the CA SDM servers for conventional (see page).
   - Restart the CA SDM servers for advanced availability (see page 866).

   These configuration rules become selectable configuration object names in the Archive and Purge Rule Detail form.

Archive and Purge Rule Fields

You can use the following fields to define or edit rule definitions.

- **Rule Name**
  Specifies a unique identifier for the rule.
- **Status**
  Indicates whether this rule is active. The inactive rule runs only once, even if it is scheduled for a recurrent process.
- **Schedule**
  Specifies a workshift during which the rule should be in effect.
- **Recurrence Interval**
  Specifies how often this rule will run.
- **Archive File Name**
  Specifies the name of the file where you want to store the historic records. Enter the file name that you have mentioned while defining the archive and purge path. For more information, see the Define the Archive and Purge Path (see page 968) topic.
- **Operation Type**
  Specifies one of the following types of operation that the rule must execute:
  - **Archive/Purge**
    Archives the historic records to a file and purges the archived records from the database.
  - **Purge Only**
    Purges historic records from the database, but they are not written to the archive file.
  - **Archive Only (Test Run)**
    Writes historic records to the archive file without purging them from the database. Use this option to test a newly created or edited archive and purge rule.

- **Config. Object Name**
  Specifies the name of the database object this rule can archive and purge. The Object Name field is automatically populated according to your selection in the Config. Object Name field.

- **Days Inactive**
  Specifies the number of days a record is inactive to be eligible for the archive and purge from the database.

- **Additional Query**
  Archives and purges specific inactive records among the existing inactive records. Use this field when you want to create different rules for archiving and purging the subsets of expired records for the same object. Use the same syntax as you use for stored queries.
  The following query archives and purges only assigned inactive request records with a priority of 1:

  ```
  priority = 1 AND (assignee IS NOT NULL OR group IS NOT NULL) and active = 0
  ```

  The following query format archives and purges records that are based on time-span:

  ```
  close_date < EndAtTime(\'LAST_YEAR\')
  ```

Use a Predefined Rule

You can use the predefined rules in CA SDM to archive and purge historical data. These predefined rules are set to Inactive, by default. Set it active to use the rule.

Example: Use the predefined rule to archive and purge the KPI data.

Follow these steps:

1. Select Archive and Purge, Archive and Purge Rules on the Administration tab.
2. Search for any of the following predefined rules for KPI data:
   - KPI Ticket Data
   - KPI Data (System)
   - KPI Data (Stored Query)
   - KPI Data (SQL)
3. Select the rule from the search result.
4. Click **Edit** to modify the archive and purge rule fields (see page 971).

Important! Ensure that you select the **Active** option from the **Status** field.

5. Click Save.
   The predefined rule is ready for use.

Verify the Archive and Purge Results

You check the results of the archive and purge rule that you have scheduled. Do one or both of the following actions:

- View the Archive and Purge History (see page 973).
- View the Archive and Purge Log File (see page 973)

View the Archive and Purge History

You can view the history for each archive and purge rule. For example, view the objects that are purged by a rule.

Follow these steps:

1. Select Archive and Purge, Archive and Purge History on the Administration tab.
   The Archive and Purge History List page opens.
   Note: To display the Additional Search Arguments field, click the spigot icon. This field is intended only for expert users who understand SQL and Majic and can use it to specify search arguments that are not available in the standard search filter fields. To specify an additional search argument, enter a SQL WHERE clause in this field.

2. Click Show Filter and specify the filter criteria. For example, enter the earliest start date to show only entries from the specified time frame.

The list of matching rules are displayed.

- Click the rule name for which you want to review the rule configuration.
  The Archive and Purge Rule Detail page opens.

View the Archive and Purge Log File

You can check the arcpur.log file from the $NX_ROOT/log/ directory to find the errors that have occurred while executing the scheduled archive and purge rule.

Note: The size limitation for arcpur.log files is defined in $NX_ROOT/NX.env as

```
# The size limit for the Archive and Purge log file and data file.
@NX_ARCPUR_FILESIZE=2000000000
```

Archive and purge creates arcpur.log.0, arcpur.log.1 though arcpur.log.9 after reaching the file limit for each log files.

(If necessary) Restore the Archived Data

You can restore the archived data when you need them in the database again.

Follow these steps:

1. Start the daemons in dbadmin mode. Dbadmin mode allows limited access, so you can safely run pdm_load to restore the archived data. Run the pdm_d_mgr -s DBADMIN command on the following servers, depending on your CA SDM configuration:
   - Conventional: Primary server
   - Advanced Availability: Background server
2. Go to the root directory or the UNC location where you have stored the archived data.
3. Locate the archived data file (.dat file).
4. Copy the file to the following servers, depending on your CA SDM configuration:
   - Conventional: Primary server
   - Advanced Availability: Background server
5. Run pdm_load against the data file. For example:

   ```
   pdm_load -a -f 2004611T1726_Call_Request.dat
   ```

6. If there is a problem with the pdm_load command, complete the following steps:
   a. Check the command line and $NX_ROOT/log/arcpur.log for errors.
   b. Restart the CA SDM servers (see page 866).
7. To prevent the record from being archived and purged at the next cycle, complete the following steps:
   a. Update the record to make it active again.
   b. Inactivate the associated archive and purge rule.

Setting Up Multi-Tenancy

This article contains the following topics:

Manage Multi-Tenancy

This article contains the following topics:

How to Initialize a New Tenant

As the service provider, you may want to build a standard set of data for a new tenant, such as categories, data partitions, ticket templates, and so on. This task can be done by using pdm_extract or pdm_tenant_extract to build a pdm_userload input file containing the data you want.

If necessary, you can edit this file with any text editor. It can then be loaded into the database using pdm_userload with the -t argument to set the tenant column to the new tenant.

The following process describes how to initialize a new tenant:

1. Create the tenant in the ca_tenant table. Use the online Create Tenant (see page) page.

2. Load the standard data as previously described.
   Use pdm_userload -t to set the tenant.

3. Create contact records for the new tenant.
   Load outside data or use pdm_userload -t.

How to Convert an Existing Tenant Implementation to the Tenant Object

You may have used data partitions and another CA SDM object to achieve some of the functionality now provided by multi-tenancy. If you want to convert an implementation to multi-tenancy, the first step is to map the data in the previously-used object to the new tenant object. The previously-used object is called the *pre-tenant* object. For most sites with these requirements, the org (organization) object is the pre-tenant object, but the following approach can be used for any pre-tenant object.

1. If the pre-tenant object is not org, verify that its Majic object definition specifies TENANT_REQUIRED.

2. Verify the attribute mappings from the pre-tenant object to the new tenant object in the buildtenant.xml file in the following location:
   $NX_ROOT/samples/multi_tenancy

Note: You must copy buildtenant.xml to the $NX_ROOT/site/cfg directory. In addition, buildtenant.xsd must be in the same directory as buildtenant.xml, or you will receive an error. When you install the product, buildtenant.xsd is located in $NX_ROOT/site/cfg, so you do not have to copy this file.

The default settings are based on org. If the pre-tenant object is not org, you must edit the file.

3. Run pdm_buildtenant -f (see page 983).
   A new tenant is created for each pre-tenant object, and sets the tenant attribute in the pre-tenant object to reference the new tenant.

4. Log in to CA SDM, and review both the tenant object and the pre-tenant object.

> **Note:** In some situations, you want to map multiple pre-tenant objects to a single tenant object. To do this, manually update the pre-tenant objects affected, and then delete or inactivate the unused tenants.

How to Populate the Tenant Attributes in Your Tables

To populate the tenant attribute in all or a subset of a table, use the *pdm_settenant* utility. This utility uses a configuration file to select the objects to be tenanted and to specify where to obtain the tenant for the objects. You can specify an explicit tenant, or specify that the tenant should be derived from an SREL reference in the object to be tenanted.

To populate the tenant attributes in your tables using pdm_settenant, complete the following steps:

1. Create or edit a configuration file.
   The configuration file selects the rows that will have their tenant attribute set and specifies a source for the tenant attribute's value. The product provides a sample settenant.xml file in the following location:
   $NX_ROOT/samples/multi_tenancy

> **Note:** You can modify the sample settenant.xml file, or create a file and copy it to the $NX_ROOT/site/cfg directory. In addition, settenant.xsd must be in the same directory as settenant.xml, or you will receive an error. When you install the product, settenant.xsd is located in $NX_ROOT/site/cfg, so you do not have to copy this file.

2. Run pdm_settenant -f [configuration file] -r (see page 985)
   The pdm_settenant utility reads its configuration file and processes each rule it defines in sequence.
   We recommend that you use this utility first to populate the tenant attribute in the cnt (contact) object, and then use the cnt object as a source for populating tenant into other objects.
   After the cnt object is properly tenanted, it can be used as a base for setting tenant in other tables by completing the following steps:

   a. Specify a TenantRule with type="SREL" in the configuration file for an attribute referencing the cnt object to set tenant in other tables.

b. (Optional) Specify a TenantRule with type="Name" < tenantname > to set tenant explicitly in some of the tables.

3. Run pdm_settenant with a new configuration file.

4. Rerun pdm_settenant as required.
   After you have populated the tenant column in an object, you can use SRELs to that object as the basis of an SREL TenantRule for setting tenant in other objects.

Example: SREL Type Syntax

SREL type syntaxt checks for cnt objects that do not have a tenant value specified and uses the tenant value from the linked organization object:

```
<Object name="cnt">
<TenantRule type="SREL">organization</TenantRule>
<Where>tenant is null</Where>
</Object>
```

Example: Name Type Syntax

Name type syntax checks for org objects that do not have a tenant value specified and sets their tenant field to the name of an actual Tenant object:

```
<Object name="org">
<TenantRule type="Name">Tenant A</TenantRule>
<Where>tenant is null</Where>
</Object>
```

Tenant Hierarchies

A *tenant hierarchy* is a structured tenant group that is system-created or modified when you assign a *parent tenant* to a tenant. The tenant becomes a *subtenant* of the parent and higher tenants (if any) in that hierarchy.

Note: The service provider can create multiple unrelated hierarchies, or none. Even in a system with tenant hierarchies, you can define standalone tenants.

A subtenant typically represents a subdivision within its *supertenants*. A subtenant can have its own business rules and data, and supertenant data is "pushed" to the subtenant automatically on a read-only basis.

CA SDM supports a tenant hierarchy of unlimited depth. However, the *service provider* can specify a limit on the total number of tenants and the depth of tenant hierarchies (default is four levels). The service provider also determines whether individual tenants can have subtenants.

Note: The service provider can participate in tenant hierarchies, but this is not required. The service provider cannot have a parent tenant.

Create a Subtenant

Subtenancy allows you to build and modify tenant hierarchies for organizational and data-sharing purposes. To place a tenant into a tenant hierarchy, you assign it a parent tenant.

Follow these steps:

1. On the Administration tab, select Security and Role Management, Tenants.

   Note: The Security and Role Management, Tenants option is available only when multi-tenancy is enabled.

2. Click an existing tenant to Edit, or click Create New.
   Enter any required data or changes.

3. Select a Parent Tenant.

   Note: The Parent Tenant drop-down only displays tenants that are allowed to have subtenants.

4. Click Save.
   The tenant is a subtenant of the parent tenant.

   Note: When a tenant is a subtenant, it belongs to the Subtenant group of the parent tenant, as do the subtenants (if any) of that subtenant, and so on. The parent tenant joins the Supertenant group of the subtenant, as do the supertenants (if any) of that supertenant, and so on. Each joins the Related Tenants group of the other.

System-Maintained Tenant Groups

CA SDM generates and maintains three tenant groups automatically for each tenant in a tenant hierarchy (*tenant* is the tenant name):

- *tenant*_subtenants (tenant, its child tenants, and their lower subtenants)
- *tenant*_supertenants (tenant, its parent tenant and its higher supertenants)
- *tenant*_relatedtenants (entire single hierarchy)

System-maintained tenant groups can be used like user-defined tenant groups. However, only their names and descriptions can be modified.

Tenant Data Assignments

CA SDM displays the tenant in the same format in both the View and Edit versions of a detail page for an existing object, because the tenant for an existing object cannot be changed from the web interface.

When you edit a tenanted object, drop-down lists on the edit page are automatically restricted to values that are public, owned by the same tenant as the base object or any tenants above it in the tenant hierarchy, or owned by the service provider (if the drop-down list applies to a SERVICE_PROVIDER_ELIGIBLE attribute).

There are no changes on the detail page for lookup fields associated with a tenanted object. If a user with access to multiple tenants clicks a lookup link to a tenanted table, the web engine automatically restricts the lookup to values appropriate for the attribute, and displays a banner message on the pop-up search or list page.

Note: Tenant restrictions are not displayed in the search filter, and they cannot be changed by the user.

Tenant becomes a selector (either a lookup or a drop-down list) when you ask to create a tenant-required object.

If the tenant field is empty, you can specify a tenant value directly by filling in the field, or indirectly by specifying a value for a tenant-implying attribute (such as Affected End User). The interface displays the following suffixes:

- **(T)**
  Indicates an attribute that is tenant-implying; that is a lookup to a tenant-required table.
- **(TO)**
  Indicates an attribute that is optionally tenant implying that is, a lookup to a tenant-optional table.

web.cfg properties control the text of these indicators.

Except for the tenant attribute itself, tenant-implying attributes are always shown as lookups, even if created with a dtlDropdown macro.

CA SDM automatically sets the tenant when you look up or autofill a tenanted value into any tenant-implying field (except that filling a SERVICE_PROVIDER_ELIGIBLE field with a reference to a service provider object does not set the tenant). After the tenant is set, lookups for tenant-implying fields are restricted in the same way as existing tenanted objects.

Note: Until you save the object, the tenant field remains editable, and you can change the tenant by directly updating it. When you change the tenant, CA SDM automatically clears any tenant-implying fields containing references to objects belonging to the previous tenant.

CA SDM typically initializes the Tenant selector to empty. You can change this behavior in several ways:

- Open the Create New page from a page such as the Quick Profile, which pre-populates a tenant-implying field
- Set the Retain Tenant user preference
  This is a new user preference that initializes the tenant for new objects to the same tenant as the last detail page viewed or updated, or in the last list page search filter restriction.
- Open the page with a URL that explicitly specifies a tenant
  This is not provided in any predefined URL, but is available to allow sites to create menu items or buttons that specify a tenant.

Note: If you create configuration items from another CA Technologies product (such as CA APM) or the command-line interface, then the object is Public.

Create a Tenanted Object

The service provider can add tenant-specific data to objects such as issues, requests, change orders, and so on. You can add a tenant to a ticket (such as an incident) that is created from a Scoreboard tab.

Follow these steps:

1. Click File, New Incident.
2. Complete any of the following steps:
   a. Select the tenant from the Tenant drop-down.
   b. Click Affected End User (or any other tenant-implying field).
      The Contact Search page appears. Search for a user; you can filter the search by tenant.
   c. Enter a name into the Affected End User field.
      The tenant data completes automatically.
3. Continue to create the incident.

Activity Notifications

Activity Notifications control both the contents of notifications and which contacts receive notifications for various events in the history of a ticket.

In a multi-tenancy environment, the notification rule is a tenant-optional object. Public notification rules apply to all tickets; tenanted rules apply only to tickets with the same tenant as the rule, or to tenants in its subtenant hierarchy. The tenanting restriction is applied in addition to any condition specified with the rule itself.

Default Notification Rules are stored as public objects. If multi-tenancy is installed, you must create a copy of the Notification Rule for each of the tenants, otherwise the Update Contacts option is restricted.

Repositories

The repository (doc_rep) object is tenant-optional. Tenants can define their own repositories, and it is possible to define public repositories for objects such as attachments to public knowledge documents. Each tenant can have its own default repository, and you can specify a default public repository.

All attachments are either public or associated with a single tenant. If a tenant does not have its own default repository, the public repository is displayed as the default for its tenanted objects.

How to Export and Import Tenant Data

This article contains the following topics:

The service provider can extract tenant data from an existing multi-tenancy implementation and import it into a new system.

Note: Depending on the volume of your data, the extraction process can take several hours. You may have to perform the extract and import in multiple phases, as follows:

- **Initial**
  Extracts a base line and creates a control file used in subsequent phases .
- **Update**
  Uses the control file to extract only data that has changed since the previous run.
- **Final**
  Performs the same steps as Update, except that it also extracts animations. Animations are omitted from both the Initial and Update phases.

To extract data from one database and import it into another, complete the following steps:

1. Run an initial phase of pdm_tenant_extract (see page 989) to extract base-line data. This builds the control file used by subsequent phases.

2. Prepare a new, clean MDB for the extracted data.

   Important! The output from the initial phase *must* be loaded into a database that has never been used for the product or for any other product. Each table loaded from initial phase data is truncated prior to the load, which could cause loss of data if the database is already in use.

3. To avoid duplicate privileged contacts appearing on the new system, you must inactivate the privileged contacts. Log onto CA SDM and change the Status of these contacts to "inactive" before loading the extracted data.

4. To avoid referential problems during the data load, run the appropriate drop constraints script:

   - (Oracle) Run $NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql
   - (SQL Server) Run $NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql

5. Use pdm_userload (see page 990) to load the data from the initial phase into the clean MDB prepared in steps 2 and 3.

6. Run an update or final phase of pdm_tenant_extract to extract additional data created or modified since the previous phase. Pdm_tenant_extract uses the control file created in step 1 to determine the data already processed by the previous phase.

7. Use pdm_userload to load the data extracted in step 5 into the same MDB containing data loaded from the previous phases.

   Note: For more information about this utility, see pdm_userload (see page 990).

8. Repeat steps 5 and 6 as required until all data has been imported into the new database. The last run should be the final phase.

9. To protect the integrity of the new database, restore the constraints dropped in step 3 by running the appropriate add constraints script:

   - (Oracle) Run $NX_ROOT/samples/views/Oracle/OracleAddConstraints.sql
   - (SQL Server) Run $NX_ROOT/samples/views/SQLServer/SQLAddConstraints.sql

10. Use pdm_tenant_delete (see page 987) to delete the extracted data from the original database.

11. Ensure that all repositories associated with extracted tenants are copied to the target settings.

How to Handle Attachments and Repositories

Attachments are stored in repositories. You must copy all repositories that are associated with extracted tenants to the target system, including public repositories. This process is primarily a manual operation, with the following steps:

1. Redefine location-specific information for all repositories, after completion of the initial load of the data into the target system. This task includes changing the following values:
   - Server Name
   - Upload Path
   - Servlet Path
   - Archive Path
2. Manually create all required directories and folders.
3. Copy all attachment files from the previous location to the new repository location after (or during) the load of the data from the Final phase.

After you complete these steps, all references for attachments in the target system should be successful. However, copies of the attachments remain on the source system. Use the pdm_clean_attachments.pl utility (see page 985) to clean these redundant attachments.

Utilities Used for Multi-Tenancy

This article contains the following topics:

This section describes utilities that are used to manage a multi-tenancy environment.

Note: Required parameters are enclosed within "{ }", while optional parameters are in "[ ]".

pdm_buildtenant -- Creating Tenants from Another Object

The *pdm_buildtenant* utility is used to create tenants from another object. You may have used data partitions and another CA SDM object to achieve some of the functionality now provided by multi-tenancy. If you want to convert an implementation to multi-tenancy, the first step is to use pdm_buildtenant to map the data in the previously-used object to the new tenant object.

Important! Before you run pdm_buildtenant, you *must* configure the service provider.

In this section, the object used to hold tenant-like information is named the pre-tenant object. For most sites with these requirements, the org (organization) object is the pre-tenant object, but the following approach can be used for any pre-tenant object.

The pdm_buildtenant utility builds the tenant objects from pre-tenant objects. This application creates a tenant for each pre-tenant object, and sets the tenant attribute in the pre-tenant object to reference the new tenant. This utility has the following syntax:

```
pdm_buildtenant [-h] | [-f [configuration_file]
```

- **-f configuration_file**
  (Optional) Specifies the location of a configuration file specifying the rules for creating tenants from the pre-tenant object. If this argument is not included, pdm_buildtenant uses the configuration file from the $NX_ROOT/site/cfg directory. This file assumes the pre-tenant object is org; if this is not the case, you *must* edit the configuration file before using pdm_buildtenant.

  Note: You *must* copy buildtenant.xml to the $NX_ROOT/site/cfg directory. In addition, buildtenant.xsd must be in the same directory as buildtenant.xml, or you receive an error. When you install the product, buildtenant.xsd is located in $NX_ROOT/site/cfg, so you do not have to copy this file.

- **-h**
  Displays usage information for pdm_buildtenant.

The following is the format of the configuration file:

```
<?xml version="1.0" encoding="utf-8" ?>
<BuildTenant>
   <Object from="MajicObjectName">
    <Attribute from="sourceAttribute1" to="tenantAttribute1" />
    <Attribute from="sourceAttribute2" to="tenantAttribute2" />
   </Object>
</BuildTenant>
```

The *from* attribute of the Object tag identifies the pre-tenant object. Each Attribute tag identifies an attribute to be copied from the pre-tenant object to an attribute of the new tenant.

Important! For UNIX implementations of multi-tenancy, you *must* run pdm_task to export LIBPATH before executing the pdm_settenant and pdm_buildtenant utilities. If you do not run pdm_task before executing these utilities, you receive system errors. Use ../pdm_task to run the command.

pdm_clean_attachments -- Delete Redundent Attachments After Importing Tenant Data

After importing tenant data, you should delete redundant attachments. This utility has the following syntax:

```
pdm_perl pdm_clean_attachments.pl [-h] | [-n repository_name] | [-S|-K]
```

- **-h**
  Specifies to display command line help.
- **-n *repository_name***
  Specifies the name of the repository to process. If not specified, all repositories are processed.
- **-S**
  Specifies that only CA SDM repositories are processed.
- **-K**
  Specifies that only Knowledge Management and Embedded Images repositories are processed.

Note: Running the pdm_clean_attachments.pl command without any arguments processes all repositories.

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

pdm_settenant -- Assigning Tenants to Objects

After you define tenants, you must use the *pdm_settenant* utility to set the tenant column in other objects. This utility has the following syntax:

```
pdm_settentant [-h] | {-f [configuration_file] | -r} [-d domsrvr]
```

- **-d domsrvr**
  (Optional) Specifies a domsrvr to use. If this argument is not specified, pdm_settenant uses the default domsrvr.
- **-f *configuration_file***
  (Optional) Specifies the location of a configuration file specifying the data that will be updated and the rules for updating the file. If this argument is not specified, pdm_settenant uses the configuration file from the $NX_ROOT/site/cfg directory (after the configuration file is copied to the $NX_ROOT/site/cfg folder).
  Note: You can modify the sample settenant.xml file, or create a file and copy it to the $NX_ROOT /site/cfg directory. In addition, settenant.xsd must be in the same directory as settenant.xml, or you will receive an error. When you install the product, settenant.xsd is located in $NX_ROOT/site /cfg, so you do not have to copy this file.

The following sample XML code describes the format of this file:

```
<?xml version="1.0" encoding="utf-8" ?>
<SetTenant>
   <Object name="MajicObjectName">
    <TenantRule type="SREL">MajicColumName</TenantRule>
    <Where>tenant is null</Where>
   </Object>
   <Object name="MajicObjectName">
   <TenantRule type="Name">TenantName</TenantRule>
   <Where>tenant is null</Where>
   </Object>
</SetTenant>
```

Each Object tag specifies a CA SDM object to be tenanted. The TenantRule tag specifies how pdm_settenant should determine the tenant, and the Where tag selects the objects to be tenanted. There are two types of TenantRule tags:

- type="Name"
  Specifies an explicit tenant by name.

- type="SREL"
  Specifies an SREL attribute in the object. Pdm_settenant copies the tenant of the object referenced by the SREL.

- **-h**
  Displays usage information for pdm_settenant.

- **-r**
  Outputs a report displaying the total number of rows in each tenant-required table, and how many have a null tenant column.

Note: If both the -f and -r arguments are specified, pdm_settenant outputs a report after completing its update. If you only specify the -r argument, pdm_settenant outputs a report, but does not update any data.

Running pdm_settenant without any arguments displays usage information. To run pdm_settenant using the default configuration file, specify the -f option without the configuration_file argument. The pdm_settenant utility reads its configuration file and processes each rule it defines in sequence. It writes output to the pdm_settenant.log file in the $NX_ROOT/log directory.

You can run pdm_settenant as many times as needed. The first pass may take a significant time (possibly several hours at a large site). Subsequent passes run faster, as they only need to process rows that have not been updated. This prepares the database prior to installing the multi-tenancy option.

Important! On UNIX implementations of multi-tenancy, you must run pdm_task to export LIBPATH before executing the pdm_settenant and pdm_buildtenant utilities. If you do not run pdm_task before executing these utilities, you will receive system errors. Use .. /pdm_task to run the command.

Assign Tenants to Objects Considerations

After you define tenants, you can use the pdm_settenant (assign tenants to objects) utility to set the tenant column in other objects. When you change the tenant for an object, you must consider whether to change the tenancy on related tenanted objects in order to maintain data integrity. Failure to keep these objects synchronized can cause data to appear missing from CIs, relationships, MDRs, versioning, and so on. The following CA CMDB objects are tenanted:

- nr -- CI definitions
- nr_com -- Log entries associated with a CI
- bmhier -- Relationships associated with CIs
- mdr_idmap -- MDR provider definitions
- ci_mdr_idmap -- CI/MDR federated mappings

For each CI, do the following to synchronize data when you use pdm_settenant to change tenancy:

- Specify nr for the CI object name.
- Change the log entries associated with the CI in nr_com so that you can view the log entries for the new tenant.

Example: XML to Change the Tenant and Log

The following XML changes the tenant for a CI named CITest to T2 and also changes the corresponding log entries in nr_com:

```
<TenantRule type="Name">T2</TenantRule>
<Where>name = 'CITest'</Where>
</Object>
<Object name="nr_com">
<TenantRule type="Name">T2</TenantRule>
<Where>asset_id.name = 'CITest'</Where>
\</Object>
```

pdm_tenant_delete -- Deleting Tenant Data from a Database

The *pdm_tenant_delete* utility removes all data for a specified tenant from the database.

Important! The referential constraints on the ca_ tables must be dropped before running pdm_tenant_delete and restored afterwards.

This utility has the following syntax:

```
pdm_tenant_delete -h|-t tenant_name [-C|-R] [-Q]
```

- **-h**
  Displays the usage information for pdm_tenant_delete.

- **-t *tenant_name***
  Specifies the name of the tenant of the data to be deleted.

  Note: The tenant must be marked inactive before you can use this utility to delete the data.

- **-C**
  Specifies that all contacts for a tenant will be marked inactive. Since contacts can be shared between products, default logic should not mass delete or mass inactivate contacts unless explicitly requested.

  Note: This option is ignored if the -R option is specified.

- **-R**
  Specifies that all rows in all tenanted tables marked CA_COMMON in ddict.sch will be deleted, including the tenant object itself.

  Important! These tables are shared between multiple products, so use this option with caution.

- **-Q**
  Specifies quick query processing to execute database queries as fast as possible. If this argument is not specified, the utility uses background query processing so that queries run only when the system is otherwise idle. This argument improves running time at the expense of a greater impact on an active system.

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

pdm_tenant_extract -- Extracting Tenant Data

The *pdm_tenant_extract* utility extracts all data for a specified tenant from the database. It extracts the data in pdm_userload format so that it can easily be loaded into another database. This utility has the following syntax:

```
pdm_tenant_extract -h | -c control_file [-d domsrvr] [-g yes|no] [-o output_file]    -
p phase  [[-t tenant_name]...] [-Q] [table1 [table2...]]
```

- **-h**
  Displays the usage information for pdm_tenant_extract.

- **-c *control_file***
  Specifies the location of the control file for this tenant extract. For the Initial phase, the file is created in the specified location (and must not already exist). The file must exist for the Update and Final phases.

- **-d domsrvr**
  (Optional) Specifies a domsrvr to use.

- **-g yes|no**
  (Optional) Specifies whether or not public data is included in the output file. If this argument is not specified, public data from all tables is included.

- **-o *output_file***
  (Optional) Specifies the location of the output file. If this argument is not specified, output is directed to stdout.

- **-p *phase***
  Specifies the phase of the extract. Use one of the following values:
  I -- Initial
  U -- Update
  F -- Final

- **-t *tenant_name***
  Specifies the name of a tenant to be extracted. This argument is required for the Initial phase and can be repeated for multiple tenants. It is not valid on the Update and Final phase.

- **-Q**
  Specifies quick query processing to execute database queries as fast as possible. If this argument is not specified, the utility uses background query processing so that queries run only when the system is otherwise idle

- ***table1 [table2...]***
  (Optional) Specifies the tables to extract. If omitted, all tables are extracted.

Important! The output from the initial phase must be loaded into a database that has never been used for CA SDM or for any other product. Each table loaded from initial phase data is truncated prior to the load, which could cause loss of data if the database is already in use.

Note: To avoid referential problems during the data load, run the appropriate drop constraints script ($NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql or $NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql). After the loads complete, re-apply the constraints with the appropriate xxxAddConstraints.sql script found in the same directory.

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

pdm_userload -- Load Tenant Data

The *pdm_userload* utility is used to load data into a CA SDM database. This utility is available even if multi-tenancy is not installed. Multi-tenancy adds support for one additional argument (-t) that specifies the name of a tenant whose id must be inserted into the tenant column of all rows inserted or updated into a tenanted table. `The specified tenant must already be in the database.

When extracting data, complete the following steps to avoid errors in stdlog:

1. Before you start loading data, shut down CA SDM and restart the product in DBADMIN mode as follows:
   - **Windows**
     Run pdm_d_mgr -s DBADMIN
   - **UNIX**
     Run pdm_init -s DBADMIN
2. After the data loads, shut down CA SDM using the pdm_halt command.
3. Restart CA SDM in normal mode.

How to Implement Multi-Tenancy

This scenario describes how an administrator, as the CA SDM privileged user, implements multi-tenancy for the first-time. From start to finish, the CA SDM implementation changes as follows:

1. A single client uses a single implementation.
2. Multiple independent clients (tenants) and their users *share* a single implementation. Each tenant experiences the implementation as solely for its own use.

As the administrator, you use the CA SDM Administration interface to perform these steps:

1. Step 1: Install and enable multi-tenancy in setup mode (see page).
2. Step 2: Create the service provider tenant (see page).
3. Step 3: Create additional tenants (see page).
4. Step 4: Assign tenant access for a role (see page).
5. Step 5: Create subtenants (see page).
6. Step 6: Create tenant groups (see page).
7. Step 7: Change multi-tenancy to on mode (see page) and restart services.
8. Step 8: Review the implementation and correct (see page) any problems.

Step 1: Install and Enable Multi-Tenancy

You activate multi-tenancy by installing a multi-tenancy option in the product, and then enabling the setup mode. The setup mode specifies that multi-tenancy features are in effect for administrators. This mode lets you can view and edit tenant-related objects and attributes. However, the product does not enforce tenancy restrictions, and nonadministrator users see no changes. This mode lets you prepare multi-tenancy by performing tasks such as defining tenants or assigning tenants to roles without impacting normal use of the product.

Important! When multi-tenancy is in setup mode, web interface changes are active for service provider administrators. This behavior lets you view and edit tenancy-related objects and data on the web interface. However, tenancy restrictions are not enforced, and users other than service provider administrators do not see any product interface changes. Therefore, you can continue to use the product while implementing multi-tenancy.

Follow these steps:

1. Log in to CA SDM as an administrator and click the Administration tab.
2. In the tree on the left, click Options Manager, Multi-Tenancy.
   The Option List page appears.
3. Click multi_tenancy.
   The multi_tenancy Options Detail page appears.
4. Click Edit.
   The Update Options page appears.
5. Select setup from the Option Value drop-down list.
6. Click Install.
   The multi_tenancy option is installed.

7. Click Refresh.
   The page displays your changes.

8. Close the window.
   The Option List page reappears.

9. Restart services.
   Multi-tenancy is ready for you to implement in setup mode.

Step 2: Create the Service Provider Tenant

You use the product to create the service provider tenant. When you create the first tenant, the following occurs:

1. The first tenant always becomes the service provider.

   Important! You cannot change this designation -- on the Create Tenant page, the Service Provider check box and Record Status field are read-only.

2. The product associates the privileged user (typically ServiceDesk on Windows, or srvcdesk on Linux/UNIX) to the service provider tenant. The product sets all system contacts (such as System_AHD_Generated) to belong to the new service provider tenant.
   Note: Windows provides an Administrator system user. The privileged user must assign a tenant to the Administrator user manually.

Follow these steps:

1. Select Security and Role Management, Tenants on the Administration tab.

   Note: The Security and Role Management, Tenants option is available only when multi-tenancy is installed and in either setup or on mode.

2. Click Create New.
   The Create New Tenant page appears.

3. Complete the following fields:

   - **Name**
     Displays the tenant name.

   - **Service Provider**
     Identifies that this tenant is the service provider.

   - **Tenant Number**
     (Information Only) Displays the tenant number. CA SDM does not use this option.

- **Record Status**
  Sets the tenant to Active or Inactive.

- **Parent Tenant**
  Specifies another tenant above this tenant, making this tenant a subtenant in a tenant hierarchy.

- **Subtenants Allowed**
  Allows this tenant to have subtenants. The tenant cannot modify the setting.

- **Tenant Depth**
  (Information Only) Indicates the tenant depth of this tenant.

- **Supertenant Group**
  (Information Only) Identifies the system-maintained tenant group that contains this tenant and all tenants above it in the tenant hierarchy.

- **Subtenant Group**
  (Information Only) Identifies the system-maintained tenant group that contains this tenant and all tenants below it in the tenant hierarchy.

- **Foreign Key Group**
  (Information Only) Identifies the system-maintained tenant group that contains tenants that can be referenced from an SREL in data that belongs to this tenant. The foreign key group is the same as the supertenant group.

- **Related Tenant Group**
  (Information Only) Identifies the system-maintained tenant group consisting of both the supertenant and subtenant groups for this tenant.

- **Terms of Usage**
  Specifies the Terms of Usage statement for the tenant. For more information about creating a terms of usage statement, see Setting Up Terms of Usage (see page 1000).

- **Logo**
  Specifies the URL for the tenant logo file, which can be any web image type.

- **Location**
  Displays the Location lookup page, which lets you specify a location.

- **Contact**
  Displays the Contact lookup page, which lets you specify a contact.

Note: If no contact is associated with the respective tenant, the Email Address and Pager Email Address fields are inactive.

4. Click Save.
   The product creates the service provider tenant.

5. Close the window.

6. Right-click the Tenant list and click Refresh.
   The Tenant List is updated and displays the service provider tenant.

7. Log out of CA SDM.

Step 3: Create Tenants

You use the product to create additional tenants. You can create as many tenants as required to manage multiple separate enterprises that provide support to clients.

Follow these steps:

1. Log in to the Administrator interface as a member of the service provider. An easy way to do this login is to log in as the privileged user (for example, ServiceDesk). This user automatically belongs to the service provider tenant.

2. Select Security and Role Management, Tenants on the Administration tab.

   Note: The Security and Role Management, Tenants option is available only when multi-tenancy is installed and in either setup or on mode.

3. Click Create New.
   The Create New Tenant page appears.

4. Complete the fields in this page. Some of the fields are self-explanatory. Following fields require explanation:

   - **Service Provider**
     Identifies whether a tenant is the service provider. The first created tenant is always the service provider, afterward, this check box is read-only.

   - **Tenant Number**
     (Information Only) Displays the tenant number. CA SDM does not use this option.

   - **Subtenants Allowed**
     Allows this tenant to have subtenants. The tenant cannot modify the setting.

   - **Tenant Depth**
     (Information Only) Indicates the tenant depth of this tenant.

   - **Supertenant Group**
     (Information Only) Identifies the system-maintained tenant group that contains this tenant and all tenants above it in the tenant hierarchy.

   - **Subtenant Group**
     (Information Only) Identifies the system-maintained tenant group that contains this tenant and all tenants below it in the tenant hierarchy.

- **Foreign Key Group**
  (Information Only) Identifies the system-maintained tenant group that contains tenants that can be referenced from an SREL in data that belongs to this tenant. The foreign key group is the same as the supertenant group.

- **Related Tenant Group**
  (Information Only) Identifies the system-maintained tenant group consisting of both the supertenant and subtenant groups for this tenant.

- **Terms of Usage**
  Specifies the Terms of Usage statement for the tenant. For more information about creating a terms of usage statement, see Setting Up Terms of Usage (see page 1000).

- **Logo**
  Specifies the URL for the tenant logo file, which can be any web image type.

> **Note:** If no contact is associated with the respective tenant, the Email Address and Pager Email Address fields are inactive.

5. Click Save and close the window.
   The product creates the tenant.

6. (Optional) Click Tenant Groups to add this tenant to a new group or to an existing one.

Step 4: Assign Tenant Access for a Role

The role of a CA SDM user governs both access authorization and the user interface. The roles available to users depend on their access type. Multi-tenancy lets you control the tenant or tenant group that a user can access within the role. When multi-tenancy is installed, the Role Detail page includes additional options that let you assign or edit tenant access.

> **Note:** You can grant tenant users access to data other than their own. Non-service provider tenant analysts only have access to their own tenant and subtenants. However, you can you update their function access to include the tenant of the analyst. For example, you can define a role to set separate read and write access to certain tenant groups for users within that role.

Follow these steps:

1. Navigate to Security and Role Management, Role Management, Role List.
   The Role List appears.

2. Click the role for which you want to assign tenant access.
   The Role Detail page appears and provides Tenant Access and Tenant Write Access drop-down lists on its Authorization tab. Tenant Access is view-only, and Tenant Write Access allows create and update also.

3. Click Edit.
   The Update Role page appears.

4. Select options for Tenant Access and Tenant Write Access:

   - **Same As Tenant Access**
     Sets the access to be the same as the Tenant Access setting. This value is the default for the Tenant Write Access drop-down list and is only available for the Tenant Write Access option.

   - **All Tenants**
     Removes tenant restrictions. A user in a role with this access can do the following:

     - View any object in the database (read access).

     - Create and update (write access) any tenanted object in the database.

     When a user with All Tenants access creates an object, the user must select the tenant of the new object.

   - **Single Tenant**
     Sets tenant access for a role to a named tenant. When you select this option, another field appears that lets you select a specific tenant. A user in this role can access only those objects associated with the named tenant.

   - **Tenant Group**
     Sets tenant access for a role to a user-defined or system-maintained tenant group. After you select this option, another field appears that lets you select a specific tenant group. A user in this role can access only those objects associated with one of the tenants in this group. When a user with tenant group access creates an object, the user must select the tenant for the new object.

   - **Contact's Tenant**
     Sets tenant access for the role to the tenant of the contact using it. A user in this role can access only those objects associated with their own tenant.

   - **Contact's Tenant Group**
     Sets role access for an analyst role to the tenant group that the analyst works with, as specified on the contact record for the analyst. If the user with the role is not an analyst, this selection has the same effect as Contact's Tenant. This option is only available for analysts.

   - **Contact's Subtenant Group**
     Sets tenant access for the role to the subtenant group of the contact using it. A user in this role can access only those objects associated with their own subtenant group.

   - **Contact's Supertenant Group**
     Sets tenant access for the role to the supertenant group of the contact using it. A user in this role can access only those objects associated with their own supertenant group.

   - **Contact's Related Tenant Group**
     Sets tenant access for the role to the Related Tenants Group of the contact using it. A user in this role can access only those objects associated with their own related-tenant group.

- **Update Public**
  Controls whether a service provider user in the role has the authorization to create or update public data. All users can view public data, regardless of access rights for the current role. Tenant users (users belonging to a tenant other than the service provider) cannot update public data, regardless of their role.

- **Click Save**
  Tenant access is assigned for the role. When a user queries the database, the product restricts the results to objects belonging to tenants associated with the role of the user.

Step 5: Create Subtenants

Subtenancy lets you define and modify tenant hierarchies for organizational and data-sharing purposes. To place a tenant into a tenant hierarchy, you assign the tenant a parent tenant.

Follow these steps:

1. On the Administration tab, select Security and Role Management, Tenants.
   The Tenant List appears.

   Note: The Security and Role Management, Tenants option is available only when multi-tenancy is enabled.

2. Click an existing tenant to Edit, or click Create New.
   The Tenant Detail page appears, which lets you enter any required data or changes.

3. Select a Parent Tenant.

   Note: The Parent Tenant drop-down list only displays tenants that are allowed to have subtenants.

4. Click Save.
   The tenant is a subtenant of the parent tenant.
   Note: When a tenant is a subtenant, it belongs to the subtenant group of the parent tenant. The parent tenant joins the supertenant group of the subtenant. Each tenant joins the Related Tenants group of the other.

Step 6: Create Tenant Groups

A tenant group is a collection of tenants that share access to CA SDM objects. Tenant groups let you classify, manage, and control access to tenants. You can assign a role to a tenant or tenant group. When multi-tenancy is active, the product associates each role with: all tenants (public), a single tenant, or a single tenant group. Use tenant groups whenever a role needs access to more than one tenant. For example, you can assign analysts to a tenant group containing tenants belonging to a particular geographic location.

The product generates and maintains three tenant groups automatically for each tenant in a tenant hierarchy (*tenant* is the tenant name):

- *tenant*_subtenants (tenant, its child tenants, and their lower subtenants)
- *tenant*_supertenants (tenant, its parent tenant and its higher supertenants)
- *tenant*_relatedtenants (entire single hierarchy)

You use the system-maintained tenant groups like user-defined tenant groups. However, you can only change the system-maintained tenant group names and descriptions.

Example: Role A Needs Access to Tenant A, Tenant B, and Tenant J

Instead of assigning the role to each tenant separately, you can do the following:

1. Create a tenant group, and add Tenant A, Tenant B, and Tenant J to the group.
2. Assign Role A to this tenant group.
   Users (contacts) assigned to Role A can access the tenant group, which is comprised of Tenants A, B, and J.

Follow these steps:

1. Log in as the service provider, click the Administration tab, and select Security and Role Management.
2. Click Tenant Groups.

   Note: The Security and Role Management, Tenant Groups option is available only when multi-tenancy is installed (either on or setup).

3. Click Create New.
   The Create New Tenant Group page appears.
4. Complete the tenant group fields and click Save.
   The tenant group is created.
5. Close the window.
   The Tenant Group List appears.

6. Right-click the Tenant List and select Refresh.
   The Tenant Group List is updated.

7. Click Update Tenants on the Tenant Group Detail page and add tenant members to the group.

8. (Optional) Repeat Steps 3 through 6 for each tenant group you want to create.

Step 7: Change Multi-Tenancy to On Mode

You change changing the Multi-Tenancy option to on mode to make the multi-tenancy implementation function fully. Each tenant then views the implementation as solely for its own use. Each tenant cannot update or view the data of another tenant.

Follow these steps:

1. Log in to CA SDM as an administrator, and click the Administration tab.

2. In the tree on the left, click Options Manager, Multi-Tenancy.
   The Option List page appears.

3. Click multi_tenancy.
   The multi_tenancy Options Detail page appears.

4. Click Edit.
   The Update Options page appears.

5. Select setup from the Option Value drop-down list.

6. Click Edit.
   The Update Options page appears.

7. Select on (the default) from the following values in the Option Value drop-down list:

   - **on**
     (Default) Disallows a check-in to a tenant-required table when the tenant is null and an SREL to a table with a tenant is not available.

   - **on (warn)**
     Writes an error to the log but allows the check-in to proceed when a tenant-required object with a null tenant is created or updated.

   - **on (allow)**
     Writes a warning to the log but allows the check-in to proceed when a tenant-required object with a null tenant is created or updated.

8. Click Save, and then Refresh.
   The page displays your changes.

9. Close the window.
   The Option List page reappears.

10. Restart services.
    Multi-tenancy is fully functional.

Step 8: Review the Implementation and Correct

Review the multi-tenancy implementation and correct any problems.

Follow these steps:

1. Log in to CA SDM using the privileged username (typically ServiceDesk).

2. Click the Administration tab and browse to the Tenant List.
   The Provider shows as Yes for the privileged user in the Tenant Name.

3. Verify that your multi-tenancy restrictions are enforced by browsing to a Contact List.
   If tenant-required tables incorrectly include untenanted data in a multi-tenancy system, the following message appears in the Contact List:

   ```
   AHD05358 There were nn untenanted active Contact objects at CA Service Desk Manager startup.
   ```

   Important! If untenanted data is in the database, you can set the multi-tenancy option mode to on (warn) or on (allow). These modes let you update tenant-required tables with a null tenant. This method prevents data loss when a service level agreement (SLA) or attached event executes for a ticket that does not include a tenant.

4. (Optional) Disable multi-tenancy if problems occur and complete the following steps:

   a. Restore the Domain_Constraint and usp_role tables.

   b. Set the Multi-Tenancy option to the setup mode.

   c. Recycle the system.

   The site can resume previous operations while you correct whatever issues required the reversion.

Setting Up Terms of Usage

Contents

For each tenant, you can configure a terms of usage statement which presents the end user with an initial statement when they log in to CA SDM. The terms of usage statement reminds the end user about the proper use of the product that they must agree to before they can continue to log in to CA SDM. A log is generated after the user Accepts or Rejects the statement.

In CA SDM, you can configure a terms of usage statement from the Security and Role Management node on the Administration tab. You can set the Service Provider tenant or subtenants to display the same or different terms of usage statements. You select the terms of usage statement in the Terms of Usage field on the Tenant detail form.

Note: You must enable multi-tenancy and configure one or more tenants before you can associate a terms of usage statement with a tenant.

Create a Terms of Usage Statement

End users are presented with a terms of usage statement when they log in to CA SDM that they must agree to before they can continue to log in. You can create a terms of usage statement and select it to display for a tenant or an analyst.

Follow these steps:

1. Select Security and Role Management, Terms of Usage on the Administration tab.

   The Terms of Usage List page appears.

2. Click Create New.

   The Create New Terms of Usage page appears.

3. Complete the following fields and click Save:

   Name

   Displays the name of the terms of usage statement.

   Status

   Sets the terms of usage statement as active or inactive.

   Description

   Displays a description of the terms of usage statement.

   Text
   Specifies the text of the terms of usage statement. Click the Edit Terms of Usage button to edit the text in an HTML editor.

   The Terms of Usage statement is saved. You can now associate the terms of usage with your tenants.

Update Terms of Usage Statement of a Tenant

You can configure a tenant to display a terms of usage statement upon login. The end user must accept the terms of usage statement before they can continue to log in.

Follow these steps:

1. Select Security and Role Management, Tenants on the Administration tab.

   The Tenant List page appears.

2. Select the Tenant link you want to update.

   The Tenant Detail page appears.

3. Click Edit.

   The Update Tenant page appears.

4. Select the terms of usage statement from the Terms of Usage drop-down and click Save.

   Note: If you select <empty> in the Terms of Usage drop-down, CA SDM displays the terms of usage statement for the tenants parent, grandparent, and so on until a terms of usage statement is found. If a terms of usage statement is not found at any level, CA SDM proceeds with the login. If you create a terms of usage statement without text, CA SDM does not display a terms of usage statement and lets the end user log in to CA SDM.

   The tenant is updated.

Setting Up Security

This article contains the following topics:

Before you allow people to use CA SDM, it is important that you set up security to determine the following:

- Which users can access the system

- What level or levels of access users can have
- How users are authenticated when they log in

CA EEM User Base Configurations

CA EEM is a central repository of user information (identities). CA EEM defines user authentication and access to other applications. If you have several CA Technologies products installed, some of them can use CA EEM to store identities and access policies. CA SDM only uses CA EEM for authentication. CA EEM is not a CA SDM configuration option and must be installed separately.

The CA EEM repository of user records is *either* of the following sources:

- An external LDAP directory
- Its own internal tables in the MDB

CA EEM has an LDAP interface for use when it is configured to use the MDB.

Note: The MDB tables used by CA EEM are different from the ones used by CA SDM.

If your organization uses a directory server, such as Active Directory or eTrust Directory, consider configuring CA EEM to use the directory for its user base. This configuration makes the users in your directory accessible by any other application that uses CA EEM. Because CA EEM centralizes access management, it is typically installed on a single server.

CA SDM

CA SDM stores contact information in MDB tables. These tables have no relationship to CA EEM. CA SDM does not use CA EEM for access or identity management. CA SDM manages its own access and security with Access Types and Data Partitions.

CA SDM uses CA EEM only for authentication. If you want to use CA EEM to authenticate users in CA SDM, install CA EEM. If you integrate CA SDM with CA EEM, it replaces the CA SDM operating system authentication with CA EEM authentication.

Note: To integrate CA EEM and CA SDM, you must set the *eiam_hostname*, *use_eiam_artifact*, and *use_eiam_authentication* options in Options Manager, Security.

To summarize:

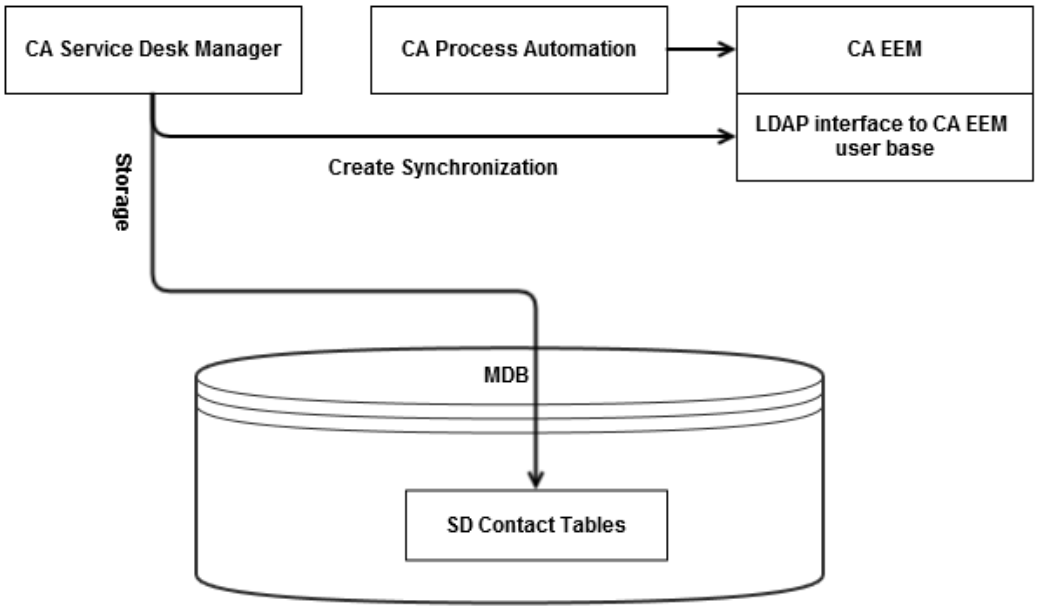
- The CA SDM user base is separate from that of CA EEM.
- CA SDM uses the MDB to store Contact information. CA SDM also features an LDAP integration, which allows it to create new Contacts from an LDAP server and synchronize existing contacts with the directory.

- CA EEM is CA's solution to centralized user management. If you have several CA products installed, they all may be using CA EEM to store identities and access policies.
- CA EEM may be configured to either point to an external (LDAP) directory or use the MDB to store user information. CA EEM itself has an LDAP interface for use when it is configured to use the MDB.

Note: The tables used by CA EEM in the MDB are different from the ones used by CA SDM.

CA EEM as LDAP Configuration

When CA EEM is configured to use MDB rather than an external directory to store user information, CA EEM exposes the user directory using an LDAP interface. If your site does not use an external LDAP server, you can still get the advantages of external LDAP configuration by configuring CA SDM to use CA EEM as an LDAP source. This configuration can be useful if your site does not use an LDAP server but you want to consolidate user management in CA EEM. Other CA products also use CA EEM, which can greatly simplify user management.



Note: This configuration is applicable only when CA EEM is configured to use the MDB. If CA EEM is configured to an external LDAP server, configure CA SDM to point to the same LDAP server, *not* CA EEM. For more information, see How to integrate CA SDM with LDAP (see page 1207).

Configure the CA EEM r8.4 SP4 CR05 User Store

You can configure CA EEM r8.4 SP4 CR05 to store user records in an external LDAP directory or in its own internal MDB tables. When CA EEM uses an external LDAP directory, it is a read-only interface; you cannot add or modify users through the CA EEM interface.

Follow these steps:

1. Click Start, Programs, CA, Embedded Entitlements Manager, EEM UI.
   The CA EEM user interface appears.
2. Click the Configure tab.
3. Click the EEM Server sub-tab.
4. On the left-hand pane, click the Global Users / Global Groups link.
5. On the right-hand pane, select one of the following options:
   - Store in internal datastore
   - Reference from an external directory
   - Reference from CA SiteMinder

   Note: If you select the Reference from an external directory option, you are prompted for the LDAP server details.
6. Click Save.
   The user store configuration for CA EEM is complete.

Configure the CA EEM r12 CR02 User Store

You can configure CA EEM r12 CR02 to store user records in an external LDAP directory or in its own internal MDB tables. When CA EEM uses an external LDAP directory, it is a read-only interface; you cannot add or modify users through the CA EEM interface.

Follow these steps:

1. Click Start, Programs, CA, Embedded Entitlements Manager, Admin UI.
   The CA EEM user interface appears.
2. Click the Configure Tab.
3. Click on User Store subtab.
4. On the left-hand pane, click the User Store link.
5. On the right-hand pane, select one of the following options:

- Store in internal user store
- Reference from an external LDAP Directory.
- Reference from CA SiteMinder

Note: If you select the Reference from an external directory option, you are prompted for the LDAP server details.

6. Click Save.
The user store configuration for CA EEM is complete.

Add Users and Groups

If CA EEM is configured to reference an external directory, you cannot add users using the CA EEM user interface. CA EEM is a read-only interface to the LDAP server. You must use whatever interface is provided with your particular LDAP server product to update user records.

Follow these steps:

1. Click Start, Programs, CA, Embedded Entitlements Manager, Admin UI/EEM UI.
2. Log in using the CA EEM administrator user name and password. These are specified during the CA EEM installation. CA EEM must be installed separately and is not a configuration option for CA SDM.
3. Click the Manage Identities tab.
4. On the left-hand pane, click the Users tab to search for and update existing user records.

Note: To manage the CA EEM groups, click the Groups tab.

5. Click the icon to the left of the Users folder.
The form for creating a user record appears.
6. Complete the form and click Save.
The new CA EEM user record is saved in the MDB.

Note: The steps to edit an existing user record and maintain group records are similar to these steps.

Security Considerations

When you first install CA SDM, the system is set up to allow maximum access to any contact that does not have an explicit access type that is defined in the contact record. Perform the following steps before using the application:

1. Review the predefined access types to determine a reasonable default for your system. Administrator is set as the default access type, which is not a good choice for most sites. For example, some sites offer read-only CA access to most members of the IT organization. If you set CMDB User as the default access type, you do not have to set the access type of new users unless they need additional privileges. Similarly, if most users require the privilege to write configuration information, you can select CMDB Analyst as the default access type.

2. Assign the access types of remaining contacts explicitly.
   For example, if you select CMDB User as the default access type, modify the contact records for your analyst contacts to assign an access type of analyst.

CA EEM Authentication for CA Process Automation

CA SDM and CA Process Automation communicate using a web services exchange over HTTP. Although every measure is made to pass minimal amounts of sensitive information between the products, a malicious entity can access user names, passwords, and proprietary information. You can take deliberate steps to secure server communication.

For CA Process Automation authentication, consider the following recommendations:

- As an option, you can configure CA Process Automation to use CA EEM as an authentication server. CA Process Automation implements default groups and policies within CA EEM. You can modify the default groups and policies to meet the needs of your organization.

- Using CA EEM eliminates the need to pass plain text user names and passwords for authentication purposes. If you are using multi-tenancy, CA EEM is required for enabling multi-tenancy within CA Process Automation.

  Note: To achieve authentication security in this integration, it is not necessary to have CA SDM configured to use CA EEM. However, CA EEM is required for CA Process Automation multi-tenancy implementation.

- Configure CA Process Automation to communicate using secure communications over HTTPS. HTTPS URLs use SSL/TLS to eliminate plain text exchanges while protecting proprietary and other sensitive data from accidental or malicious disclosure.

User Authentication

This article contains the following topics:

CA SDM provides a user authentication solution that you can modify as part of the access type. The same authentication is used by all CA SDM interfaces and by other CA products.

Authentication is flexible, allowing you to take advantage of external authentication mechanisms, such as Windows, HTTPD user validation or LDAP authentication. You can also select from a variety of internal authentication options, including operating system password, PIN, guest user access, or no access at all.

How CA SDM Authenticates Users

CA SDM authenticates users based on the user ID defined in their contact record. The product also does the following when a user requests access to the system:

1. If an external user ID is available (from HTTPD or Windows validation), CA SDM looks up the contact by login ID. If the contact is found and has an access type that permits external authentication, the user is allowed into the product.

2. If there was no successful external authentication, CA SDM prompts the user for a user ID and password. The product looks up a contact record for the user ID, obtains the access type, and then authenticates the user as specified by the access type.

Many installations find the predefined access types define authentication that is reasonable for that type of user; however, in some cases you may need to modify the authentication information for a predefined access type or define a new access type to handle a different authentication method for some of your users. You should review the authentication settings for the predefined access types to determine if they meet your needs, or if you need to modify them, or define additional types.

External Authentication

CA SDM permits users to access the system without supplying a user ID if all of the following conditions are met:

- External authentication is set for the user.
- The user's externally authenticated user ID is associated with a contact in your contact table.
- The contact record has an access type whose authentication definition permits external authentication.

External authentication does not permit users to access the system in the following cases:

- A user attempts access through a non-secure server.
- A user attempts access but is assigned to an access type that does not allow external authentication.

None of the predefined access types use external authentication. If you want to use external authentication for users, consider modifying the employee, analyst, and administrator access types to set external authentication. Your individual site requirements and different types of users determine whether to allow external authentication. When external authentication is used, the server configuration controls the access to files and directories. When you define authentication for an access type, you can decide the usage as follows:

- Do not use any external authentication that is already implemented, such as the user login on Windows or validation by the HTTPD server.
- Use the authentication that is implemented and allow or deny access based on it.

Note: If external authentication is not allowed, the user is authenticated based on the validation type that you specify.

Following are some examples of external authentication:

- If a user who has administrator access logs into a Windows computer, the user can perform administrative tasks without re-entering any login information.
- If a user who has HTTPD server validation, the user can access the web interface without re-entering any login information. Because the administrator access type specifies the analyst web user type, the appropriate web interface for the analyst is presented automatically.

Validation Types

Validation types authenticate users only under the following circumstances:

- The user access type does not permit external authentication.
- The user access type permits external authentication, but the user has not been validated externally (for example, the user has attempted access through a nonsecure server).

CA SDM provides you with the following validation options:

- **No Access** -- Users of this type have no access unless external authentication is allowed and is valid.
- **Open** -- Users of this type have access, with no additional authentication required.
  - **OS** -- Users of this type enter their operating system password for access. The operating system used for validation is the one running User Validation Host. This option is the default validation type for the administrator, analyst, and employee access types.
  - **PIN** -- Users of this type gain access by entering the correct value for the PIN field in their contact record as their password. You define the PIN field by entering the field attribute name when you select PIN as the validation type. PIN is the default validation type for the customer access type, which uses the value in the customer ID (contact_num) field as the PIN.

Logged In User Counts and Session Counts

The following KPIs count the number of unique licensed users that are logged in to the system (for example, CA SDM Web UI, SOAP Web Services, REST Web Services, and so on), regardless of how many sessions each user has opened:

Note: For a licensed user, ensure that the Licensed? check box is selected from the Access type page of the contact (navigate to Security and Role Management, Access Type on the Administration tab and search for the contact).

- webConcurrentLicenseCt
- webConcurrentSOAPLicenseCt
- webConcurrentRESTLicenseCt
- webConcurrentTotalLicenseCt

The following KPIs count the numbers of unique unlicensed users that are logged in to the system, regardless of how many sessions each user has opened:

- webConcurrentNonLicenseCt
- webConcurrentSOAPNonLicenseCt
- webConcurrentRESTNonLicenseCt
- webConcurrentTotalNonLicenseCt

The following KPIs count the number of unique sessions that started during the interval:

- webSessionCt
- webSOAPSessionCt
- webRESTSessionCt

For more information about the KPI description, see the KPI detail page (navigate to Service Desk, KPIs on the Administration tab and search for the KPI). For more information about how these KPIs count from different session types, see the How KPIs Count from Different Session Types (see page 1010) topic.

How KPIs Count from Different Session Types

There are different session types that are defined in the system. The following table shows how KPIs count these sessions:

Note: All predefined KPIs are installed as Inactive. For a KPI to begin functioning in your system, it must be set to Active. Navigate to Service Desk, KPIs on the Administration tab and search for the inactive KPI. Open the KPI and click Activate.

Important! Multiple versions of a KPI with the same name cannot be active at the same time.

Session Type	Session Type Description	Counted by KPIs
Web Client	Web browser session	webSessionCt webConcurrentLicenseCt webConcurrentNonLicenseCt webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
Java Client	Java client session	webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
Web Services	SOAP Web services session	webSOAPSessionCt webConcurrentSOAPLicenseCt webConcurrentSOAPNonLicenseCt
Utility	Server utility session	webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
Portal	Portal session	webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
Knowledge Chat	Knowledge Chat session	webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
Mail Server	Mail Server session	webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
Custom Application	Custom Application session	webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
PDA Client	PDA Client session	webSessionCt webConcurrentLicenseCt webConcurrentNonLicenseCt webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
REST Client	REST Web Services Session	webRESTSessionCt webConcurrentRESTLicenseCt webConcurrentRESTNonLicenseCt webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt

Example: KPIs calculating user counts

One licensed (that have the Licensed? check box selected) and two unlicensed end users are logged into the web self-service interface and reviewing some announcements.

At the same time five licensed analysts (that have the Licensed? check box selected) are logged into the analyst interface and working on incidents. One of the analysts also logs in to the SOAP Web Services interface.

- The webConcurrentLicenseCt KPI shows a count of six, meaning that six licenses are currently being used, irrespective of the number of interfaces each user is using.
- The webConcurrentNonLicenseCt KPI shows the count of two, which means that two unlicensed users are logged on to the system, irrespective of the number of interfaces each user is using.
- The webSessionCt KPI shows a count of eight, meaning that eight total users are logged in to the CA SDM Web UI.
- The webSOAPSessionCt KPI shows a count of one, meaning that one user is logged in to the SOAP Web Services interface.

(Applicable for advanced availability configuration only) Example: KPIs calculating user counts from different nodes

A licensed analyst logs in to the analyst interface from the background server and works on incidents. The same analyst logs in to the analyst interface from the application server. The webConcurrentLicenseCt KPI shows a count of one, meaning that one license is currently being used, irrespective of the number of nodes or servers the user has logged in from.

Establishing Support Structure

This article contains the following topics:

Setting Up Your CA SDM System

This section contains the following topics:

Shared Codes

This article contains the following topics:

In CA SDM, different types of tickets share certain underlying codes, such as priority, severity, impact, and urgency codes. Requests and change orders share some codes, and all types of tickets share other codes.

Consider the following information about shared codes:

- By default, numeric values rank them.
- You can modify the codes.
- You cannot add or delete shared codes.
- You can use impact, priority, severity, and urgency codes.

Based on your service desk model, set up the following codes:

Shared Codes	Description
Priority	Must be set up for all service desk models.
Severity	Must be set up for internal and combined service desk models.
Impact	Must be set up for internal and combined service desk models.
Urgency	Must be set up for internal and combined service desk models.

Priority Codes

Priority codesindicate a ranking order by which the service desk should respond to tickets (that is, they specify the level of attention a ticket should receive). Priority codes are referenced in requests, change orders, and issues; therefore, they apply to all service desk models.

You can use priorities to escalate tickets manually or automatically by monitoring events. In many service desk installations, priority codes are used on the scoreboard to provide analysts with a real-time status of their requests and change orders.

You can assign a service type to a priority code, which is then automatically assigned to tickets when the priority code is specified. This lets you associate a specific level of service to a ticket based on the assigned priority. For example, the system-defined service type, 4-hour resolution, is automatically associated with priority 1. Tickets that are assigned a priority of 1, therefore, are automatically assigned this service type, including all the service type events that are associated with the 4-hour resolution service type.

Severity Codes

Severity codesidentify the extent of the damage to equipment affected by a request. Severity codes are referenced in requests only; therefore, they apply only to internal and combined service desk models.

Note: Severity is often used as a synonym for priority. Some sites use priority only, ignoring severity altogether. If you want to distinguish between how serious a problem is on a technical level (severity) and how quickly you want it handled (priority), you can use severity and priority codes.

Impact Code values helps to calculate the Incident Priority.

Impact Codes

Impact codesmeasure the significance of a ticket on the functioning of the system. For example, if a change order could affect the functioning of the entire system, it would be assigned a high impact. Impact codes are referenced in requests and change orders only; therefore, they apply only to internal and combined service desk models.

Note: Impact and urgency codes (see page 1014) are similar, but they have distinct purposes.

Urgency Codes

Urgency codesmeasure the significance of the request for users of the system (that is, they indicate the importance of the request to the overall production environment). For example, if a request could jeopardize the mission of the enterprise, the Urgency code can be a value of 5-Immediate. Urgency codes are referenced in requests only; therefore, they apply only to internal and combined service desk models.

Urgency and impact codes serve distinct purposes, but are often confused because they coincide. For example, a request to report a fire in a critical data center can have a 3-Single Group Impact and 5-Immediate Urgency. These codes apply because the fire impacts more than one group but not necessarily the entire organization. Because the data center is critical for operations, the urgency requires immediate attention.

Status Codes

This article contains the following topics:

Status codes are used to track the status of an item. Separate status codes track requests, change orders, issues, and workflow tasks. In each case, there are predefined status codes that you can use if they suit your needs. Otherwise, you can modify the predefined status codes or define new ones that are specific to your site. Depending on your service desk model, you set up the following codes:

Status Codes	Description
Request/ Incident/ Problem	Must be set up for internal and combined service desk models.
Change Order	Must be set up for internal and combined service desk models.
Issue	Must be set up for external and combined service desk models.
Task	Must be set up for all service desk models.

Status codes let analysts sort and select information based on the status so that they can carefully track their progress. How carefully you define the status codes determines how accurate the analysts can be in describing the actual status of an item.

You can mark any status code as active or inactive. When you mark a status code as inactive, it is no longer available for analysts to use, but it remains available for future use (that is, it is not deleted from the database). If you decide later to use the status code, you need only to go back to it and mark it as active.

Note: The same area definitions are available for request, incident, and problem tickets. On the Administration tab, these areas are referred to as request/incident/problem areas. For brevity, they are referred to here simply as request areas.

Request Status Codes

The following table describes the predefined status codes for request tickets.

Request Status Code	Description
Acknowledged	The receipt of a request has been acknowledged.
Closed	A request has been completely resolved.
Closed -- Unresolved	A request has been closed but still must be resolved.
Fix in Progress	A request is pending a fix.
Hold	The service type events for the request are on hold.
Open	A request has been defined and is being used to monitor and manage its completion.
Problem Closed	A problem request is completely closed.
Problem Fixed	A problem request is fixed, but not closed.
Problem Open	A request has been identified as a problem.
Researching	A request is open pending additional research and analysis.
Work in Progress	Work is being done to fix a request.

If your site uses other terminology for identifying the request status, you should define status codes that suit your needs and ignore the predefined status codes, or change the definitions to match your use. For example, you may want to define additional request status codes, such as the following codes:

Request Status Code	Description
Duplicate	Requests that have been opened but may be a duplicate of an existing request for another user.
Emergency	Critical requests that must be addressed immediately.
Report	Requests that are resolved and closed, but should be reported on at a management level.
Test	Requests that are resolved, but should be tested for one week before closing.

Problem Status Codes

The following table describes the predefined status codes for problem tickets.

Problem Status Code	Description
Acknowledged	The receipt of a problem has been acknowledged.
Closed	A problem has been completely resolved.
Closed -- Unresolved	A problem has been closed but still must be resolved.
Fix in Progress	A problem is pending a fix.
Hold	The service type events for the problem are on hold.

Problem Status Code	Description
Open	A problem has been defined and is being used to monitor and manage its completion.
Problem Closed	A problem is completely closed.
Problem Fixed	A problem is fixed, but not closed.
Problem Open	A request has been identified as a problem.
Researching	A problem is open pending additional research and analysis.
Work in Progress	Work is being done to fix a problem.

If your site uses other terminology for identifying the problem status, you should define status codes that suit your needs and ignore the predefined status codes, or change the definitions to match your use. For example, you may want to define additional problem status codes, such as the following codes:

Problem Status Code	Description
Duplicate	Problems that have been opened but may be a duplicate of an existing problem for another user.
Emergency	Critical problems that must be addressed immediately.
Report	Problems that are resolved and closed, but should be reported on at a management level.
Test	Problems that are resolved, but should be tested for one week before closing.

Incident Status Codes

The following table describes the predefined status codes for incident tickets.

Request Status Code	Description
Acknowledged	The receipt of an incident has been acknowledged.
Closed	An incident has been completely resolved.
Closed -- Unresolved	An incident has been closed but still must be resolved.
Fix in Progress	An incident is pending a fix.
Hold	The service type events for the incident are on hold.
Open	An incident has been defined and is being used to monitor and manage its completion.
Incident Closed	An incident is completely closed.
Incident Fixed	An incident is fixed, but not closed.
Incident Open	An incident has been identified as a problem.
Researching	An incident is open pending additional research and analysis.
Work in Progress	Work is being done to fix an incident.

If your site uses other terminology for identifying the incident status, you should define status codes that suit your needs and ignore the predefined status codes, or change the definitions to match your use. For example, you may want to define additional incident status codes, such as the following codes:

Request Status Code	Description
Duplicate	Incidents that have been opened but may be a duplicate of an existing request for another user.
Emergency	Critical incidents that must be addressed immediately.
Report	Incidents that are resolved and closed, but should be reported on at a management level.
Test	Incidents that are resolved, but should be tested for one week before closing.

Change Order Status Codes

The following table describes the predefined status codes for change order tickets.

Change Order Status Code	Description
Approval in Progress	A change order is open, pending approval.
Approved	A change order has been approved.
Cancelled	A change order has been cancelled.
Closed	A change order has been completed.
Hold	The service type events for the change order are on hold.
Implementation in Progress	A change order is being implemented.
Open	A service order has been defined in a change order and the change order is being used to monitor and manage its completion.
Rejected	A change order has been rejected.
Resolved	A change order has been resolved.
RFC	A request for change has been submitted.
Suspended	Stops workflow tasks on a change order.
Verification in Progress	A change order is being verified.
Backed Out	Implemented change order was backed out.
Implemented	Change was implemented.

If your site uses other terminology for identifying the status of a change order, you should define status codes that suit your needs and ignore the predefined status codes, or change the definitions to match your use. For example, you may want to define additional change order status codes, such as those listed in the following table:

Change Order Status Code	Description
Duplicate	Change orders that have been opened but may be a duplicate of an existing change order for another user.
Emergency	Critical change orders that must be addressed immediately.
Report	Change orders that are completed and closed, but should be reported on at a management level.

Closure Codes

Use closure codes to define the final outcome of change orders, such as successful or unsuccessful. Set closure codes manually or as part of the Update Status activity on a change order when the status is closed, finished or resolved.

Issue Status Codes

The following table describes the predefined status codes for issue tickets.

Issue Status Code	Description
Approval in Progress	An issue is open, pending approval.
Cancelled	An issue has been cancelled.
Closed	An issue has been completed.
Hold	The service type events for the issue are on hold.
Implementation in Progress	An issue is being implemented.
Open	An issue has been defined and open so that it can be monitored and managed until it is resolved.
Suspended	Stops workflow tasks on an issue.
Transaction in Progress	A transaction with a customer concerning this issue is in progress.
Verification in Progress	An issue is being verified.

If your site uses other terminology for identifying the status of an issue, you should define status codes that suit your needs and ignore the predefined status codes, or change the definitions to match your use. For example, you may want to define additional issue status codes, such as the following:

Issue Status Code	Description
Duplicate	Issues that have been opened but may be a duplicate of an existing issue for another user.
Emergency	Critical issues that must be addressed immediately.

Issue Status Code	Description
Report	Issues that are completed and closed, but should be reported on at a management level.

Task Status Codes

Task status codes describe the different possible states of a workflow task. Each task in an issue or change order or request/ incident/ problem workflow has its own status, separate from the ticket status. Workflow tasks allow analysts to keep track of how long it takes to complete individual tasks within a ticket.

The following table describes the predefined status codes for workflow tasks.

Task Status Code	Description
Approve	Task approved.
Cancelled	Task is cancelled and no further updates are possible.
Complete	Task is complete.
Pending	Task is started.
Reject	Task is rejected.
Reopen	Task has been re-opened.
Reopen - Wait	A prior task was reopened.
Skip	Skip task.
Wait	Task has not started.

If your site uses other terminology for identifying the status of a workflow task, you should define status codes that suit your needs and ignore the predefined status codes, or change the definitions to match your use.

For each task status code, you can assign a type of behavior that occurs when the task reaches this state, which provides much more information about the progress toward completing the task. You can also use the accumulate function to track time and cost involved in completing the ticket.

Task Types

Task types help determine the behavior of specific workflow tasks and task status codes. To produce defining characteristics for each type of task, you can identify the task status codes or specific states that can be used.

Because change orders, issues, and request/ incident/ problem use workflow tasks, set up task types for all service desk models. The task status codes identify the behaviors associated with each task. For example, you can set the Approval task type to allow Approve, Reject, Pending, and Wait as available states. When the Approval task type enters the Pending state, you can send notification to a specific manager, analyst, and so forth.

You can mark any task type as active or inactive. When you mark a task type as inactive, it is no longer available for analysts to use, but it remains available for future use (it is not deleted from the database). If you decide later to use the task type, mark it as active again.

Note: You can view the predefined task types in the Task Type List page of the administrative function of the web interface.

Example: Task Status Codes

The following table contains some example status codes:

Task Status Code	Description
Approval	Approve or reject ticket
Group End Task	End of group tasks
Group Start Task	Start of group tasks
Start Approval	Approval to start the ticket

In this example, the Group Start Task and Group End Task types define a group of tasks in an issue or change category that must be completed. Tasks in the group can be executed in any order. After the Group Start Task is in the Pending state (started), all tasks in the group are also placed in this state.

Define Code for Application Data Components

You can define codes for your application data components. To create a code, select Service Desk, Application Data, Codes, <code_that_you_want_to_create> from the Administration tab.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants. If you are the Service Provider, select the appropriate tenant from the dropdown menu. The public (shared) option creates the object for all tenants.

Code	Description
Attribute Alias	CA SDM includes an ODBC driver that allows an external application, such as Web Intelligence, to submit SQL SELECT queries directly to the CA SDM object manager (domsrvr). The driver depicts CA SDM Majic object names and attributes as tables and columns of a virtual database. In addition, the driver allows an unlimited number of attribute alias columns to be added to each object. Each attribute alias defines a pseudo-column corresponding to a column of a joined table. For example, the attribute alias assignee_organization_name corresponds to the Majic dotted join assignee.organization. name.

Code	Description
	Attribute alias codes provide a flattened view of the database. They allow you to include columns from related tables. By convention, an attribute alias name is the same as the Majic join name, with the dots replaced by underscores. For example, if a Call Request report needs to show the assignee's organization name, and this column was not provided out of the box, you could define an alias called assignee_organization_name that equates to assignee.organization.name. To create this code, the object name is the majic object name associated with the attribute alias. For more information about objects, see the Technical Reference (see page 3821) topic.
Auto Close Settings (https://wiki.ca.com/display/CASM/.Define+Auto+Close+Settings+v14.1)	You can use a configurable setting to allow automatic closure of CA SDM tickets. When a ticket is set to a Resolved status, the ticket is automatically closed in the number of business hours specified. The Auto Close activity notification sent to the end user displays the number of business hours before the ticket is closed. You can configure business hours for each tenant. If the status is changed before the configurable number of hours ends, the ticket closure is canceled. As a system administrator, you can perform the following actions: ▪ Define an Auto Close ticket setting to control the number of business hours, for the end user, before the ticket is automatically closed. ▪ Set up an Auto Close activity notification to notify the appropriate contacts when automatic closure is scheduled for a ticket. When an analyst changes the status of a ticket to a Resolved status, the ticket is automatically closed in the number of business hours specified. After the ticket is closed, an activity log is added to the ticket. The Auto Close activity notification sent to the end user displays the number of business hours before the ticket is closed. The number of hours is configurable and tenant-specific. If the status of a ticket is changed before the configurable number of hours ends or expires, the automatic ticket closure is canceled. For each ticket type and tenant, you can define a different number of business hours. If business hours are not defined for a particular tenant, the public setting is used instead. If you use multi-tenancy, consider the following: ▪ The system uses the default public Auto Close setting when a tenant-specific Auto Close setting is not found. ▪ There is one Auto-Close setting for each tenant.
Contact Type	Contact type codes are classifications for the people associated with your network, such as vendors, analysts, or customers. Contact type codes let you sort and select information based on the kind of person involved with a ticket. For example, you can report on how many tickets were created by an outside vendor contact. You can also use contact types to restrict certain functions to certain types of users. For example, only users with the contact type of analyst can resolve tickets.
Cost Centers	A cost center is a group or unit that uses purchased assets. Cost center codes are used to roll up groups of purchased assets for budgeting and reporting purposes. A cost center could be an internal department, a subsidiary, or any group that needs to have its assets tracked separately.

Code	Description
Countries	You can associate country codes with your organization's location codes, as part of the address information.
Departments	You can define department codes to reflect the departments within your organization. Departments can then be associated with records such as contacts and groups.
End User Roles	End user role codes categorize the various people who contact the service desk. For example, a user might be an existing customer, a potential customer, or a sales manager.
iCalender Event Templates	iCalendar event templates control the information that is exported to iCalendar format. The following predefined templates are installed with CA SDM: ▪ Change Schedule ▪ KnowledgeScheduleCreation ▪ KnowledgeScheduleExpired ▪ KnowledgeScheduleReview ▪ KnowledgeScheduleStart **Note:** You can edit the predefined iCalendar event template codes, but you cannot delete or create them. **Important!** The SchedExpMaximum variable in web.cfg controls the maximum events allowed for an export. Increasing the default (1000) could cause system instability. If you attempt to export more than the value specified in SchedExpMaximum, a message appears refusing your exporting request. You can set a display alarm (such as 1 Day before or 1 Hour before) for each event that creates a calendar.
Impact	Impact codes indicate how much a ticket affects work being performed. You can use impact codes to select and sort records, and organize them for reports. The predefined impact codes are: ▪ 1-Entire organization ▪ 2-Multiple Groups ▪ 3-Single Group ▪ 4-Small Group ▪ 5-One person ▪ None = No Impact is assigned You can change the symbols for impact codes. For example, your site might decide not to use numbers at all and assign codes of low, medium, high, and so on. **Note:** You can edit the predefined impact codes, but you cannot delete or create them.

Code	Description
Location	Location codes precisely identify a physical place. You can use location codes to identify where inventory components reside, such as contacts and resources like printers. Location codes can identify any type of place, for example, a city, building, or a specific floor of a building. You can configure automatic ticket assignment for the location, based on request areas, change categories, issue categories, and groups. For example, to auto assign issue tickets in a certain category to analysts associated with this location, click the Update Issue Categories button on the Auto Assignment tab and select the category from the list. For more information about configuring Auto Assignment, see Auto Assignment (https://wiki.ca.com/display/CASM/.Auto+Assignment+v14.1).
Organization	Organization codes can define the companies, divisions, or departments in your enterprise. You can use organization codes to indicate the working and reporting relationships of your service desk users. This information is defined on a user's contact records and displayed on their tickets. Organizations can also be assigned to the resources in an asset class, or the issues assigned to a specific ticket area or category.
Outage Type	Outage types represent a single general type of outage for an incident that a user reports, or to specify other types of outages such as a scheduled or test outage. When a user reports an outage incident, you can specify an outage type on the ticket to help categorize and track the incident. For example, you can use an outage type of Facilities on a ticket to indicate that an outage that affected the end-user facilities.
Position	Position codes can indicate the job title of a person who opens a ticket.
Priority	Priority codes indicate the amount of attention a ticket should receive. Priority codes are used when defining automatic notification and external processing for specific types of situations. They are also used as a label in the scoreboard to prioritize tickets. You can modify a priority code's symbol. For example, your site might decide not to use numbers at all and assign priority codes of low, medium, high, and so on. You can modify a priority code's associated service type. For example, you could change the service type for priority code 1 from the default value of 04hr resolution to a custom service type of 02hr resolution.
Product	Product codes identify the products supported by your service desk.
Reason	Reason codes define the purposes for opening tickets. For example, a reason for opening an issue might be an inquiry, a complaint, or a suggestion.
Reporting Methods	Reporting method codes define the ways a ticket can be reported to the service desk. For example, a customer might create an issue over the phone or via e-mail.
Resolution	Incident management focuses on getting the end user up and running as fast as possible. Analysts can indicate what they did to resolve an incident by using a resolution code. Resolution codes specify the category code of the ticket resolution, for example, an Applied Patch resolution code indicates that the ticket was addressed by applying a patch or fix to the software.
Resolution Method	Resolution methods define the ways the service desk can resolve tickets. For example, an analyst can resolve an incident or request through a chat session or an on-site visit.
Root Cause	

Code	Description
	Root cause codes identify the source of a problem reported in your service desk. Root cause codes comprise a set of nodes, which are separated by periods to indicate where the root cause fits into a hierarchy of root causes. For example, the root cause name Network. Cable.Install indicates the Install root cause as part of the Cable root cause, which in turn is part of the Network root cause. By default, the Root Cause Selection window displays as a hierarchical selection list. If you want to display the Root Cause Selection window as a normal list, you can install the no_hier_list option through the Options Manager.
Severity	Severity codes indicate the effect a ticket has on people. For example, a printer problem might affect a larger number of people than the failure of user system or computer. Severity codes are used to select and sort tickets and organize them for reports.
State /Province	State/province codes identify the states and provinces where tickets might originate in your service desk.
Symptom	Symptom codes represent a single general symptom for an incident that a user reports. When a user reports an incident, you can specify a symptom code on the ticket to help categorize and track the incident. For example, you can use a symptom code of Slow Response on a ticket for an application that is not running as fast as a user expects.
Timer	Timers act as a stopwatch with various thresholds that give the analyst indications of elapsed time. You can define the amount of time the timer remains at each threshold, and have the timer change color, beep, or display a reminder as it reaches each threshold. A service desk analyst cannot control the stopwatch; only the administrator can control it. Requests are the only type of ticket that uses timers; therefore, set up timers for internal and combined service desk models. For more information, see Timer Setup (see page 1026).
Time Zone	You can set up specific time zones for servers, service types, contacts, and locations in your CA SDM system. You can set up local service types that apply to a specific time zone and global service types that apply across the entire enterprise. This setup eliminates the need for the administrator to know the time zone of a server and manually adjust the work shift times to fit different time zones. For more information, see Time Zone Setup (see page 1026).
Urgency	Urgency codes indicate the importance of the user tasks affected by a ticket. You assign urgency codes to tickets based on how it affects user tasks. Urgency codes can be used to select and sort information and to organize it for reports.
Web Macro	CA SDM includes a number of predefined macros. Most of these macros insert JavaScript text to create an element on a web form. Use Web Screen Painter to create and modify forms using these macros.
Workshift	Workshift codes specify the dates, days, and times when the monitoring of an event is in effect. You can add new workshifts or update existing workshifts. Workshifts often coincide with the times your service desk is operating. By defining workshifts, you can set up events and monitor them precisely. For more information, see Workshift Setup (see page 1028).
Timespan	Timespan codes allow you to define time spans that can be applied to stored queries. You can create time spans that control the start time, end time, and trigger time of stored queries.
Site	

Code	Description
	Site codes represent general groupings, such as cities or regions. Sites can include several locations, which are physical places like buildings or floors. Site records are referenced in location records. You should create site records before location records so the sites are available when you define the locations.

Timer Setup

The following threshold values are predefined for the timer:

Threshold Duration	Color
00:00:00	Green
00:01:00	Yellow
00:05:00	Red

The predefined values start the timer at green. After one minute, the timer changes to yellow. After five minutes, the timer changes to red. The elapsed time is displayed when the analyst views the request in detail and is reset each time a new request is selected. You can add steps to this process or change existing steps.

You can mark any timer as active or inactive. When you mark a timer as inactive, it is no longer part of the process, but it remains available for future use (that is, it is not deleted from the database). If you decide later to use the timer, back to it and mark it as active.

Timer codes control the reminders to analysts that they have been working on a request longer than the recommended amount of time. This way of reminding analysts has the recommended amount of time defined as a threshold, such as 5 minutes. The timer then uses various methods to indicate that the threshold has been reached. These methods include sounding beeps, changing the background color of the Timer field on the Request Detail window, or displaying messages telling the analyst to resolve the request as quickly as possible.

The Timer field that tracks the time spent on a request is reset each time the request is opened, and service desk analysts cannot control it or change it.

Time Zone Setup

Contents

Timezone codes are specified for users in their contact record. A timezone code displays the local time for users, regardless of their locations around the world, in the Time field on the Quick Profile, thus allowing you to see if it is currently during business hours for them.

You can add new timezone codes, and modify the predefined ones. Timezone codes indicate the time difference difference between a particular time zone and Greenwich Mean Time (GMT). You can also specify when to start and end Daylight Savings Time, if applicable.

Service Type Event Triggers

Service types define the events that are triggered after a specified delay time.

Example: Event Triggers by Work Shift Schedule

In this example, a work shift schedule associated with the service type constrains the actual time an event is triggered, as follows:

- Work shift is 8:00 a.m. to 5:00 p.m.
- Event delay is three hours
- Current server time is 3:00 p.m.

The event is triggered tomorrow at 9:00 a.m. server time because of the following:

- According to the current server time, two hours remain in the work shift for today (Current time is 3:00 p.m. Work shift ends at 5:00 p.m.)
- The event delay is three hours. Two hours of this delay are spent in the current day's work shift (3:00 p.m. to 5:00 p.m.). One additional delay hour is carried over to the next day's work shift (8:00 a.m. to 9:00 a.m.)

Consequently, the event begins at 9:00 a.m. the following day.

Time Zone Event Triggers

A time zone associated with the service type can constrain event trigger times.

Example: Event Triggers by Time Zone

In this example, a time zone associated with the service type constrains the actual time an event is triggered as follows:

- Work shift is 8:00 a.m. to 5:00 p.m.
- Event delay is three hours
- Current server time is 3:00 p.m.
- Current time in time zone is 12 noon

The event is triggered today at 6:00 p.m. server time because of the following:

- According to the current server time, two hours remain in the work shift for today (Current time is 3:00 p.m. Work shift ends at 5:00 p.m.).
- According to the current time zone time, five hours are left in the work shift for today (Current time is 12 noon Work shift ends at 5:00 p.m.).
- The event delay is three hours (12 noon to 3:00 p.m. time zone time. 3:00 p.m. to 6:00 p.m. server time).

Consequently, the event begins at 6:00 p.m. server time or 3:00 p.m. time zone time.

Time Zone Rules

You can specify a time zone for a server, for a location, and for a service type. You can also tell CA SDM to use the time zone of the Affected End User of a ticket. CA SDM uses the following rules to determine which time zone triggers an event:

- **Affected End User time zone** -- CA SDM uses this rule when the following conditions exist:
  - The Use End User Time Zone option is selected.
  - A time zone is specified for the affected end user of the ticket.
- **Affected End User location time zone** -- CA SDM uses this rule when the following conditions exist:
  - The Use End User Time Zone option is selected.
  - No time zone is specified for the affected end user of the ticket.
  - A time zone is specified for the affected end-user location.
- **Service type time zone** -- CA SDM uses this rule when the following conditions exist:
  - A time zone is specified for the service type.
  - The Use End User Time Zone option is not selected.
- **Server time zone** -- CA SDM uses this rule when the following conditions exist:
  - A time zone is specified for the server.
  - The Use End User Time Zone option is not selected.
  - No time zone is specified for the service type.
- **No time zone support** -- CA SDM uses this rule when the following conditions exist:
  - No time zone is specified for the service type.
  - The Use End User Time Zone option is not selected.
  - No server records exist.

Workshift Setup

Contents

You can create new workshift codes.

Follow these steps:

1. Select Service Desk, Application Data, Codes, Workshifts on the Administration tab.
   The Workshift List page appears.

2. Click Create New.
   The Create New Workshift page appears.

3. Complete the fields as appropriate. The following tabs are available on the Create Workshift, Workshift Detail, and Update Workshift pages:

   - **Schedule**
     Specifies the days, date, and time of the workshift. You can specify days, or dates, or both days and dates. Specifying a time is optional. Use the following syntax:

     ```
     day_range date_range [{time}]
     ```

     - **day_range**
       Specifies a day or range of days in the following format:

       ```
       week_day | week_day - week_day
       ```

       Valid week_day values are Sun, Mon, Tue, Wed, Thu, Fri, and Sat.

     - **date_range**
       Specifies a date or range of dates in the following format:

       ```
       date | date - date
       ```

       Enter date as mm/dd/yy, where mm is the month, dd is the day, and yy is the year.

     - **{time}**
       Specifies a time or range of times in the following format:

       ```
       {hh:mm[:ss] [am or pm]} | {hh:mm[:ss] [am or pm]} - {hh:mm[:ss] [am or pm]}
       ```

       Time values must be enclosed in braces. Enter time in hours, minutes, and optionally seconds, where hh represents hours, mm represents minutes, and ss represents seconds. You may optionally specify am to identify a time from midnight to noon; this is the default and need only be specified for clarity. You must specify pm to set a time interval from noon to midnight. You may also omit am and pm and specify hours from noon to midnight in 24-hour format, for example 13:30. If am and pm are used, hour values greater than 12 are invalid.

       Note: If the server and clients are in different time zones, events take place according to the time zone of the server.

     Examples:

     ```
     Mon - Fri {8:00 am - 5:00 pm}
     ```

```
Sun {9:00 - 12:00 2:00 pm - 4:00 pm}

Sat 12/24/08 - 1/1/05 {8:00 - 12:00 14:00 - 4:00 pm}

7/4/09
```

Note: Sat 12/24/08 - 1/1/09 indicates every day from December 24, 2008 through January 1, 2009. It does not mean just Saturdays within the specified date range. 7 /4/09 means no work hours on July 4, 2009.

- **Auto Assignment**
  Allows you to configure automatic ticket assignment for the workshift, based on request areas, change categories, and issue categories. These fields are optional. Editable. For more information about configuring Auto Assignment, see the Auto Assignment (see page 1132) topic.

You can click the More icon to display the Additional Search Arguments field. This field is intended only for expert users who understand SQL and Majic. You can enter a SQL WHERE clause in this field to specify an additional search argument.

4. (Optional) Perform the following steps to configure automatic assignment of request, incident, or problem tickets for this workshift:

   a. Click Update Request Areas.
   The Request/Incident/Problem Area Search page appears.

   b. (Optional) Complete the filter fields to display only the area records of interest and click Search.
   The Request/Incident/Problem Area Update page appears.

   c. Select the areas you want to assign to this workshift from the Request Areas Available list. To select multiple areas, hold down the CTRL key while clicking the left mouse button, or hold down the Shift key to select a range of areas.

   d. Click the double right-arrow button.
   The selected areas move to the Request Areas Assigned list.

   e. Click OK.
   The Workshift Detail page displays the selected request areas on the Auto Assignment tab.

5. (Optional) Perform the following steps to configure automatic assignment of change orders for this workshift:

   a. Click Update Change Categories.
   The Change Category Search page appears.

b. (Optional) Complete the filter fields to display only the category records of interest and click Search.
The Change Categories Assigned Update page appears.

c. Select the categories you want to assign to this workshift from the Change Categories Available list. To select multiple categories, hold down the CTRL key while clicking the left mouse button, or hold down the Shift key to select a range of categories.

d. Click double right-arrow button.
The selected categories move to the Change Categories Assigned list.

e. Click OK.
The Workshift Detail page displays the selected change categories on the Auto Assignment tab.

6. (Optional) Perform the following steps to configure automatic assignment of issue tickets for this workshift:

a. Click Update Issue Categories.
The Issue Category Search page appears.

b. (Optional) Complete the filter fields to display only the category records of interest and click Search.

c. The Issue Categories Assigned Update page appears.

d. Select the categories you want to assign to this workshift from the Issue Categories Available list. To select multiple categories, hold down the CTRL key while clicking the left mouse button, or hold down the Shift key to select a range of categories.

e. Click double right-arrow button.
The selected categories move to the Issue Categories Assigned list.

f. Click OK.
The Workshift Detail page displays the selected issue categories on the Auto Assignment tab.

7. Click Save.
The new code definition is saved.

Create Personal Responses

You can create personalized responses and attach them to requests, issues, and change order records when adding activities to the record. For example, you can append a personalized response on the Status Change or Log Comment windows available from the Activities menu.

Follow these steps:

1. From the Administration tab, navigate to Service Desk, Personal Responses.
The Personal Response list page appears.

2. Click Create New.
   The Create New Personalized Response page appears.

3. Fill in the fields on this page including:

   - **Response Owner**
     The contact who owns the response. If this field is left blank, the response is available to all analysts.

   - **Response**
     The text delivered to all those who receive this response. This field can be up to 1000 characters long.
     You can use variables in this field, for example:
     Ticket ref_num: @{call_req_id.ref_num}
     Assignee: @{call_req_id.assignee.combo_name}
     Customer: @{call_req_id.customer.combo_name}
     Description: @{call_req_id.description}

4. Select the type of records for which you want this response available. By default, all record types are selected.

5. Click Save.

Edit a Sequence Number Format

Contents

Sequence Numbers

Sequence numbers define the format for your ticket numbering scheme. You can modify the predefined sequence number formats, but you cannot create new ones.

Note: CA SDM treats the number format as a character string, not as a sequence of numbers. Therefore, when you load tickets into CA SDM from another system, assign a unique prefix or suffix so that existing tickets are not inadvertently overwritten.

When a ticket is opened, it is automatically assigned the next available sequential number. For example, if the last request opened is 5, the next one is assigned the number 6.

Important! After you install a new version of CA SDM, the internal record ID for all tickets is reset to 1. To help ensure that duplicate record IDs are not created, do not create tickets before restoring any backed-up data.

You can configure how requests, change orders, and issues are numbered by including a unique prefix or suffix in the numbering scheme for each one. For example, if you want to track requests by month, you can add a month identifier as a prefix or suffix to the request numbering scheme.

Because you define a separate numbering scheme for each type of ticket, set up numbering schemes for all service desk models. You can control the format of the numbering of requests, change orders, and issues by changing the Sequence Number settings. By default, new tickets are numbered using consecutive integers. Because the number field of a ticket is actually a string field and not numeric, you assign additional string values to use as prefixes or suffixes when the ticket number is generated for a new ticket. For example, you can specify r:, c:, and i: for prefixes for requests, change orders, and incidents. This setup lets users easily differentiate between the various ticket types and prevents confusion.

Incidents and problems share numbering schemes with requests, because incidents and problems are internally different types of requests.

Edit a Sequence Number Format

You can edit an existing sequence number format, but you cannot create new ones.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants. A tenant dropdown appears in the search filter. If you select <empty> in this dropdown, the search is public. A tenant column also appears on the list page.

Follow these steps:

1. Select Service Desk, Sequence Numbers on the Administration tab.
   The Sequence Number Control List page appears.

2. Select the symbol for the sequence number format to edit.
   The Sequence Number Control Detail page appears.

3. Click Edit.
   The Update Sequence Number Control page appears.

4. Edit the fields as needed:

   - **Symbol**
     The name identifying the sequence number format.

   - **Prefix**
     The character string that forms the first part of the ticket number.

   - **Code**
     The internal code name for the number format. Cannot be changed.

   - **Suffix**
     The character string that forms the last part of the ticket number.

5. Click Save.
   The format definition is saved and the Sequence Number Format Detail page appears.

Define Closure Codes

You use closure codes to indicate the final outcome of a change order. You set the field manually or when updating status activity on a change order. CA SDM provides the following default closure codes:

- **Successful**
  Indicates the change order was successful.
- **Unsuccessful**
  Indicates the change order was unsuccessful.
- **Successful with Errors**
  Indicates the change order was successful, but directly or indirectly caused errors.

You can define closure codes to use in managing change orders.

Follow these steps:

1. On the Administration tab, select Service Desk, Change Orders, Closure Code.
   The Closure Code List appears.
2. Click Create New.
   The Create New Closure Code page appears.
3. Complete the required fields.
4. Save and close the window.

Define Change Type Codes

Change type codes identify how change orders fit within the operating practices of the organization. Predefined codes are provided for the following ITIL change types:

- **Standard** -- A change to a service infrastructure that is pre-authorized by change management and has an accepted and established procedure to provide a specific change requirement
- **Normal** -- A change that is raised by request from the initiator (an individual or group) that requires the change
- **Emergency** -- A change that is accelerated outside of normal processing, which sometimes adds a higher risk or impact than if handled normally

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. Select Service Desk, Change Orders, Change Type on the Administration tab.
   The Change Type List appears.

2. Click Create New.
   The Create New Change Type page appears.

3. Complete the required fields:

   - **Symbol**
     Defines an identifier for the change type code. This identifier appears in the Type field on a ticket.

   - **Status**
     Specifies whether this database record is active or inactive. Select a value from the drop-down list.

4. Click Save.
   The change type record is saved and the Change Type Detail page appears.

Define Change Order Status Transition

Change order status transitions control the movement of a change order ticket from one discrete state to another (for example, from Open to Closed). With transitions, you can define a subset of the full status list and determine the next status of the ticket as it continues through its lifecycle. You can use the predefined transitions (listed on the Change Order Transitions List page), modify the transitions, or create transitions.

Note: You can specify how strictly the system enforces Status policies by configuring the Status Policy Violations option in Options Manager (General Options). This option only applies to automated system processes, such as integrations and macros.

You can define a subset of the full status list and determine the next status of the ticket as it continues through its lifecycle.

Note: Because status transitions can be shared between integrations such as CA Workflow and Events and Macros, do not inactivate predefined status transitions unless explicitly requested.

Follow these steps:

1. On the Administration tab, select Service Desk, Change Orders.
   The Change Order Transition List page appears.

2. Complete the fields as appropriate. The following fields require explanation:

- **From Status**
  Defines the current status of the ticket, for example, Open.

- **To Status**
  Specifies a valid next status of the ticket, for example, Assigned.

- **Default Transition**
  Specifies the default status transition. CA SDM uses the default transition when a user clicks the default transition button on the ticket detail page, or when a user (including a web services user) updates the status to a <d> value. You can only configure one default transition for each status (or one for each tenant in a multi-tenanted system).

- **Must Comment**
  Indicates that a comment for the transition must be supplied. Specifying this option indicates that an analyst must supply an activity log comment when changing the status on a request.

- **Condition**
  Specifies the condition by which the transition is allowed. For example, when the condition "nonprty 1&2 assigned req" is associated with the Request Transition of Acknowledged to Hold, the condition verifies if the transition to move the status from Acknowledged to Hold is allowed.

- **Condition Error Message**
  Specifies the message returned to the user if the transition is rejected.

- **Description**
  Specifies the message returned to the user if the transition is rejected.

The transition is defined.

3. Click Save, Close Window.
   The new transition appears in the Change Order Transition List when you refresh the page.

Update Initial Status Transitions

You can update the list of statuses that are valid at initial creation of the ticket.

Follow these steps:

1. On the Transitions List page, click the Initial Transitions button.
   The Initial Transitions page appears and displays all available status codes and descriptions.

2. Fill in the following check boxes as appropriate:

   - **Allowed**
     Specifies a valid transition for the status list. Use this option to restrict status workflows.

   - **Default**
     Specifies the default status transition. CA SDM applies the default transition when a user clicks the default transition button on the ticket detail page, or when a user (including a web services user) updates the status to a <d> value. There is only one default transition for each status (or one for each tenant in a multi-tenanted system).

- **Must Comment**
  Specifies that an activity log comment for the transition is required when changing the status on a ticket. An error message appears on the ticket form when the analyst attempts to close the ticket without adding a comment.

3. (Optional) Select a status code in the Name column to update its details.

4. Click Save.
   The updated status transition appears on the Transitions list.

Define Workflow Task Status Code

Workflow task status codes can be attached to change orders, issues or requests/ incidents/ problems. For example, this code can indicate how close the change order is to being completed. Each workflow task has its own status, which remains separate from the status for the entire change order. Workflow task status codes allow you to locate, categorize, and track change orders based on their workflow status.

Follow these steps:

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

1. On the Administration tab, browse to Service Desk and select any of the following:

   - Change Orders
   - Issues
   - Requests/ Incidents/ Problems

2. Select Workflow Task Status Codes.
   The Task Status Code List appears.

3. Click Create New.
   The Create New Task Status page appears.

4. Complete the fields as appropriate.

   Symbol - Defines an identifier for the task status code. This identifier appears in the Status field next to the tasks listed on the Workflow Tasks notebook page of the issue or change order. This is a required field.

   Code - Displays the internal code for the task status. This is a required field.

   Record Status - Identifies whether the database record is active or inactive. This is a required field. Select a value from the drop-down list.

Allow Task Update - When checked, indicates that an analyst can change the status of the task. This allows a qualified person to override a status that is entered by default, such as Pending.

Task Completed - When checked, indicates that the task is complete when it reaches this status. This option cannot be selected if Allow Task Update is selected.

Allow Accumulate - When checked, includes tasks with this status in calculations of estimated cost and duration for the original issue or change order. If not selected, tasks with this status are not included in estimates made by choosing the Accumulate feature on the Issue Detail or Change Order Detail window.

Continue to Next Tasks - When checked, changes the status of the next task to Pending when the current task reaches this status. This option can only be selected if Task Completed is selected.

Stop Service Type Events - When checked, automatically delays service type events when a task is changed to this status. For example, the predefined Hold status has this option checked, so that when you change the status of a task to Hold, all service type events are stopped.

Cannot Update Message - Displays the contents of this field if Allow Task Update is not selected and someone tries to change a task with this status.

Last Modified Date - Displays when the record was last modified, in the time zone of the server. This field is read-only, and is filled automatically each time the record is updated.

Last Modified By - Displays the name of the contact who last updated this record. This field is read-only, and is filled automatically each time the record is updated.

5. Click Save.
   The task status code definition is saved.

Define Change Status Codes

Change order status codes indicate how close a change order is to being completed. The status code appears in the Status field on a change order. Once change orders are assigned status codes, you can locate, categorize, and track them based on their condition.

Follow these steps:

1. On the Administration tab, select Service Desk, Change Orders, Status.
   The Change Order Status List appears.

2. Click Create New.
   The Create New Change Order Status page appears.

3. Complete the fields as appropriate. The following fields require explanation:

   - **Make Change Order Active**
     Activates an inactive change order, request, or issue when assigned to a ticket.

- **Stop Service Type Events and Targets**
  Automatically delays service type and events and targets for a ticket. For example, the predefined Hold status has this option checked, so when you change the status of a ticket to Hold, all service type events and targets are stopped.

- **Make Change Order Resolved**
  Indicates that a change order is resolved.

4. (Optional) Use the controls available on the tabs at the bottom of the page to configure the following:

   - **Change Order Transitions**
     Controls how users select available statuses on the ticket form. With transition controls, you can control how a ticket transitions through different statuses by limiting the status list. You can use predefined transitions, modify the transitions, or create transitions.

   - **Change Order Dependent Attribute Controls**
     Controls how attributes are designated as required (must supply) or locked (cannot update) depending on ticket status. With dependent attribute controls, you can determine which fields are shown, or required for the status. You can use predefined attributes, modify the attributes, or create dependent attributes.

5. Click Save.
   The status record is saved and the Change Order Status Detail page appears.

Risk Level

Risk levels determine the amount of risk involved in a change order. Risk levels are calculated after submitting risk surveys for a change order.

- **Level**
  Specifies the name of the risk level.

- **Value**
  Specifies the value of the risk level.

- **Description**
  Specifies the description of the risk level.

- **Status**
  Specifies if the risk level is active or inactive.

Define Issue Status

Issue status codes indicate how close an issue is to being completed. The status code appears in the Status field on an issue. Once issues are assigned to status codes, you can locate, categorize, and track them based on their condition.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Administration tab, browse to Service Desk, Issues, Status.
   The Issue Status List displays.

2. Click Create New.
   The Create New Issue Status page displays.

3. Complete the fields as appropriate.

   Record Status -- Shows whether this database record is active or inactive. This is a required field. Select a value from the drop-down list.

   Code -- Identifies the internal code for the status. This is a required field.

   Make Issue Active -- When checked, activates an inactive change order, request, or issue when you assign this status to the ticket.

   Stop Service Type Events -- When checked, automatically delays service type events when a ticket is changed to this status. For example, the predefined Hold status has this option checked, so that when you change the status of a ticket to Hold, all service type events are stopped.

   Make Issue Resolved -- When checked, indicates that an issue is resolved when it reaches this status.

4. Click Save.
   The Issue Status Detail page displays.

5. Click Close Window.
   The new status appears in the Issue Status List when you redisplay the list.

Define a Priority Calculation

This article contains the following topics:

Priority calculation is a predefined set of values that automatically set Priority, Urgency, and Impact values on problems and incident tickets.

Note: If you migrated from a previous release, the priority calculation values must be enabled after the migration. For more information about enabling priority calculation, see the Configure Ticket Management After Upgrade (see page 1040) topic.

You can define a priority calculation to handle, incidents, problems, or both. However because two priority calculations cannot handle the same ticket type, you can review and update existing priority calculations before you create ones. For example, if you want to add a priority calculation to manage problem tickets, first clear the Problem field on the active priority calculation. Then, create a priority calculation to manage problem tickets.

If multi-tenancy is installed, you can use one public priority calculation that applies to all tenants or several tenant-specific priority calculations.

Follow these steps:

1. On the Administration tab, select Service Desk, Request/Incidents/Problems, Priority Calculation.
   The Priority Calculation List page appears.

2. Click Create New.
   The Create Priority Calculation page appears.

3. Complete the following fields as appropriate:

   - **Name**
     Identifies the priority calculation.

   - **Status**
     Specifies the ticket status for this priority calculation.

   - **Incidents**
     Specifies whether this priority calculation applies to incident ticket types.

   - **Problems**
     Specifies whether this priority calculation applies to problem ticket types.

   - **Spelling**
     Verifies the spelling of text in the Description field.

   - **Description**
     Specifies the purpose of the priority calculation.

4. Complete the priority calculation by setting the Priority value based on Impact and Urgency. For example, if the Urgency is 5-Immediate and the Impact affects the 1-Entire Organization, you can select the Priority value of 1 from the drop-down list.

5. Set the following Priority Calculation Options as appropriate:

   - **Impact Default**
     Specifies the initial Impact (see page 3757) value to display when the user creates a ticket.

   - **Override Impact**
     Works with the Impact Increment field. Specifies whether the user can override the ticket Impact value with the Impact level specified in the attached Affected Service.

- **Impact Increment**
  Works with the Override Impact field. Increments the Impact by the specified amount when the user overrides the Impact value. When the ticket uses a blackout window, the Impact value increments only when the open date is within the blackout window time frame. The Impact value can only raise to a maximum of 1-High. For example, if you set the value to 2 and the default Impact is 3-Medium, the user can only override the Impact on a ticket to 1-High.

- **Urgency Default**
  Specifies the Urgency (see page 3807) value to display when the user creates a ticket.

- **Override Urgency**
  Specifies whether the user can override the ticket Urgency value with the Area Urgency level specified in Incident or Problem area.

- **Urgency Increment**
  Works with the Override Urgency field. Increments the Urgency level by the specified amount when the affected end user sets the Escalate Urgency flag.

- **Capture Reason**
  Specifies whether the user is required to enter the reason for changing the Urgency or Impact values. If the user changes the Urgency or Impact values, the Escalate Detail page appears while saving the ticket. The user is required to describe the reason for changing the Urgency or Impact values.

- **Enable for Templates**
  Specifies whether to use the priority calculation for tickets that use templates.

6. Click Reset Matrix if necessary to restore the settings to the defaults.
   The default values reset.

7. Click Save.
   The Update Priority Detail page appears. On the next new or updated ticket or Knowledge Document, the fields update according to the values in the active priority calculation. If no priority calculation is active for a ticket type, the system clears the Priority, Urgency, and Impact fields.

Priority Calculation Search Fields

The following fields are available to search for active and inactive priority calculations:

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The Public Data option specifies whether to include public and tenant priority calculations, exclude public priority calculations, or only show public priority calculations.

- **Name**
  Identifies the priority calculation.

- **Description**
  Specifies the purpose of the priority calculation.

- **Incident**
  Specifies whether to search for priority calculations that manage incidents.

- **Problem**
  Specifies whether to search for priority calculations that manage problems.

- **Status**
  Specifies whether the priority calculation is active or inactive.

Note: You can click the More icon to display the Additional Search Arguments field. This field is intended only for expert users who understand SQL and Majic and can use it to specify search arguments that are not available in the standard search filter fields. You can enter a SQL WHERE clause in this field to specify an additional search argument.

Use Ticket Templates to Calculate Priority Values

If you want ticket templates to calculate priority, you configure the priority calculation with the *Enable for Templates* option. If you enable this option the Urgency and Impact values come from the template, but the priority field comes from priority calculation record. The priority value displays as read-only.

If you do not enable this option, the Urgency, Impact and Priority fields come from the template. You can edit the priority field and no priority calculation is done for the ticket until it is saved.

To use ticket templates to calculate priority values

1. On the Administration tab, select Service Desk, Requests/Incidents/Problems, Priority Calculation.
   The Priority Calculation List appears.

2. Select the priority calculation that you want to use for calculating priority with templates. You can also create a priority calculation to use ticket templates to calculate priority values.

3. Select *Enable for Templates* from the Priority Calculation Options list.

4. Click Save.
   The option is enabled.

Manage Request/Incident/Problem Status

This topic contains the following information:

- Define Dependent Attribute Controls (see page 1046)

Define a Request/Incident/Problem Status

Request/incident/problem status codes indicate how close a ticket is to resolution. Status codes allow you to track the progress of tickets, and categorize and locate tickets based on their condition. As a system administrator, you can use predefined status codes, modify the predefined status codes, or create new status codes.

You can mark any request/incident/problem status as active or inactive. When you mark a status code as inactive, it is no longer available for analysts to use, but it remains available in the database for future use. If you decide to use the request/incident/problem status in the future, you can go back and mark it as active.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Administration Tab, select Service Desk, Requests/Incidents/Problems, Status.
   The Request/Incident/Problem Status List page appears.

2. Click Create New.
   The Create New Request/Incident/Problem Status page appears.

3. Complete the request/incident/problem status fields (see page 1044) as appropriate.

4. Click Save.
   The Request/Incident/Problem Status Detail page appears.

5. Click Close Window.
   The new request/incident/problem status appears in the Request/Incident/Problem Status List when you redisplay the list.

Request/Incident/Problem Status Fields

The following fields are required to create or update the request/incident/problem status:

- **Symbol** -- Defines a unique identifier for the record. This identifier appears in the Status field on a ticket.

- **Record Status** -- Shows whether the database record is active or inactive.

- **Code** -- Defines the internal code for the status.

- **Make Active** -- If checked, specifies that an inactive change order, request, or issue is active when you assign this status to it.

- **Stop Service Type Events and Targets** -- If checked, specifies that service type events are delayed automatically when a ticket is changed to this status. For example, the Hold status that is predefined for requests, issues, and change orders has this option checked. When you change the status of a ticket to Hold, all service type events are stopped.

- **Make Resolved** -- If checked, causes the request, change order, or issue to have the Resolve Date /Time automatically set when it is changed to this status.

- **Description** -- Gives a detailed description of the record.

- **Status valid for** -- Defines what ticket types the record is valid for. The default is checked for all ticket types (Requests, Incidents, and Problems).

Note: If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

Update a Request/Incident/Problem Status

As a system administrator, you can modify the predefined status codes or status codes you have created. Request/incident/problem status codes indicate how close a ticket is to being resolved. Status codes let you carefully track the progress of tickets, categorize and locate tickets based on their condition.

You can mark any request/incident/problem status as active or inactive. When you mark a status code as inactive, it is no longer available for analysts to use, but it remains available in the database for future use. If you decide to use the request/incident/problem status in the future, you can go back and mark it as active.

Follow these steps:

1. On the Administration Tab, browse to Service Desk, Requests/Incidents/Problems, Status.
   The Request/Incident/Problem Status List appears.

2. Select the request/incident/problem status.
   The Request/Incident/Problem Status Detail page appears.

3. Click Edit.
   The Update Request/Incident/Problem Status page appears.

4. Update one or more of the fields as needed.

5. (Optional) Use the controls available on the tabs at the bottom of the page to configure the following:

- **Request/Incident/Problem Transitions**
  Controls how users select available statuses on the ticket form. With transition controls, you can control how a ticket transitions through different statuses by limiting the status list. You can use predefined transitions, modify the transitions, or create transitions.

- **Request/Incident/Problem Dependent Attribute Controls**
  Controls how attributes are designated as required (must supply) or locked (cannot update) depending on ticket status. With dependent attribute controls, you can determine which fields are shown, or required for the status. You can use predefined attributes, modify the attributes, or create dependent attributes.

6. Click Save.
   The Request/Incident/Problem Status page appears.

7. Click Close Window.
   The modified request/incident/problem status appears in the Request/Incident/Problem Status List when you redisplay the list.

Define Dependent Attribute Controls

You can designate certain attributes as required or locked depending on the status of the CA SDM ticket (change order, issue, incident/problem/request). For example, a manager can prevent an analyst from editing the summary of a request after approval. For each ticket type, you can use predefined attribute controls, edit the attribute controls, or define attribute controls.

Note: When defining "required" dependent attribute controls for a particular status (all ticket types), be aware that the Edit in List option available on the ticket's list page cannot present the dependent attributes field values that are required. If the required attribute field value is not already part of the saved ticket, and if the required attribute field is not presented in the edit in list format to display its values, then the end user cannot save the ticket. Consequently, the ticket's detail page must be used instead of the Edit in List option to edit the dependent attribute fields values that are required.

Follow these steps:

1. On the ticket's detail page for the status, select the Request/Incident/Problem Dependent Attribute Control tab at the bottom of the page.
   The Attribute Control List appears.

2. Click Create.
   The Update Request Status Acknowledged Dependent Attribute Control page appears

3. Complete the following fields as appropriate:

   - **Tenant**
     Specifies the name of the tenant.

- **Attribute**
  Specifies the name of the attribute control, for example, Summary.

- **Locked**
  Specifies the attribute as locked (read only) while the ticket is in the status for which the dependent attribute is defined.

- **Required**
  Specifies the attribute as required (must be supplied).

4. Click Save.
   The attribute control for the status appears on the list page.

Define Status Transitions

Contents

You can define a subset of the full status list and determine the next status of the ticket as it continues through its lifecycle.

You can also specify how strictly the system enforces status transition policies by configuring the Status Policy Violations option in Options Manager (General Options).

Note: Because status transitions can be shared between integrations such as CA Workflow and Events and Macros, do not inactivate predefined status transitions unless explicitly requested.

To define a status transition

1. On the Administration tab, select Service Desk, Requests/Incidents/Problems, and specify one of the following:

2. Incident Transitions

   - Problem Transitions

   - Request Transitions

   The Transition List page appears.

3. Click Create.
   The Update Status Transitions page appears.

4. Complete the fields as appropriate.
   The transition is defined.

5. Click Save, Close Window.
   The transition appears in the Transition List when you refresh the page.

Edit Status Transitions

You can edit a status transition.

To edit a status transition

1. On the Transition List select a status from the list.
   The Transitions Details page appears.

2. Click Edit.
   The Update Transition Detail page appears.

3. Edit the fields as appropriate.

4. Click Save, Close Window.
   The updated status appears on the Transition Type list.

Update Initial Status Transitions

You can update the list of statuses that are valid at initial creation of the ticket.

To update an initial status transition

1. On the Transitions List page, click the Initial Transitions button.
   The Initial Transitions page appears and displays all available status codes and descriptions.

2. Fill in the following check boxes as appropriate:

   - **Allowed**
     Specifies a valid transition for the status list. Use this option to restrict status workflows.

   - **Default**
     Specifies the default status transition. CA SDM applies the default transition when a user clicks the default transition button on the ticket detail page, or when a user (including a web services user) updates the status to a <d> value. There is only one default transition for each status (or one for each tenant in a multi-tenanted system).

   - **Must Comment**
     Specifies that an activity log comment for the transition is required when changing the status on a ticket. An error message appears on the ticket form when the analyst attempts to close the ticket without adding a comment.

3. (Optional) Select a status code in the Name column to update its details.

4. Click Save.
   The updated status transition appears on the Transitions list.

View Status Transitions

The Transitions List page displays information about the transitions that let you control the movement of a ticket from one status to another (for example, from Open to Closed). The list records the current and new status values of the operation performed (update or insert). You can display the Transitions List for each ticket type.

To view status transitions

1. On the Administration tab, select Service Desk, Requests/Incidents/Problems, and specify one of the following:

2. Incident Transitions

   - Problem Transitions

   - Request Transitions

   The Transitions List page appears and lists attributes. The following fields require explanation:

   - **Status**
     Displays the current ticket status, for example, Open.

   - **New Status**
     Displays the new ticket status, for example, Closed.

   - **Tenant**
     Displays the tenant name.

   - **Default**
     Displays the default transition.

   - **Must Comment**
     Displays whether a comment for the status must be supplied.

   - **Status Description**
     Provides a brief description of the record.

Status Transition Fields

The following fields require explanation:

- **From Status**
  Defines the current status of the ticket, for example, Open.

- **To Status**
  Specifies a valid next status of the ticket, for example, Assigned.

- **Default Transition**
  Specifies the default status transition. CA SDM uses the default transition when a user clicks the default transition button on the ticket detail page, or when a user (including a web services user) updates the status to a <d> value. You can only configure one default transition for each status (or one for each tenant in a multi-tenanted system).

- **Must Comment**
  Indicates that a comment for the transition must be supplied. Specifying this option indicates that an analyst must supply an activity log comment when changing the status on a request.

- **Condition**
  Specifies the condition by which the transition is allowed. For example, when the condition "nonprty 1&2 assigned req" is associated with the Request Transition of Acknowledged to Hold, the condition verifies if the transition to move the status from Acknowledged to Hold is allowed.

- **Transition Type**
  Links a transition type to this transition. Transition types and their corresponding statuses control when employees can close and reopen Incidents and Requests using self-service. This field only displays for Incident and Request status transitions.

- **Condition Error Message**
  Specifies the message returned to the user if the transition is rejected.

- **Description**
  Specifies a description for the status transition.

Setting Up Category or Area

This topic contains the following information:

Change Order and Issue Categories

This article contains the following topics:

Change categories and issue categories define the logical groupings into which change orders and issues can be organized.

Note: Unlike request/incident/problem areas, change order categories and issues categories are managed separately:

- Set up change categories for internal and combined CA SDM models.
- Set up issue categories for external and combined CA SDM models.

You can use categories to specify default values for certain fields in tickets. You can automatically associate a level of service to tickets by assigning a default service type to categories. You can also associate a survey with a category.

For each category, you can specify attributes or qualities to be associated with the ticket and create a workflow that identifies all the individual tasks required to fulfill the ticket. By defining behaviors that are associated with the workflow tasks, you can notify key personnel when the status of the task changes or as activities close the ticket.

Whenever an analyst assigns a ticket to a category, all the information you have associated with the category is automatically entered on the ticket. For example, if you indicate a service type, it becomes associated with the ticket, and its associated service type events.

Predefined Change Categories

The following sets of predefined change categories are installed with CA SDM:

- Add
- Change
- Move
- Retire

Note: All these category sets are subdivided into more specific categories. For example, the Change category set includes categories for changing servers and workstations.

Predefined Issue Categories

The following predefined issue categories are installed with CA SDM:

- Hardware.pc.install
- Software.pc.install

You can set the status of any category to active or inactive. When you make a category inactive, it is no longer available for analysts to use, but it is not deleted from the database. If you decide at a later time to use the category, change the status back to active.

Rules for Changing Categories on a Ticket

The following rules affect only workflow tasks.

- If the previous category used Classic Workflow and the new category uses CA Process Automation, the CA Process Automation process definition links to a workflow on a CA Process Automation server.

- If both the old and new categories use CA SDM workflow, the rules from previous releases apply.
- If the new category uses CA Process Automation and the old uses CA SDM workflow, the following occurs:
  - All incomplete and pending (those tasks that can be updated) workflow tasks of the CA SDM 6.0 style, are set to Cancelled status, regardless of the KEEP_TASKS option. Any completed workflow tasks remain, but they cannot be reopened.
  - All incomplete and nonactive tasks (such as tasks in Wait status) are deleted.
  - The CA Process Automation definition instantiates.
- If the new category uses CA SDM workflow and the old category uses CA Process Automation, the following occurs:
  - The CA Process Automation instance is forcibly set to a status of Terminated.
  - The new category workflow tasks are added as normal.

In a CA SDM workflow, a ticket with a running CA Process Automation instance cannot be closed.

Create Workflow Task Types

Workflow task types specify lists of allowed status codes for workflow tasks assigned to those types. For example, Approval tasks may only allow Approve, Reject, Pending, and Wait status codes, while Install Software tasks may allow Pending, Wait, and Completed status codes.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Administration tab, browse to Service Desk and select any of the following:
   - Change Orders
   - Issues
   - Requests/ Incidents/ Problems
2. Select Workflow Task Types.

   The Task Type List displays.
3. Click Create New.

   The Create New Task Type page displays.
4. Complete the following fields as appropriate.

5. (Optional) Select Update Status Codes on the Status Codes tab and select the codes that you want to assign to the task type.

6. Click Save.

   The workflow task type is created.

Request/Incident/Problem Areas

Request areas define the logical groupings into which you can organize request, incident, and problem tickets. For example, tickets pertaining to an application can be assigned to the predefined Applications area. Whenever an analyst assigns a ticket to a request area, all the information you have associated with the request area is automatically entered on the ticket. For example, if you indicate a service type, it becomes associated with the ticket and all its associated service type events.

Note: The same area definitions are available for request, incident, and problem tickets. On the CA SDM Web Interface Administration tab, these areas are referred to as request /incident/problem areas. For brevity, they are referred to here simply as request areas.

You can set the status of any request area to active or inactive. When you make a request area inactive, it is no longer available for analysts to use, but it is not deleted from the database. If you decide later to use the request area, you need only change the status back to active.

You can use request areas to do the following:

- Specify default values for the group and assignee fields on tickets.
- Automatically associate a level of service to tickets by assigning a default service type to the request area.
- Associate a survey with a request area.
- Select and report on tickets by area by defining your own custom request areas. Eventually study request trends and analyze problem causes. Focusing your view to specific request areas can help make these studies more significant and revealing.

The following predefined request areas are installed with CA SDM:

- Applications
- Email
- Hardware
- Networks
- Printer

- Software
  Software is subdivided into several request areas.

Define a Category or Area

Contents

Issues or change orders can be assigned to categories so that default values defined for a category automatically appear in the fields while creating the issues or change orders.

Request/incident/problem areas define the general areas into which request, incident, and problem tickets can be organized. Categorizing these ticket types lets you generate reports, study trends, and analyze problem causes.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Administration tab, browse to Service Desk, and select any of the following:
   - Change Orders, Categories
   - Issues, Categories
   - Requests/Incidents/Problems, Areas

   The corresponding Area or Category List appears.
2. Click Create New and complete the fields, as appropriate:
   - For information about request/incident/problem areas, see Request/Incident/Problem Area Fields (see page 1055).
   - For information about issue category fields, see Issue Category Fields (see page 1056).

- For information about change category fields, see Change Category Fields (see page 1057)

3. (Optional) Add Properties to Requests/Incidents/Problems Areas (see page 1058) from the **Properties** tab.

4. (Optional) Attach a classic workflow (see page) or attach a CA Process Automation workflow (see page) (if you have integrated CA SDM with CA Process Automation).

> **Note:** You can attach classic workflow to each ticket type area only if you have applied a patch. Find the patch and download details from CA Support Online.

5. (Optional) Enable Auto Assignments (see page) from the **Auto Assignment** tab.

6. Click Save and close the window.
   The category or area is defined.

Request/Incident/Problem Area Fields

The following fields appear on the Create, Detail, and the Update pages for Request/Incident /Problem Areas:

- **Symbol**
  Defines a unique identifier for the record.

- **Organization**
  Specifies the company, division, or department that is associated with the request/incident /problem area. You can enter a value directly or click the magnifier to search for an organization.

- **Record Status**
  Shows whether the database record is active or inactive.

- **Group**
  Identifies the group that is responsible for this record.

- **Assignee**
  Shows the name of the person assigned to the record.

- **Service Type**
  Shows the level of support service received by the contact affected by the record.

> **Note:** Service types are automatically attached to issues based on the service type defined for its issue category. If different service types have been defined for other values on the issue (priority and contact, for example) the service type used is the one with the best (lowest) ranking. For example, if an issue is opened and the From contact has a 12-hour resolution service type, which is ranked as 2, while the priority code has a 4-hour resolution service type, which is ranked as 1, the service type for the issue is a 4-hour resolution.

- **Survey**
  Identifies the defined survey associated with this record. You can enter a value directly or click the magnifier to search for a survey.

- **Area Urgency**
  Specifies how critical the [Request, Incident, Problem] is to the business area.

- **Self-Service Include**
  Displays the request/incident/problem area in the self-service interface.

- **Self-Service Symbol**
  Defines a unique identifier for this request/incident/problem area in the self-service interface.

- **Description**
  Provides a detailed description of the record.

- **This category is valid for the following**
  Defines what ticket types the record is valid for. The default is enabled for all three ticket types (Requests, Incidents, and Problems).

Issue Category Fields

The following fields appear on the Create Issue Category, Issue Category Detail, and Update Issue Category pages:

- **Symbol**
  (Required) Defines an identifier for the category.

- **Code**
  (Required) Defines the internal code for the category.

- **Record Status**
  (Required) Indicates whether this database record is active or inactive. You can select a value from the drop-down list.

- **Group**
  Identifies the group that is responsible for the record. Your system administrator defines groups of contacts that are responsible for different types of issues, requests, incidents, change orders, and so on. Any individual contact assigned to the group can handle the task once it is assigned to the group. Enter a value directly or click the search icon to search for a group.

- **Assignee**
  Identifies the person assigned to the record. Enter a value directly or click the search icon to search for a contact.

- **Service Contract**
  Identifies the service contract name associated with this record. This field is read-only.

- **Service Type**
  Defines the level of support service received by the contact affected by the change order. For example, some users may have contracted for 24-hour support, while others might receive on-site training. Enter a value directly or click the search icon to select a defined service type.

- **Survey**
  Identifies the defined survey associated with this record. Enter a value directly or click the search icon to search for a survey.

- **Children Allowed**
  Allows issues assigned to this category to have subordinate issues. Organizes issues into a hierarchy of parent-child relationships to divide large issues into smaller, more manageable issues.

- **Self-Service Include**
  Displays this category in the self-service interface.

- **Self-Service Symbol**
  Defines a unique identifier for this category in the self-service interface.

- **Description**
  Gives a detailed description of the record.

Change Category Fields

The following fields appear on the Create Change Category, Change Category Detail, and Update Change Category pages:

- **Code**
  (Required) Defines the internal code for the category.

- **Type**
  Defines the level at which change orders are implemented within an organization.

- **Record Status**
  (Required) Indicates whether this database record is active or inactive. You can select a value from the drop-down list.

- **CAB**
  Specifies the group that is responsible for reviewing Requests for Changes (RFCs). The CAB provides multiple perspectives necessary to ensure proper decision making about implementing changes. The CAB can include members from the application team, development manager, component owner, QA, support, and any additional parties deemed necessary. You can enter the value directly or click the search icon to search for the group.

- **Organization**
  Identifies the company, division, or department that is associated with the change category. Enter a value directly or click the search icon to search for an organization.

- **Group**
  Identifies the group that is responsible for the record. Your system administrator defines groups of contacts that are responsible for different types of issues, requests, incidents, change orders, and so on. Any individual contact assigned to the group can handle the task once it is assigned to the group. Enter a value directly or click the search icon to search for a group.

- **Assignee**
  Identifies the person assigned to the record. Enter a value directly or click the search icon to search for a contact.

- **Service Type**
  Defines the level of support service received by the contact affected by the change order. For example, some users may have contracted for 24-hour support, while others might receive on-site training. Enter a value directly or click the search icon to select a defined service type.

- **Survey**
  Identifies the defined survey associated with this record. Enter a value directly or click the search icon to search for a survey.

- **Risk Survey**
  Indicates the defined risk for change orders associated with change categories.

- **Children Allowed**
  Allows change orders assigned to this category to have subordinate issues. Organizes issues into a hierarchy of parent-child relationships to divide large issues into smaller, more manageable issues.

- **Self-Service Include**
  Displays this category in the self-service interface.

- **Self-Service Symbol**
  Defines a unique identifier for this category in the self-service interface.

- **Service Contract**
  Identifies the service contract name associated with this record.

Add Properties

Properties are characteristics or attributes of tickets that are affected by the area or category the ticket is assigned to. For example, when you assign a request to a request area, the properties associated with that area are automatically assigned to the request.

Follow these steps:

1. On the Properties tab, click Add Property.
   The Create New Property Template page appears.

2. Complete the fields as appropriate. To limit the property values to selections from a predefined set, you can specify validation rules.

   The following values on the Properties pages are not self-explanatory:

   - **Sequence**
     Defines the order in which the properties appear on the Properties tab of the tickets assigned to this Area or Category. The property with the lowest sequence number is listed first.

   - **Active**
     Specifies whether the property is active or inactive.

- **Value Required**
  Indicates whether a value must be entered for this property on tickets assigned to this Area or Category. If selected, the word Yes appears in the Required column when this property is listed on the Properties tab of a ticket.

- **Validation Rule**
  Indicates the name of a rule that has been defined to validate user-entered values for this property. Enter the validation rule name directly or click the search button to search for a validation rule.

- **Label**
  The name of the property as it appears on the Properties tab.

- **Examples**
  Examples of appropriate values for the property. For example, if a freeform text field is intended to contain information about a network type, this field might include LAN, WAN, and SAN as example values. These examples appear on the ticket to provide guidance for entering the actual property value.

3. Click Save.
   The detail page lists the new property on the Properties tab.

   The keep_tasks option determines what happens when you assign an existing ticket to a different category:

   - If keep_tasks is not installed, existing properties and workflow tasks are removed from the ticket, and any properties or tasks associated with the new category are added.

   - If keep_tasks is installed, existing properties and tasks are retained on the ticket, and any properties or tasks associated with the new category are added.

Create Property Validation Rules

You can create validation rules to ensure that only valid values are assigned to custom properties. For example, if you have defined a property named Operating System, you can define the validation rule as a drop-down list containing the options Windows, UNIX, and Linux.

Properties that are defined without validation rules are presented to the user as freeform text boxes, which allow any text string to be entered. Validation rules make reporting on area and category values less complex and less error prone.

Note: Property validation rules are reusable. They are not specific to a particular property. You can apply any existing validation rule to properties defined for change categories, issue categories, or request/incident/problem areas.

Depending on which type of validation rule you have configured for a property, when the user assigns a ticket to the category or area to which that property is attached, one of the following controls appears on the ticket properties tab:

- Text Edit Box
- Check Box
- Drop-down List.

Follow these steps:

1. Access the create, detail, or update page for the custom property you want to assign a property validation rule. For example:

    a. Select Service Desk, Change Orders, Categories on the Administration tab.
    The Change Category List page appears.

    b. Click the Add.IT.Server link.
    The Add.IT.Server Change Category Detail page appears.

    c. Select the Properties tab and click the Add Property button.
    The Create New Property Template page appears.

2. Click the Validation Rule link.
    The Property Validation Rule Search page appears.

3. Specify any filter criteria and then click Search.
    The rules that match your filter criteria are displayed.

    Note: Validation rules are not specific to a particular category or area type. You can apply any existing validation rule to properties for change categories, issue categories, or request/incident/problem areas. Although you can create multiple checkbox validation rules, it is not necessary to do so. You can reuse an existing checkbox rule as many times times as you want by applying a different label. For example, if you have an existing checkbox rule named CB, and you later want to apply a checkbox validation rule to a different property, you can select CB from the Property Validation Rule List and then enter a different label on the Create New Property Template page.

4. Click Create New if there is no existing validation rule that meets your needs.
    The Create New Property Validation Rule page appears.

5. Complete the fields as appropriate.

6. For Dropdown validation rules only, the Property Value List tab appears on the Create New Property Validation Rule page. To specify the list of options that appears in the dropdown menu:

    a. Click Add Property Value.
    The Create New Property Value page appears.

    b. Complete the fields as appropriate and click Accept.

> **Note**: The Accept button accepts the changes, closes the window, and applies them to the current record, but you must still click the Save button on the main record window to make the changes permanent.

The Create New Property Validation Rule page appears with a highlighted status indicator showing the number of property values that are pending.

c. Repeat the above steps until you have added all the property values you want the dropdown list to contain.

7. Click Save on the Create New Property Value page.
   The Create New Property Template page appears, with the validation rule name filled in.

Attach a CA Process Automation Workflow

A workflow *process definition* identifies a collective series of tasks, steps, and conditions that are structured in a specific order for individuals or parties to initiate and complete. An administrator creates the workflow process definition and stores it on the CA Process Automation server.

From CA SDM, you attach a workflow process definition to a ticket area or category. Later, when a user creates a ticket with the area or category, the system automatically launches a workflow process instance. The Workflow Tasks tab tracks the workflow progress to completion.

> **Note: (Applicable, if you have applied the patch)** You can attach this workflow for each ticket type (request or problem or incident).

Follow these steps:

1. Click Use ITPAM from the Workflow tab.
   The CA Start Request Form is displayed with the following fields:

   - **Name**
     Specifies a name of CA Process Automation workflow process definition.

   - **Path**
     Specifies the location where the CA Process Automation process is stored on the CA Process Automation server. For example: ServiceDesk/Process/.

   - **Description**
     Describes the workflow.

2. Select the process definition.
   The Start Request Form closes and the process definition appears on the Workflow tab.

3. Click Save.
   The system saves the process settings. The next ticket that a user creates in the specified ticket category or area automatically attaches the workflow and creates a process instance. When the ticket area or category has an attached CA Process Automation process definition, the Workflow Tab contains the following fields:

   - **CA IT PAM Start Request Form**
     Searches for CA IT PAM Start Request forms.

   - **CA IT PAM Process Name**
     Specifies a CA Process Automation workflow process name. The process name you specify must match one of the processes that you specified in the Options Manager *caextwf_log_categories* parameter.

   - **CA IT PAM Process Path**
     Specifies the location where the process is stored on the CA Process Automation server. For example: ServiceDesk/Process/.

Attach a Classic Workflow

Classic workflow is provided as a standard CA SDM component. To allow flexibility, you can define workflow tasks as optional, which allows the analyst to delete them from the task list. All mandatory workflow tasks must be complete before the ticket can be closed. The only exception is that if the ticket status is set to Cancelled, the workflow process terminates automatically. If a ticket is removed from a category with an attached workflow, or assigned to a different category, the workflow process terminates automatically. If the new category has an attached workflow, its process starts automatically.

Ensure that you apply the patch before attaching this workflow to the request/incident/problem area. If you have customized the following files, ensure that you save the customization, apply the patch and then reapply the changes to these files:

- detail_pcat.htmpl
- pcat_wftpl_tab.htmpl
- detail_in.htmpl
- detail_cr.htmpl
- detail_pr.htmpl
- detail_pr.htmpl
- detail_pcat.htmpl
- list_wftpl.htmpl
- detail_wftpl.htmpl
- detail_bhvtpl.htmpl

- detail_cr.htmpl
- detail_in.htmpl
- list_ntfl.htmpl
- list_ntfm.htmpl
- detail_act_type_assoc.htmpl
- detail_evt.htmpl
- detail_macro.htmpl
- list_act_type_assoc.htmpl
- detail_ntfm.htmpl
- list_evt.htmpl
- detail_ntfl.htmpl
- list_slatpl.htmpl
- std_head.htmpl
- detail_sdsc.htmpl
- list_macro.htmpl
- xx_wf_tab.htmpl

Follow these steps:

1. Click Add Classic Workflow from the Workflow tab.

   Note: (Applicable, if you have applied the patch) For each ticket type (request or problem or incident), you can attach a classic workflow. For example, select the Request tab and click Add Classic Workflow. Similarly click Incident or Problem tab to attach the classic workflow, if required.

   The Workflow Definition List appears.

2. Complete the following fields as appropriate:

   - **Task** -- (Required) Defines the CA SDM workflow task type. Click this link to select a task from the Task Type List. For more information about task types, see Define Workflow Task Types (see page 1052).

- **Sequence** -- The order in which this task appears on the ticket's Workflow Tasks tab. The task with the lowest sequence number is listed first. Numbers do not need to be sequential.
- **Record Status** -- (Required) Identifies whether the database record is active or inactive. Select a value from the drop-down list.
- **Assignee** -- The name of the person assigned to the ticket. Enter a value directly or click the search icon to search for a contact.
- **Group** -- The group that is responsible for the ticket. Any individual contact assigned to the group can handle the task once it has been assigned to the group. Enter a value directly or click the search icon to search for a group.
- **Deleteable** -- Determines whether the user can delete this task from tickets.
- **Service Type** -- The level of support received by the organization. For example, some users may have contracted for 24-hour support, and others might receive on-site training. Enter the service type directly into the field, or click the search icon to select the desired service type.
- **Estimated Duration** -- Indicates the estimated date when the task should be finished. The date and time display in mm/dd/yyyy hh:mm am | pm format. Enter the date and time directly or click the calendar icon to select a date.
- **Estimated Cost** -- Estimates how much it costs to complete the task. Enter the amount as an integer without commas or periods. It is best to enter the amount in dollars only.

3. Click Accept. Repeat steps 1 and 2 to add more workflows.
   The workflow tasks appear on the Workflow tab.
4. Use the controls on the following tabs to configure the workflow tasks:
   - **Behaviors**
     Specifies behavior macros to perform actions based on conditions associated with the issue workflow status. For details about working with this tab, see Create a Behavior (see page).
   - **Auto Assignment**
     (Optional) Specifies how workflow tasks are automatically assigned to groups. For details about working with this tab, see Enable Workflow Auto Assignment (see page).

Create a Behavior

You can configure behavior macros to perform specified actions automatically, based on conditions associated with the issue workflow status.

Follow these steps:

1. Click Add Behavior.
   The Create New Behavior Template page appears.

2. Select a workflow task status and active or inactive from the drop-down lists and enter a description of what activities the behavior is configured to perform, then click Save.

   Note: You cannot define the actual functionality of the behavior until it has been saved.

3. Click the behavior's workflow status code on the Behavior tab of the Workflow Template page.
   The Behavior Template Detail page appears.

4. Click the To Do tab.
   Any conditions and macros that have been defined for the behavior appear in the Macro List.

5. Click Edit to update the Macro List.
   Any conditions and macros that have been defined for the behavior appear in the Macro List.

6. Click the Condition link.
   Macro List page appears, displaying the available condition macros.

7. Select a macro from the list.
   The macro symbol appears in the Condition field of the To Do tab on the Update Behavior Template page. For more information about macros, see create a macro from the How to Configure SLAs (see page 1099) topic.

8. Click Update Actions On True.
   The Macro List page appears.

9. Select Action in the Type drop-down list and click Search.
   The Actions On True Update page appears.

10. Select the actions you want to apply when the condition is true and click the arrow button to move them to the selected list, then click OK.
    The Update Behavior Template page appears, displaying your action selections.

11. Click Update Actions On False.
    The Macro List page appears.

12. Select Action in the Type drop-down list and click Search.
    The Actions On False Update page appears.

13. Select the actions you want to apply when the condition is false and click the arrow button to move them to the selected list, then click OK.
    The Update Behavior Template page appears, displaying your action selections.

Enable Auto Assignment

You can specify how CA SDM automatically assigns tickets in an area. You can select location-based auto assignment or CI-based auto assignment.

Note: The Options Manager autoasg_override option controls the circumstances under which auto assignment takes place. If the value of this option is set to 1 (default), CA SDM ignores any existing assignee and group settings and auto assigns tickets in all cases. If you want CA SDM to auto assign tickets only if they are not already assigned, set the option value to 0.

Follow these steps:

Complete the following fields from the Auto Assignment tab and click Save.

- **Auto Assignment Mode**
  Specifies how auto-assignment occurs. You use the Configuration Item Based option to base the auto assignment on the CI Assignable Attribute value.
  - **Disabled** -- Bases the auto-assignment on the Area Defaults option when it is installed.
  - **Configuration Item Based** -- Bases the auto-assignment on the CI Assignable Attribute value.
  - **Location Based** -- Bases the auto-assignment on the location value.
    The automatic assignment process begins with the workshifts defined for the area, proceeds next to groups, and finally to locations. If at any point relationships are defined that fail to satisfy the requirements of the auto assignment process, the process attempts to assign the Default Assignee and Default Group of the area. If no defaults have been defined, the ticket assignment is not changed.

  Note: For details about the auto assignment processing logic, see the Auto Assignment (see page 1132) topic.

- **Assignable CI Attribute**
  Specifies the configuration item attribute to use for the group assignment. You can enter a value directly or click the magnifier to search for an attribute.

Assign Groups

To configure auto assignment for a request/incident/problem area, you must at a minimum define the relationships between analyst groups and the area.

Assignees are chosen from groups that meet all of your specified auto assignment criteria. If no additional constraints are defined, tickets are auto assigned to the group member with the fewest active tickets.

If no groups are associated with the area, the default group and assignee are assigned. If these defaults are not defined, the ticket is left for manual assignment.

Follow these steps:

1. On the Auto Assignment tab of one of the pages, click Update Groups.
   - Change Orders Detail
   - Issues Detail
   - Requests/Incidents/Problems, Areas Detail

   The Group Search window opens.
2. To filter the search, complete one or more of the search fields, or leave all fields blank to search for all groups, then click Search.
   The Groups Assigned Update window opens.
3. Use the arrow buttons to move available groups to or from the Groups Assigned list.
4. Click OK.

Assign Locations

If you assign a location to a request/incident/problem area, the tickets in that area are auto assigned only if a matching location is found. For example, a request ticket is auto assigned if there is an eligible analyst at:

- The affected asset's location
- The affected customer's location

If the affected asset or customer has no specified location, the request is assigned to the default group and assignee. If these defaults are not defined, the request is left for manual assignment.

Follow these steps:

1. On the Auto Assignment tab of one of the following pages, click Update Locations.
   - Change Orders Detail
   - Issues Detail
   - Requests/Incidents/Problems, Areas Detail

   The Location Search window opens.
2. To filter the search, complete one or more of the search fields, or leave all fields blank to search for all locations, then click Search.
   The Locations Assigned Update window opens.

3. Use the arrow buttons to move available locations to or from the Locations Assigned list.

4. Click OK.

Assign Workshifts

You can constrain auto assignment by relating the request/incident/problem area to a workshift. The workshift determines the timeframe within which tickets are eligible for auto assignment. Tickets opened outside the hours of the workshift are assigned to the default group and analyst or left for manual assignment.

Follow these steps:

1. On the Auto Assignment tab of one of the following pages, click Update Workshifts.
   - Change Orders Detail
   - Issues Detail
   - Requests/Incidents/Problems, Areas Detail

   The Workshift Search window opens.

2. To filter the search, complete one or more of the search fields, or leave all fields blank to search for all workshifts, then click Search.
   The Workshifts Assigned Update window opens.

3. Use the arrow buttons to move available workshifts to or from the Workshifts Assigned list.

4. Click OK.

Define Behavior Template

A behavior template defines an action when a task changes status. For example, an email notification can be sent to a manager when the status of an approval task changes to Pending.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

The Create New Behavior Template page contains the following fields:

- **Status**
  Specifies the status of the template, such as Approve or Pending.

- **Active**
  Specifies if the template is active or inactive.

- **Description**
  Specifies a description of the template.

This page also contains the following tabs:

- **To Do**
  Identifies selected macros to run when the status change identified in the Status field takes place.

- **Transition Information**
  Identifies conditions that prevent the task from reaching the specified status, prior to the macros on the To Do tab run.

Note: All behaviors defined for a specific issue or change category are listed on the Workflow Task Template Detail window for that category and become part of any issue or change order that is assigned to that category.

Define Change and Issue Categories for Self-Service

You can use the Self-Service Include option to define which change and issue categories to include on tickets for self-service. You can also define different self-service symbols than the ones viewed by the analyst. When the ticket is saved, the self-service symbol appears in the Change (or Issue) Category field. If the ticket displays in the analyst interface, the normal symbol for the category appears.

Follow these steps:

1. On the Administration tab, select Service Desk, Change Orders (or Issues), Categories.
   The Category List page appears.

2. Select Edit In List.
   The top portion of the page displays the editable fields.

3. Select the desired category from the Symbol list.

4. Complete the following fields:

   - **Self-Service Include**
     Specifies whether this category is shown in the self-service interface.
     Default: Yes

   - **Self-Service Symbol**
     Specifies a unique identifier for this category in the self-service interface.

   - **Active**
     Specifies whether the category is active or inactive.

   The category is defined for self-service.

5. Click Save.
   The updated category appears in the Change (or Issue) Category List when you redisplay the list.

Change Category Fields

The following fields appear on the Create Change Category, Change Category Detail, and Update Change Category pages:

- **Symbol**
  (Required) Defines an identifier for the category. This is a required field.

- **Code**
  (Required) Defines the internal code for the category. This is a required field.

- **Type**
  Defines the level at which change orders are implemented within an organization.

- **Record Status**
  (Required) Indicates whether this database record is active or inactive. You can select a value from the drop-down list.

- **CAB**
  Specifies the group that is responsible for reviewing Requests for Changes (RFCs). The CAB provides multiple perspectives necessary to ensure proper decision making about implementing changes. The CAB can include members from the application team, development manager, component owner, QA, support, and any additional parties deemed necessary. You can enter the value directly or click the search icon to search for the group.

- **Organization**
  Identifies the company, division, or department that is associated with the change category. Enter a value directly or click the search icon to search for an organization.

- **Group**
  Identifies the group that is responsible for the record. Your system administrator defines groups of contacts that are responsible for different types of issues, requests, incidents, change orders, and so on. Any individual contact assigned to the group can handle the task once it is assigned to the group. Enter a value directly or click the search icon to search for a group.

- **Assignee**
  Identifies the person assigned to the record. Enter a value directly or click the search icon to search for a contact.

- **Service Type**
  Defines the level of support service received by the contact affected by the change order. For example, some users may have contracted for 24-hour support, while others might receive on-site training. Enter a value directly or click the search icon to select a defined service type.

- **Survey**
  Identifies the defined survey associated with this record. Enter a value directly or click the search icon to search for a survey.

- **Risk Survey**
  Indicates the defined risk for change orders associated with change categories.

- **Children Allowed**
  Allows change orders assigned to this category to have subordinate issues. Organizes issues into a hierarchy of parent-child relationships to divide large issues into smaller, more manageable issues.

- **Self-Service Include**
  Displays this category in the self-service interface.

- **Self-Service Symbol**
  Defines a unique identifier for this category in the self-service interface.

- **Description**
  Gives a detailed description of the record.

- **Last Modified Date**
  Displays when the record was last modified, in the time zone of the server. This field is read-only, and is filled automatically each time the record is updated.

- **Last Modified By**
  Displays the name of the contact who last updated this record. This field is read-only, and is filled automatically each time the record is updated.

- **Service Contract**
  Identifies the service contract name associated with this record.

Add Properties to Change Categories

Properties are characteristics or attributes of tickets that are affected by the area or category the ticket is assigned to. For example, when you assign a change order to a change category, the properties associated with that category are assigned to the change order automatically.

To add properties to a change order category

1. Click CA SDM, Change Orders, Categories on the Administration tab.
   The Change Category List page appears.

2. Select the category to which you want to add properties.
   The Change Category Detail page appears.

3. On the Properties tab, click Add Property.
   The Create New Property Template page appears.

4. Complete the fields as appropriate.

> **Note**: Properties that are defined without validation rules are presented as freeform text fields, which allow the user to enter any text string. To limit the property values to selections from a predefined set, you can specify validation rules.

5. Click Save.
   The Change Category Detail page lists the new property on the Properties tab.

Category Property Fields

The Properties pages allow you to define, view, and edit custom properties for an Area or Category.

The following values on the Properties pages are not self-explanatory:

- **Sequence**
  Defines the order in which properties appears on the Properties tab of the tickets assigned to this Area or Category. The property with the lowest sequence number is listed first.

- **Active**
  Specifies whether the property is active or inactive.

- **Value Required**
  Indicates whether a value must be entered for this property on tickets assigned to this Area or Category. If selected, the word Yes appears in the Required column when this property is listed on the Properties tab of a ticket.

- **Validation Rule**
  Indicates the name of a rule that has been defined to validate user-entered values for this property. Enter the validation rule name directly or click the search button to search for a validation rule.

- **Label**
  The name of the property as it appears on the Properties tab.

- **Examples**
  Examples of appropriate values for the property. For example, if a freeform text field is intended to contain information about a network type, this field might include LAN, WAN, and SAN as example values. These examples appear on the ticket to provide guidance for entering the actual property value.

Install Incident Tracking

This article contains the following topics:

Incident tracking lets analysts track an incident by selecting one or more flags for the incident. The information that analysts specify provides your organization with metrics about incidents for reports. For example, analysts can indicate that an incident was assigned incorrectly. When a large percentage of incorrectly assigned tickets appears in a report, your organization is aware that assignments must be adjusted.

For example, analysts can specify information to help your organization do the following:

- Improve SLA responsiveness and closure at lower levels within the support organization.

- Identify tickets that are incorrectly assigned.

- Indicate that a remote control tool was used to resolve the ticket.

You install the efficiency_tracking Options Manager option, so that analysts can use tracking options that appear on the Efficiency Tracking tab of incident detail pages.

Install Incident Tracking

You can install an option to let analysts track an incident by setting particular flags for the incident. The information that analysts specify provides your organization with metrics about incidents for reports. After you install the option, the tracking flags appear on the Efficiency Tracking tab of the Incident Detail pages.

Follow these steps:

1. On the Administration tab, browse to Options Manager, Request Mgr.
   The Options List appears.

2. Click efficiency_tracking.
   The efficiency_tracking Options Detail page appears with default values set.

3. Click Edit.
   The efficiency_tracking Options Update page appears with default values set, and you can edit the Description.

4. Click Install.
   The efficiency_tracking Options Detail page appears.

5. Click Close Window.
   Incident tracking is installed; however, the Efficiency Tracking tab does not appear on incident detail pages.

6. Restart CA SDM.
   The Efficiency Tracking tab appears on incident detail pages.

Related Ticket Activities

This article contains the following topics:

When an activity is generated for a CA SDM ticket, you can propagate the activity to one or more related tickets. For example, a Problem record created from an Incident can update the Incident record when the Problem is resolved. When the activity occurs, an activity log is generated for the related ticket that includes the following information:

- Related ticket activity type, for example, Update Status
- Contact name
- Parent ticket type and its reference number

- Activity log description, for example, status updated from Work in Progress to Open

Activity logs are propagated to related tickets based on the properties set within each activity notification. The attributes of the related tickets are not modified. The following relationships are propagated:

Problems propagate to all active Incidents.

- Change Orders propagate to all active Problems and Incidents.

As a system administrator, you can perform the following actions:

- Set up activity notifications to propagate related ticket activities.
- Configure a Related Ticket activity notification to notify the appropriate contacts when the activity is propagated to related tickets.

How to Define Activity Notifications for Related Tickets

You can propagate activity logs to related tickets based on the properties set in each activity notification. The attributes of the related tickets are not modified.

To define an activity notification for related ticket activities, do the following:

1. On the Administration tab, select Notifications, Activity Notifications.
2. Open the appropriate activity notification for editing.
3. On the detail page, click the Related Ticket Activity check box to mark it as active.
4. If you have multi-tenancy, perform the following:
   - Specify the appropriate tenant type from the Related Ticket Activity drop-down list.
   - Enter the name of the tenant in the tenant field, or click the search icon to search for a tenant.
5. (Optional) Update the default Notification Rule and specify contacts to receive notification.
6. Click Save, Close Window.
   The updated activity notification appears in the Activity Notification List when you redisplay the list.

How to Define Related Ticket Activity Notifications

You can change the default settings in the Related Ticket activity notification to notify the appropriate contacts when the activity logs are propagated to related tickets (requests/incidents /problems, change orders, and issues).

To define a related ticket activity notification, do the following:

1. Open the Related Tickets activity notification on the Activity Notification List page.

2. Click Edit and change one or more of the fields as appropriate on the detail page.

3. (Optional) Update the default Notification Rule for and specify contacts to receive notification.

4. Click Save, Close Window.
   The updated Related Ticket activity notification appears in the Activity Notification List when you redisplay the list.

Audit Log Use

CA SDM creates an audit log that records the following information:

- All changes to an issue (Issue)
- All changes to a request (Call_Req)
- All changes to a change order (Change_Request)
- All changes to a data partition (Domain) tables
- The login ID of the person associated with the change and an associated day/date/time stamp
- The before and after values of the update, insert, or delete
- The creation of contacts
- Creation and update activities to the nr object

Note: The audit log captures modifications to only the contact data partition field, but no other contact record updates.

The audit log feature is automatically installed, and you can enable it by installing two Audit Log options with the Options Manager: audit_ins and audit_upd. After you have installed these options, you can access the audit log on the Administration Tab by selecting Service Desk, Audit Log List. You can search the audit log list with a built-in search tool, and use it to facilitate report generation.

Priority Calculation

This article contains the following topics:

Priority calculation is a predefined set of values that automatically set Priority, Urgency, and Impact fields on problems and incidents. Priority calculation helps you manage incidents and problems for your business needs and IT capabilities. ITIL recommends that you prioritize tickets by using a data calculation that is based on Urgency and Impact values. Support organizations define this calculation

based on their unique processes, how this calculation determines Service Level Agreements (SLAs), and other key events in the system. This calculation can also include the criticality of the CI that is linked to the incident and problem. Prioritizing tickets effectively helps you accomplish the following:

- Allocate IT resources for tickets
- Better serve customers
- Reduce costs

The CA SDM solution for Priority Calculation includes the following components:

- A Priority Calculation Matrix based on the Urgency and Impact values
- Default values for Urgency and Impact
- Urgency and Impact adjustment options based on Affected Service, Open Date, Affected End User, and Incident or Problem Area
- A Capture Reason option for manually modifying Urgency or Impact
- An Enable for Templates option for creating a ticket from a Template

When you install CA SDM, a Default priority calculation automatically manages ticket values. You can modify the Default priority calculation settings, or create additional priority calculations to manage incidents or problems. In the priority calculation, you define the outcome based on business scenarios to make the level of importance and ticket handling more consistent. Users can override some settings, but they cannot set the Priority on the ticket because this value is data-driven. For multi-tenancy, you or the tenants can create additional priority calculations with specific settings for each tenant.

When an analyst opens an incident or problem, the system automatically uses an active priority calculation and ticket values to generate Priority, Urgency, and Impact settings. The settings are based on one or more of the following fields:

- Urgency
- Impact
- Affected End User
- Incident or problem Area
- Open Date
- Affected Service

Analysts can override Urgency and Impact values as necessary. Depending on how you configure Options Manager, employees can only override incident Urgency values when the *urgency_on_employee* option is installed. When the Capture Reason flag is enabled and users override Urgency or Impact values and click Save, the Escalate Detail page appears to let users describe a reason for the change.

All ticket priority calculations, manual overrides, and reason information appear in the New Activity Log. If no priority calculation adjustments occur, the system does not create an activity log entry.

Note: If you migrated from a previous version, priority calculation is disabled by default.

Priorities

Priority codes indicate the amount of attention a ticket should receive. Priority codes are used when defining automatic notification and external processing for specific types of situations. They are also used as a label in the scoreboard to prioritize tickets.

The predefined priority codes are:

1 = High priority

2 = Medium-high priority

3 = Medium priority

4 = Medium-low priority

5 = Low priority

None = No priority is assigned.

You can modify a priority code's symbol. For example, your site might decide not to use numbers at all and assign priority codes of low, medium, high, and so on.

You can modify a priority code's associated service type. For example, you could change the service type for priority code 1 from the default value of 04hr resolution to a custom service type of 02hr resolution.

Note: You can edit the predefined priority codes, but you cannot delete them or create new ones.

How Priority Calculation Manages Ticket Values

The system adjusts problem and incident values based on active priority calculation settings to assist Analysts in handling tickets more effectively. The following table summarizes how priority calculation changes fields based on the priority calculation and user actions for problems, incidents, web service, email, and the Text API:

Action	Automatic Field Changes	Description
User changes Affected Service	Impact Priority	The system evaluates the Service Impact value on the CI of type Service to calculate the new Impact value. The CIs of type Service are defined as CIs with their class defined in the Enterprise Service family. If the open date of the ticket is within the blackout window time frame, the system increments a new Impact value based on the Impact Increment field. The system only replaces the Impact value when the new value is greater than the initial Impact value.
User changes Incident Area	Urgency	The Urgency value changes only when the new value is greater than the default value.
User changes Incident Area *and* Affected End User	Urgency Priority	If the user sets the Incident Area field first, the Urgency value changes after the user sets the Affected End User. The priority calculation sets the Priority.
User changes Urgency *and* Impact	Priority Impact	The system evaluates the Service Impact value on the CI of type Service to calculate the new Impact value. If the open date of the ticket is within a time defined by a blackout window, the system increments a new Impact value based on the Impact Increment field. The system only replaces the Impact value when the new value is greater than the initial Impact value. If the Administrator sets Capture Reason, the user must provide a reason for the modification. If the user changes the Urgency or Impact values, these values remain the same throughout entire ticket creation or ticket update unless the user modifies them again. However, the system can update the overridden values for Urgency or Impact the next time the user updates the ticket. After the system adjusts Urgency and Impact, the priority calculation sets the Priority value.
User selects New Incident based on the Knowledge Document and system has overrides for Knowledge Documents (see page 1087 1087)	Impact Urgency	The system always uses the Knowledge Document or knowledge solution values irrespective of whether the values are greater than or lesser than the default priority calculation values. For example, if a priority calculation has an Impact value of 3-Single Group and Urgency value of 3-Quickly, and Knowledge Documents have an Impact value of 2-Multiple Groups and Urgency value of 4-Very Quickly, the system applies the values from the Knowledge Document to the incident. The priority value always derives from the priority calculation.
User accepts Knowledge Document as solution to problem or incident	Impact Urgency	The system uses the values from the Knowledge Document for Impact and Urgency. The system also uses the priority calculation to set the Priority value.
User derives incident from Knowledge Document by selecting New Incident	Impact Urgency Priority	The system uses the priority calculation values.

Action	Automatic Field Changes	Description
User derives incident from Knowledge Document without system overrides for Knowledge documents (see page 1087)	Impact Urgency Priority	The system uses the priority calculation values regardless of how the user created the incident for the Knowledge Document or knowledge solution.
Ticket accepts Knowledge Document as solution to problem or incident and the system does not override for knowledge documents	Impact Urgency Priority	The system uses values from problem or incident. The Priority value originates from the priority calculation.
Ticket that is in Read Only Mode accepts Knowledge Document as solution to the problem or incident and system overrides for Knowledge Documents	Impact Urgency Priority	The system uses the Impact and Urgency values from the Knowledge Document when the values are not empty. If the Impact/Urgency value in the Knowledge Document is empty the system uses values from the problem or incident. The Priority value originates from the priority calculation.
Ticket that is in Edit Mode accepts Knowledge Document as solution to the problem or incident and system overrides for knowledge documents.	Impact Urgency Priority	The system uses values from the problem or incident. The Priority value originates from the priority calculation.

Priority Calculation Generates Urgency Value After Saving Self-Service Tickets

By design, priority calculation generates Urgency values only after self-service users save incidents. Self-service users, such as VIP employees, employees, and anonymous users, can view the generated value after saving a ticket.

For self-service users, priority calculation uses the following settings and values to generate Urgency values:

- Urgency_On_Employee is set to Yes in Options Manager
- Override Urgency value is enabled in the active priority calculation for incidents
- *Web.cfg* Urgency settings such as AnonymousUrg for anonymous users, ESCEmpUrg for VIP employees, and EmpUrg for all other employees

- Area Urgency values
- Manual user overrides

The following table summarizes how priority calculation sets the Urgency value for self-service incidents:

Self-Service User Action	Urgency Value
The user saves an incident with the default Urgency and an empty Incident Area.	The ticket shows the default Urgency value from the *web.cfg*.
The user saves an incident after overriding the Urgency value.	Regardless of the Area Urgency, *web.cfg*, or priority calculation settings, the ticket shows the Urgency value that the user selected.
The user saves an incident after selecting an Incident Area. The Incident Area does not have a predefined Area Urgency value.	The ticket shows the default Urgency value from the *web.cfg*.
The user saves an incident after selecting an Incident Area that has a predefined Area Urgency value. The Override Urgency option is also enabled on the active priority calculation for incidents.	If the Area Urgency value is greater than the Urgency in the *web.cfg*, the ticket shows the Area Urgency value. However, the updated Urgency field is not visible while the user is creating or editing the ticket. When the user saves and reopens the incident, the updated Urgency value appears on the incident.
The user saves an incident after selecting an Incident Area that has a predefined Area Urgency value. However, the Override Urgency option is disabled on the active priority calculation for incidents.	The ticket shows an Urgency value from the *web.cfg*.
The user edits an existing incident that has an Incident Area with a predefined Area Urgency value.	The Urgency drop-down list shows the Area Urgency value and all applicable *web.cfg* values.

How to Set Priority Calculation

This article contains the following topics:

By default, ticket values such as priority are based on a priority calculation. You can find and adjust the initial values for Priority and Urgency in the web.cfg. The web.cfg has separate settings for various users such as guest, VIP-user, and employee.

Note: If you migrated from a previous version, priority calculation is disabled by default. Modified Incident and Problem Detail pages require additional configuration to operate properly.

To set priority calculation, do the following:

1. On the Administration tab, select Service Desk, Request/Incidents/Problems, Priority Calculation.
   The Priority Calculation List appears.

2. Right-click the default priority calculation and select Edit from the short-cut menu.
   The default Priority Calculation Detail page shows default settings for incident and problem tickets.

3. Review default priority calculation and adjust the values accordingly. When you set priority calculation values, consider the following issues for your working environment:

   - **Issue escalation** -- When tickets require escalation to a particular VIP, you can increase the value for Urgency.

   - **Critical CIs** -- For critical CIs, you can configure Service Impact for each CI.

   - **Critical Service Uptime** -- When CIs require high availability, add a blackout window.

   - **Blackout window** -- When CI-related tickets use a particular blackout window, you can increase the Service Impact value on the priority calculation.

4. Use the Manual Override setting to allow users to change tickets settings as necessary.

5. If you want a separate priority calculation to manage, problems or incidents, configure the ticket type (see page 1085).

6. Click Save.
   On the next new or updated ticket or Knowledge Document, the fields update according to the values in the active priority calculation.

7. Consider creating additional priority calculations for each ticket type. For multi-tenancy, create and activate additional priority calculations to manage tickets for each tenant.

Define a Priority Calculation

Priority calculation is a predefined set of values that automatically set Priority, Urgency, and Impact values on problems and incident tickets.

Note: If you migrated from a previous release, the priority calculation values must be enabled after the migration.

You can define a priority calculation to handle, incidents, problems, or both. However because two priority calculations cannot handle the same ticket type, you can review and update existing priority calculations before you create ones. For example, if you want to add a priority calculation to manage problem tickets, first clear the Problem field on the active priority calculation. Then, create a priority calculation to manage problem tickets.

If multi-tenancy is installed, you can use one public priority calculation that applies to all tenants or several tenant-specific priority calculations.

Follow these steps:

1. On the Administration tab, select Service Desk, Request/Incidents/Problems, Priority Calculation.
   The Priority Calculation List page appears.

2. Click Create New.
   The Create Priority Calculation page appears.

3. Complete the following fields as appropriate:

   - **Name**
     Identifies the priority calculation.

   - **Status**
     Specifies the ticket status for this priority calculation.

   - **Incidents**
     Specifies whether this priority calculation applies to incident ticket types.

   - **Problems**
     Specifies whether this priority calculation applies to problem ticket types.

   - **Spelling**
     Verifies the spelling of text in the Description field.

   - **Description**
     Specifies the purpose of the priority calculation.

4. Complete the priority calculation by setting the Priority value based on Impact and Urgency. For example, if the Urgency is 5-Immediate and the Impact affects the 1-Entire Organization, you can select the Priority value of 1 from the drop-down list.

5. Set the following Priority Calculation Options as appropriate:

   - **Impact Default**
     Specifies the initial Impact value to display when the user creates a ticket.

   - **Override Impact**
     Works with the Impact Increment field. Specifies whether the user can override the ticket Impact value with the Impact level specified in the attached Affected Service.

   - **Impact Increment**
     Works with the Override Impact field. Increments the Impact by the specified amount when the user overrides the Impact value. When the ticket uses a blackout window, the Impact value increments only when the open date is within the blackout window time frame. The Impact value can only raise to a maximum of 1-High. For example, if you set the value to 2 and the default Impact is 3-Medium, the user can only override the Impact on a ticket to 1-High.

   - **Urgency Default**
     Specifies the Urgency value to display when the user creates a ticket.

   - **Override Urgency**
     Specifies whether the user can override the ticket Urgency value with the Area Urgency level specified in Incident or Problem area.

   - **Urgency Increment**
     Works with the Override Urgency field. Increments the Urgency level by the specified amount when the affected end user sets the Escalate Urgency flag.

   - **Capture Reason**
     Specifies whether the user is required to enter the reason for changing the Urgency or Impact values. If the user changes the Urgency or Impact values, the Escalate Detail page appears while saving the ticket. The user is required to describe the reason for changing the Urgency or Impact values.

   - **Enable for Templates**
     Specifies whether to use the priority calculation for tickets that use templates.

6. Click Reset Matrix if necessary to restore the settings to the defaults.
   The default values reset.

7. Click Save.
   The Update Priority Detail page appears. On the next new or updated ticket or Knowledge Document, the fields update according to the values in the active priority calculation. If no priority calculation is active for a ticket type, the system clears the Priority, Urgency, and Impact fields.

Use Ticket Templates to Calculate Priority Values

If you want ticket templates to calculate priority, you configure the priority calculation with the *Enable for Templates* option. If you enable this option the Urgency and Impact values come from the template, but the priority field comes from priority calculation record. The priority value displays as read-only.

If you do not enable this option, the Urgency, Impact and Priority fields come from the template. You can edit the priority field and no priority calculation is done for the ticket until it is saved.

To use ticket templates to calculate priority values

1. On the Administration tab, select Service Desk, Requests/Incidents/Problems, Priority Calculation.
   The Priority Calculation List appears.

2. Select the priority calculation that you want to use for calculating priority with templates.
   You can also create a priority calculation to use ticket templates to calculate priority values.

3. Select *Enable for Templates* from the Priority Calculation Options list.

4. Click Save.
   The option is enabled.

Multiple Priority Calculations

You can set up more than one priority calculation. However, only one active priority calculation handles problems, or incidents, or both. For example, you can have an active priority calculation for problems, and another for incidents. You can also save several inactive priority calculations for future use.

Priority Calculation Assignment for Multi-Tenancy

You or your tenants can create tenant-specific priority calculations to manage incidents and problems. When you assign priority calculations for multi-tenancy, consider the following:

- When a priority calculation has no assigned tenant, it is considered public. The status of a public priority calculation is either Active or Inactive. A priority calculation is no longer considered public when it is assigned to a tenant.

- If a tenant has no priority calculation assignment, the Default priority calculation or another active public priority calculation automatically manages problems and incidents.

- A priority calculation manages problems and incidents for one tenant. However, a separate tenant-specific priority calculation can handle each ticket type. For example, Company X has one priority calculation to handle incidents and another to manage problems.

- When tenants create their own priority calculations while public priority calculations are active, the tenant-specific priority calculation applies only to tickets for the respective tenant.
  For example, if the Default priority calculation is active, Company X tenant can create a tenant-specific priority calculation named new_priority_calculation. The new_priority_calculation settings and configurations apply only to Company X incidents and problems.

- If the tenant inactivates a priority calculation, the system uses an active public priority calculation to manage tenant problems and incidents.
  For example, Company X inactivates the tenant-specific priority calculation while there is still an active Default priority calculation. Priority calculation remains enabled for Company X because the system uses the Default priority calculation to manage incidents and problems for Company X.

Note: Because tenants can delete their own priority calculation records, we recommend that you inactivate the public priority calculations that manage incidents and problems. Instead, you or the tenants can create tenant-specific priority calculations.

- When you disable multi-tenancy and there is more than one active priority calculation that manages tenants, leave *only one* priority calculation to manage incidents and problems. For example, you can inactivate all priority calculations except one to manage incidents and another to handle problems.

How to Assign a Tenant to a Priority Calculation

For multi-tenancy, you can assign a tenant to a priority calculation. First, you inactivate public priority calculations. Then, you assign the tenant to a priority calculation and activate it.

To assign a tenant to a priority calculation, do the following:

1. On the Administration tab, select Service Desk, Request/Incidents/Problems, Priority Calculation.
   The Priority Calculation List appears.

2. Edit each public priority calculation, such as Default. Set the status to Inactive and click Save.
   The system disables the public priority calculations.

3. For each tenant, create or edit a priority calculation with tenant-specific settings for Impact, Urgency, and Priority.
   The Create Priority Calculation or Update Priority Calculation page appears.

4. In the Name field, specify the tenant.

5. In the Status field, select Active.

6. Click Save.
   The system applies tenant-specific values for Impact, Urgency, and Priority on new incidents and problems.

Ticket Type Considerations for Priority Calculation

When you configure ticket types for a priority calculation, consider the following:

- The default priority calculation lets you manage both incident and problem ticket types.

- If you are migrating from a previous release, you enable the default priority calculation or create a priority calculation to manage problems and incidents.

- Although you can have many priority calculations, only one active priority calculation can handle a particular ticket type. For example, one active priority calculation can manage problems and another can manage incidents.

- If you want to create a priority calculation and an active priority calculation already handles a particular ticket type, you first disable the ticket type on the active priority calculation. For example, if you want a priority calculation to manage problems, you disable the problem ticket type on the active priority calculation and create an active priority calculation that manages problems.

Configure Ticket Types for a Priority Calculation

You can specify the ticket types that the priority calculation manages. When the priority calculation is active, it manages Priority, Impact, and Urgency values on new tickets.

To configure ticket types for a priority calculation

1. On the Administration tab, select Service Desk, Request/Incidents/Problems, Priority Calculation.
   The Priority Calculation List appears.

2. Right-click a priority calculation and select Edit.
   The Update Priority Calculation page appears.

3. Select or clear one or more of the following options:

   - **Incidents**
     Enables or disables the priority calculation to manage new incidents.

   - **Problems**
     Enables or disables this priority calculation to manage new problem tickets.

4. Click Save.
   CA SDM uses the settings in the priority calculation to manage ticket values for new incidents, problems or both.

Use Ticket Templates to Calculate Priority Values

If you want ticket templates to calculate priority, you configure the priority calculation with the *Enable for Templates* option. If you enable this option the Urgency and Impact values come from the template, but the priority field comes from priority calculation record. The priority value displays as read-only.

If you do not enable this option, the Urgency, Impact and Priority fields come from the template. You can edit the priority field and no priority calculation is done for the ticket until it is saved.

To use ticket templates to calculate priority values

1. On the Administration tab, select Service Desk, Requests/Incidents/Problems, Priority Calculation.
   The Priority Calculation List appears.

2. Select the priority calculation that you want to use for calculating priority with templates.
   You can also create a priority calculation to use ticket templates to calculate priority values.

3. Select *Enable for Templates* from the Priority Calculation Options list.

4. Click Save.
   The option is enabled.

Use Knowledge Documents to Calculate Priority Values

If you want knowledge documents to calculate priority, you can update the field mapping. After you configure the field mapping, the analyst can create incident or problem tickets from knowledge documents. The knowledge document calculates Impact and Urgency values on the tickets. If the Impact or Urgency value is missing, the values originate from the priority calculation.

Important! If you modify and save a ticket that already contains Impact and Urgency values calculated by a knowledge document, the priority calculation overrides the values set by Knowledge Management. The audit log displays these activities.

To use knowledge documents to calculate priority values

1. On the Administration tab, select Knowledge, Service Desk Integration.
2. Select Field Mapping.
   The Field Mapping page appears.
3. For Impact and Urgency, select the following check boxes as appropriate:
   - **Populate Empty Service Desk values**
     Specifies whether to use information from Knowledge Management to populate fields in issues or requests.
   - **Overwrite Service Desk values**
     Identifies the fields in issues or requests that correspond to fields listed in the Knowledge Management column.

   Note: When the Override Service Desk values field is not enabled but Populate Empty Service Desk values field is enabled for Impact and Urgency, the knowledge values for Impact and Urgency override the Incident values.
4. Click Save.
   Incidents and problems are created, using the Impact and Urgency values from the knowledge document to calculate the Priority value. If the values are missing, the ticket obtains the values from an active priority calculation. If no priority calculation is active for the ticket type, the system clears the Priority, Urgency, and Impact fields.

Manually Override the Impact Value

When you manually override the Impact value on a problem or incident, the active priority calculation that manages the ticket type automatically adjusts the Priority value.

To manually override the Impact value

1. Open the details page for the problem or incident you want to change.

2. Change the Impact value.
   If there is an active priority calculation that manages the ticket type, the Priority value automatically changes based on the settings in the priority calculation.

3. Save the incident.
   The Activity Log on the Incident Detail page reflects the Impact values changes.

Example: Manually override the Impact value on a new incident

1. Create an incident.
   By default, the Urgency value is 3-Quickly. The Impact value is 3-Single Group. The Priority value is 3.

2. Override the Impact value to 1-Entire Organization.
   The Priority value automatically changes based on the values in the active priority calculation that manages incidents.

3. Save the incident.
   The Activity Log on the Incident Detail page reflects the Impact value changes.

Manually Override the Urgency Value

When you manually override the Urgency value on a ticket, the active priority calculation that manages the ticket type automatically adjusts the Priority value.

To manually override the Urgency value

1. Open the details page for the incident you want to change.

2. Change the Urgency value.
   If there is an active priority calculation that manages the ticket type, the Priority value automatically changes based on the settings in the priority calculation.

3. Save the incident.
   The Activity Log on the Incident Detail page reflects the Urgency values changes.

Example: Manually Override the Urgency Value on a New Incident

1. Create an incident.
   By default, the Urgency value is 3-Quickly. The Impact value is 3-Single Group. The Priority value is 3.

2. Override the Urgency value to 5-Immediate.
   The Priority value automatically changes based on the values in the active priority calculation that manages incidents.

3. Save the incident.
   The Activity Log on the Incident Detail page reflects the change in the Urgency value.

Automatically Adjust Impact for a Problem or Incident

For Configuration Items defined with a family of Enterprise Service, you can automatically adjust the Impact value for problems or incidents. When you select the Problem or Incident Area and select an Affected Service, the impact adjusts according to the CI Service Impact settings for Enterprise Service CI's and the priority calculation.

To automatically adjust Impact for a Problem of Incident

1. Create a problem or incident for an Enterprise Service type CI.

2. Select an Affected Service.

3. Select a Problem or Incident Area.
   If there is an active priority calculation that manages the ticket type, the Impact value changes based on the Increment Impact value (used for Blackout Window impact assessment) in the priority calculation and the Service Impact value from the affected service.
   If you are using the default priority calculation, with a Service Impact for the Enterprise Service CI set to 1-Entire Organization, and the Problem or Incident is not opened within a Blackout Window the Impact value in the Problem or Incident is set to 1 and the Priority value on the ticket raises to a 2.

4. Save the ticket.
   The Activity Log on the Incident Detail page reflects the Impact value's changes.

Adjust Impact for a Problem or Incident Example

The following example shows you how to adjust impact for a Problem or Incident.

1. Create an Enterprise Service CI named CI-APC and set the class as one that comes under the family Enterprise Service.
   For example, you can set the class as Other Service, Business Services, or Infrastructure Service.

2. In the Service tab within the CI Detail page, set the Service Impact field to 2-Multiple Groups.

3. On the Service Desk tab, create an incident and set the Affected Service to CI-APC.

4. Save the ticket.
   The Impact field in the incident reflects the value from the Service Impact of the selected affected service (CI-APC). In this case, the Impact value is set to 2 -Multiple Groups.
   Note: If you are using the default priority calculation and the current ticket is created during a Blackout Window period then the Impact value increments by 1 and in the case above the Impact value is then set to 1-Entire organization.

Automatically Adjust Urgency for a Problem or Incident

For problems and incidents, you can automatically adjust Urgency and Priority by specifying an affected end user that requires Special Handling or by specifying a Problem/Incident Area that has an Area Urgency value.

When you assign special handling, with the Escalate Urgency turned on, for a contact or set an Area Urgency value for a Problem/Incident area, the Urgency value within the Problem/Incident automatically adjusts according to the values in the priority calculation and the Area Urgency value for the affected end user.

Follow these steps:

1. Create a problem or incident.

2. Select an Affected End user. For an elevated urgency, select an Affected End user that requires Special Handling that has the Escalate Urgency on.
   If there is an active priority calculation that manages the ticket type, the Urgency value changes based on the Urgency Increment value in the active priority calculation.

3. Select a Problem or Incident Area.
   If there is an active priority calculation that manages the ticket type, the Urgency value changes based on the Area Urgency value in the Problem/Incident Area definition.

4. Save the ticket.
   A confirmation message reminds you that the ticket requires special handling. The Activity Log on the Problem/Incident Detail page reflects the changes of the Urgency value.

Adjust Urgency for a Problem or Incident Example

The following example shows you how to adjust urgency for a Problem or Incident:

1. On the Administrator tab, create a contact named Non-VIP.

2. Create a special handling contact named VIP and set the Escalate Urgency value on.

3. Create an area named Test Area and specify Area Urgency as 2-Very Quickly.

4. On the Service Desk tab, create an incident.

5. For the Affected End User, select Non-VIP.

6. In the Incident Area, select Test Area and save the ticket.
   The Urgency field reflects the Area Urgency value from the Incident Area definition. In this case, the Urgency is set to 2-Very Quickly.

7. Change the Affected End User to VIP and save the ticket.
   If the default Priority Calculation matrix is being used, the Urgency value is incremented by 1 and is set to 1-Immediate. A confirmation message appears that reminds you that the ticket requires special handling. The Activity Log on the Incident Detail page reflects the Urgency value's changes.

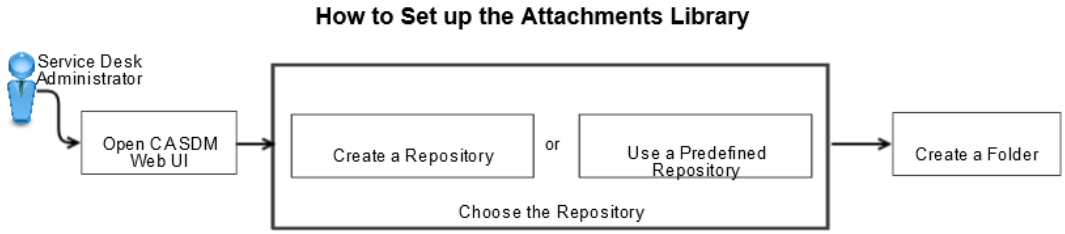
How to Set Up the Attachments Library

You can add different types of attachments to the various CA SDM entities. For example, a customer can attach a snapshot of an error to the incident. As an administrator, you set up the attachments library from where users can upload or download attachments.

Attachments can be classified, as follows:

- **Stored**: The web server uses the HTTP protocol to upload and store the stored attachments in a repository. When an analyst reviews a stored attachment, the file is retrieved from the repository and the file is displayed locally. Utilizing a web server for file storage allows storage and retrieval from the user interface.
- **Linked**: Stores only a link to the file in the database.

The following diagram shows how to set up an attachments library:



Follow these steps:

- Open CA SDM Web UI (see page 1091)
- Choose the Repository (see page 1091)
  - Setup a Repository on a Remote Computer (see page 1092)
  - Create a Repository (see page 1093)
  - Use a Predefined Repository (see page 1094)
  - Repository Fields (see page 1094)
    - Create UNC Credentials (see page 1096)
- Create a Folder (see page 1097)
  - Access Rights (see page 1097)
- Add a File to a Folder or Repository (see page 1098)

Open CA SDM Web UI

Log in to the web UI from the following servers, depending on your CA SDM configuration:

- Conventional: Primary or secondary servers
- Advanced availability: Application or background servers

Choose the Repository

The attachments are stored in repositories and you required to set up the repositories before users can work with attachments. You can add as many repositories to best suit your organization needs. For example, you might add separate repositories to store the file attachments and images. You can also add folders to your repositories to further organize your files, then upload files to the appropriate locations.

All client interfaces can access existing repositories for the upload and download of file attachments except as follows:

- Shared file repositories can be accessed only if the repository daemon is running on a computer that can access the shared file. The server name on the repository record (detail form) must be a Windows computer that has access to the share. A CA SDM repository daemon must also be running on the computer.

- Download of zip files is based on when they were uploaded. Attachments from earlier releases are downloaded without unzipping them. Unzip the file on the client computer; otherwise, attachments that are uploaded from a client interface, are also downloaded without unzipping them. That is, the server unzips the file before returning it, during a client download request.

The distributed architecture lets a site configure their repositories according to their needs. The servlet for a repository does not have to reside on the same server as the attached files. Sites can have a central servlet to access all their distributed repositories or have a dedicated servlet for each of their repository servers.

Consider the following setups when configuring repositories:

- **Repository server on a protected CA SDM server** -- Sites that designate a repository server on a protected CA SDM server behind the firewall do not need to expose the servlet on that computer. Rather, specify a servlet running on another CA SDM server or an unrestricted CA SDM server and still upload and download successfully to that repository. Depending on the network between the repository server and servlet server, some performance impact on the upload and download can occur. A good way to set up a remote repository is to install and configure another server with the repository on the remote server, and set the upload path to a local path. For more information, see the Setup a Repository on a Remote Computer (see page 1092) topic.

- **Servlet on the same server as the repository server** -- Sites that want the optimal performance for the attachment upload and download, and if the network performance is an issue and if very large files are being attached, should consider this setup. This approach requires exposing the Tomcat port (typically 8080) on the server and should be noted if the computer is behind a firewall.

CA SDM provides predefined repositories and also lets you create your own repositories to best suit your organization needs. Choose from the following options:

- Create a repository (see page 1093).

- Use a predefined repository (see page 1094).

Setup a Repository on a Remote Computer

By default, the repositories are located on the following server, depending on your CA SDM configuration:

- Conventional: Primary server

- Advanced availability: Background server

The default repositories use both the servlet and the repository daemon (rep_daemon) from these servers. To create a repository on a remote computer you must install and configure the following servers, depending on your CA SDM configuration:

- Conventional: Secondary server. The servlet runs on the primary server and the rep_daemon runs on the secondary server.
- Advanced availability: Background server. The servlet runs on the application server and the rep_daemon runs on the background server.

In the advanced availability configuration, the rep_daemon runs on all the servers, by default.

In the conventional configuration, the rep_daemon runs on the primary server, by default and you are required to verify that the rep_daemon runs on the secondary server for this setup.

(Conventional configuration only) Follow these steps:

1. Select **System**, **Configurations** on the **Administration** tab.
   The **Configuration List** page opens.
2. Select the configuration for the secondary server.
   The **Configuration Detail** page opens.
3. Click **Additional Processes**.
   The **Additional Process List** is displayed.
4. Click **Add Process**.
5. Select **Repository Deamon** as the **Process**.
6. Click **Save**.
   The repository is set up on the secondary server.

Create a Repository

Depending upon your organization needs, you can have one large repository or several small ones. Moving or combining repositories is simple because all the attributes about a repository are defined in the repository record.

Follow these steps:

1. Select **Attachments Library**, **Repositories** on the **Administration** tab.
   The **Repositories** page opens.
2. Click **Create New**.
   The **Create New Repository** page opens.

   Note: If you are the service provider, select the appropriate tenant from the **Create New Repository** page. The public (shared) option makes the repository available for all tenants.

3. Complete the Repository Fields (see page 1094) as appropriate.

4. Click **Save**.
   The repository is created.

> **Note:** To delete a repository, select Attachments Library, Repositories from the Administration tab, r ight-click on the repository, and select Delete. When you delete a repository, all files and folders within a repository are deleted as well.

Use a Predefined Repository

You can use a predefined repository (Service Desk or Knowledge or Images).You can edit a repository to best suit your organization needs.

Follow these steps:

1. Select **Attachments Library**, **Repositories** on the **Administration** tab.
   The **Repositories List** page opens.

2. Right-click the repository that you want to edit and select **Edit**.
   The **Update Repository** page opens.

3. Edit the fields as appropriate. For more information, see the Repository Fields topic.

4. Click **Save**.
   The repository definition is saved.

Repository Fields

The following fields are used to edit or create a repository.

Name

Specifies the name to uniquely identify the repository. For example, Incident Images repository can store all the images that are related to an incident.

- **Repository Type**
  Indicates the type of content that is stored in the repository. For example, to store image attachments, select **Images**.

- **Default**
  Indicates whether this is the default repository for the specified repository type. For example, when the user is creating the incident and user wants to attach an attachment to the incident, the default repository is displayed for the selection. You can only set one repository to default.

- **File Limit Size (KB)**
  Specifies the maximum size of file, in kilobytes, that a user can upload to the repository.

- **Upload Path**
  Specifies the full root directory path or the UNC path where files uploaded to the repository reside.

- **UNC Credentials**
  Specifies the credentials to access the UNC path specified in the **Upload Path** field. Click **UNC Credentials** to open the **Credentials Search** page.

  - If you have already created the credentials to access the specified UNC path, search using the fields and select the credentials.

  - If you want to create the credentials, click **Create New**. For more information about creating credentials, see the Create UNC Credentials (see page 1096) topic.

- **Background Services**

  Note: The options for background server services appears only in Advanced Availability configuration.

  Specifies the background server services for the servlet path and rep_daemon.

  - **None**
    Indicates that the background server is not used for the servlet path or for the rep_daemon. If you select this option, enter the values for **Servlet Server** and the **Repository Server** fields.

  - **Servlet Only**
    Indicates that servlet is hosted on the background server. If you select this option, the **Servlet Server** field is auto-populated with **Background Server** value. Enter the value for the **Repository Server** field. If the background server shuts down and if the standby server is promoted as the new background server, the **Servlet Server** field is populated with the new background server value.

  - **Daemon Only**
    Indicates that the rep_daemon is running on the background server. If you select this option, the **Repository Server** field is auto-populated with **Background Server** value. Enter the value for the **Servlet Server** field. If the background server shuts down and if the standby server is promoted as the new background server, the **Repository Server** field is populated with the new background server value.

  - **Servlet and Daemon**
    Indicates that background server is used for the servlet path and the rep_daemon. If you select this option, **Servlet Server** and **Repository Server** fields are auto-populated with the **Background Server** value. If the background server shuts down and if the standby server is promoted as the new background server, these fields are populated with the new background server value.

- **Servlet Server**
  Specifies the server where the servlet is running.

- **Repository Server**
  Specifies the server where the rep_daemon is up and running.

- **Archive Type**
  The archive and purge action to be taken on the contents of the repository.

- **None**
  No archive and purge process is performed.

- **Archive and Purge**
  The historic records are written to the file specified in the archive field and purged from the database.

- **Purge Only**
  The historic records are purged from the database, but are not written to the archive file.

- **Archive Path**
  Specifies the directory path or the UNC path to which files in the repository are moved during the archive process.

- **UNC Credentials**
  Specifies the credentials to access the UNC path. Click **UNC Credentials** to open the **Credentials Search** page.

  - If you have already created the credentials to access the specified UNC path, search using the fields and select the credentials.

  - If you want to create the credentials, click **Create New**. For more information, see Create UNC Credentials (see page 1096).

- **Prohibited File Types**
  The file extensions that users may not upload to the repository.

  Note: If the value in this field begins with an exclamation point (!), these file types are allowed in the current repository. For example, a value of jpg,gif in the list denotes that files with .jpg and .gif extensions are prohibited in the repository. However, a value of !jpg, gif denotes that only files with .jpg and .gif extensions are allowed in the repository.

Create UNC Credentials

You create the UNC credentials to allow users to access shared resources from the CA SDM servers using UNC path.

Important! The UNC component does not work when the CA SDM server is in the domain and the shared location is in the WORKGROUP. The UNC credentials that you use, must exist on the CA SDM server.

Follow these steps:

1. Click the UNC Credentials in the General Setting page or select Security and Role Management, UNC Credentials on the Administration tab.
   The Credentials List page opens.

2. Click Create New.
   The Create New Credentials page opens.

3. Complete the following fields as appropriate:

   - **Symbol**
     Specifies the unique identifier to identify the credentials during a search easily.

   - **Userid**
     Specifies the username to access the UNC path. The user can be a local or domain Windows user having access to the Service Desk server.

   - **Password**
     Specifies the password to access the UNC path.

   - **Active**
     Specifies if the UNC credentials are active or inactive. The inactive credentials cannot be used.

4. Click Save.
   The UNC credentials are created.

Create a Folder

Folders are used to organize the documents in repositories. For example, you can create a folder Error Images under the Images repository. This folder can contain all the snapshots of errors messages that the user has encountered.You cannot create a folder for the Service Desk Attachments repository type.

Follow these steps:

1. Select **Attachments Library**, **Repositories** on the **Administration** tab.
   The **Repositories List** page opens.

2. Right-click the repository where you want to create the folder and select **Add Folder**.
   The **Create New Folder** page opens.

3. Enter the name of the folder and a description of its contents.

4. Select the **Permissions** tab and specify the appropriate access rights (see page 1097).

5. Click **Save**.
   The folder is created.

Access Rights

You can add the following access rights to the folder in the repository:

- **Inherit from Parent**
  Indicates that this folder has the same permission settings as its parent folder. This option is only displayed for sub-folders.

- **Control by Group**
  Indicated the read or write access on this folder for specified groups. This option appears for all folders and sub-folders.

  - **Grant Write Permission to Everyone**
    Indicates that all users have write access to the folder.

  - **Grant Read Permission to Everyone**
    Indicates that all users have read access to the folder. Read permission indicates that you can view the folder, but you cannot edit, delete, or store files in it. Users with administrative rights can edit a folder even if their associated permission group cannot. If a user belongs to multiple permission groups with varying levels of access to the document, the user gets the highest available access level (for example, if one group has read-only access and the other write access, the user gets write access).

    Note: The **Grant Read Permission to Everyone** check box is automatically selected if you select the **Grant Write Permission to Everyone** check box.

  - **Available Groups**
    Displays all the groups. You can choose the groups from this list. For example, select a group and click > for **Groups with Write Permission** to provide read and write access to this folder for all the users in that group. Use **Show Filter** to specify criteria and filter the groups.

Add a File to a Folder or Repository

A knowledge administrator or a knowledge analyst can add a file to a folder or a repository. Ensure that you have an attachment library in place before proceeding.

Follow these steps:

1. Select **Attachments Library**, **Repositories** on the **Administration** tab.
   The **Repositories List** page opens.

2. Expand the repository, right-click the folder where you want to add the file, and select **Add File**.
   The **Add File** page opens.

3. Click **Browse** to navigate to the desired file and select it.

4. Enter a name for identifying the file, and a description, if necessary.

5. Click **Upload**.
   The file is uploaded to the folder of the repository.

Service Level Agreements (SLA)

This article contains the topics:

- How to Create Service Targets (see page 1111)
- Service Contracts (see page 1117)

A service level agreement (SLA) or service type is an agreement between a service desk and its customers and usually describes the level of service to be provided by the service desk. If this level of service is not provided, the service desk can be penalized. For example, a service desk that operates on a “pay per service” basis may not receive full payment for service that does not meet an agreed upon level of service. Thus, most service desks view service level agreements very seriously and make every effort to meet the type of service specified in these agreements.

In addition, most service desks keep meticulous records when service level agreements are met or violated. The service types defined with CA SDM are designed to help the service desk personnel meet their service level agreements and keep the records they need to verify that their service level agreements have been met.

How to Configure SLAs

In CA SDM, the SLA or service type describes the level of service that the service desk analyst provides to the customer. To track your enterprise commitments and schedules (as they relate to specific tickets), events are attached to service types. Events are used to define the condition under which the service type is violated and the actions to be taken after the violation. Each event has three generic behavior characteristics: conditions, actions on true, and actions on false.

- Condition identifies the measurable state of a ticket.
- Action identifies the processes that occur automatically when the condition is true or false after a specified amount of time.

Example: As a system administrator, you want to set up an SLA of 24-hours for a hardware request, failing which an email notification is sent to the Customer Support Manager and the analyst. This example is used throughout the scenario to explain how the email notification is configured for an SLA.

The following diagram shows how to configure the 24 hours. The SLA which sends an email notification, upon violation:

Follow these steps:

1. Open the CA SDM Web UI (see page).
2. Verify the Prerequisites (see page 1100).
3. Create a Macro (see page 1103).
4. Create an Event (see page 1108).
5. Create a Service Type (see page).
6. Attach the Service Type to an Object (see page).

Open CA SDM Web UI

Log in to the web UI from the following servers, depending on your CA SDM configuration:

- Conventional: Primary or secondary servers
- Advanced availability: Application or background servers

Verify the Prerequisites

Before you configure the service level agreement, ensure that you have completed the following steps:

- Installed the SLA options (see page 1100) which are necessary for your organization needs.
- Verified the Notification Method for the Recipient (see page 846)
- Created a Message Template (see page 848), if you want send an email notification upon an SLA violation and if you do not want to use a predefined message.

SLA Options

Depending on your organization needs, install the SLA options that you require to set up the SLA.

For example, in "classic" SLA processing (enabled if the classic_sla_processing option is installed in Options Manager) only one service type can apply to a ticket at any given time. When different attributes on a ticket have different service types associated with them, the higher ranked service type is used. The rank of a service type is defined when the service type is created, with the highest ranking being 1, the next being 2, and so on. For example, assume that the issue has a service type of 12-hour resolution (ranking 2), was assigned a priority code of 1, which has a service type of 4-hour resolution (ranking 1). The higher ranked service type determines the service behavior for the associated issue. In this example, 4-hour resolution is ranked higher than 12-hour resolution, so the 4-hour resolution service type is applied to the issue.

The following options can be installed from the Options Manager:

Option	Description
change_allow_sla_downgrade	Alters the behavior of the chg_sla option by allowing the system to automatically downgrade a change order's Service Type. The chg_sla option selects the best Service Type from among several change order attributes, but cannot replace the change order's current Service Type with one of lesser rank. If this option is installed, the Service Types for all affected attributes are evaluated whenever one of the attributes changes. The change order's Service Type is set to highest ranked Type found, even if the new Service Type is lesser in rank to the change order's current Service Type. The Service Type with the smallest Rank value is considered the best service. If all the Service Types considered are equal in Rank (including Service Types with empty Rank values), the Service Type created first in the database is selected. The chg_sla option must be installed for this option to function correctly. You can install similar option for issue, and request.
ttv_enabled	Runs the Time to Violation daemon, which monitors the SLAs for all open tickets and tasks. This process does not set the SLA violation, but records the date the ticket or task is violated in its current state. This projection is updated when the ticket or task is updated. This option must be installed in order for the other Time to Violation options to function correctly. **Important!** This option does not require you to install the classic_sla_processing option.

set_sl a_evt _ope n_dat e	Uses the open date/time value of a change order, issue, or request as the start date/time of attached events. The attached events are triggered as soon as the ticket is saved.

Verify the Notification Method for the Recipient

Ensure that the contact to whom you want to send the notification, is assigned to that particular notification method.

Follow these steps:

1. Select Security and Role Management, Contacts on the Administration tab.
   The Contact Search page opens.

2. Search for the contact using the filter and select the contact that you want to notify from the search result.
   The contact detail page opens.

3. Select Notification on the Contact Details tab.

4. Verify the notification method. Based on your notification priority, choose the required option. For example, you want to send an email notification for any emergency notification. Select the Email option in the Emergency field.

5. To change the notification method, click Edit, change the option, and click Save.
   The notification method for the contact is verified.

Create Message Templates

Create a message template that contains the values to use for the notification message. When you send multiple notification messages, you can use the message templates to simplify your workload.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. Select Notifications, Message Templates from the Administration tab.
   The Message Template List page opens.

2. Click Create New.
   The Create New Message Template page opens.

3. Complete the fields as appropriate.

   - **Symbol**
     Defines a unique identifier for this message template.

- **Object Type**
  Specifies the object type associated with this template. For example, select Request/ Incident/ Problem for any notification related to a ticket.

- **Record Status**
  Specifies the status of the template as either active or inactive. Set the status to Active to use the message template.

- **Auto Notification**
  Specifies to send the notification associated with this template automatically, when the activity occurs. For example, you set up an initial notification, set up the objects to notify, and set up the message template, but you are not ready to turn on the notifications. In this case, you do not select Auto Notification. When you are ready to start automatic notifications, you select the check box. The notification becomes active and occurs as defined.

- **Notify Level**
  Indicates the relative importance of sending this notification. For example, select Emergency if you want to send the email notification to the contact immediately when the associated activity occurs.

- **Notification Message Title**
  Specifies the summary title of the message. You can use variables to insert the incident number in the message title. For example, @{call_req_id.type.sym} @{call_req_id. ref_num} @{type.sym}.

- **Notification Message Body**
  Specifies the content of the message. You can use variables to insert the analyst name, end-user name, and description into the message. For example,

```
@{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}.

Assigned to: @{call_req_id.assignee.combo_name}

Customer: @{call_req_id.customer.combo_name}

Description: @{call_req_id.description}


Click on the following URL to view:

@{call_req_id.web_url}
```

  You can use the ARTIFACT keyword to specify how artifacts are handled in outbound messages, message templates, notifications, and auto-replies. The ARTIFACT keyword uses the following values:

  - **NONE** -- Specifies no validation of artifacts. This value is the same as not using the keyword.

  - **PROTECTED** -- Validates a ticket against the hash for confirmation. If confirmation fails, the artifact is considered invalid and filtering fails when filtering searching for an artifact ({{object_id}}).

- **SECURE** -- Decrypts the ticket number. If the value is not a valid password, the artifact is considered invalid and filtering fails when filtering is searching for an artifact ({{object_id}}).

- **HTML Message**
  Specifies the HTML message that is displayed to the recipient. If the recipient receives the message on an external device, such as a cell phone or PDA, the message displays in plain text only. Click Edit HTML Message to open the HTML Editor.

- **Quick View**
  Displays the message as it appears to the recipient.

- **HTML Source**
  Displays the message in the HTML source code.

4. Click Save.
   The message template is created.

Create a Macro

Macros are small scripts that define either conditions or actions. When Events or Behaviors execute, they can execute one or more Action macros. Before the macros are executed, you can use a conditional macro to determine which set of Action macros to execute.

You can use macros in the following areas:

- Events
- Behavior templates
- Activity Notifications

CA SDM includes several macros. Users can create their own macros too.

Note: Customers cannot add Action or Condition macros but can create simple macros with site-defined conditions. The Site-defined conditions are noncomplex macros that are created from GUI dialogs; they are not replacements for condition-type macros.

For each macro, you specify the object type that you want the macro to use. If you create a site-defined conditional to verify a Requests value, you set the type to Request. CA SDM displays only those object type macros that match the ones on the Events or Behaviors.

Create a macro. Use this macro to add actions to objects, check for certain characteristics, or conditions.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. Select **Events and Macros**, **Macros** on the **Administration** tab.
2. Click **Create New**.
3. Complete the fields as follows:
   - **Symbol**
     Enter a descriptive identifier for the macro.
   - **Macro Type**
     Select the type for this macro. The selected macro type controls the remaining data that is supplied.

     Note: The **Execute CA IT PAM Action** selection is only available when CA Process Automation Workflow is configured with CA SDM.
   - **Object Type**
     Select the type of object on which the macro can be run.
4. Click **Continue**.
   The page fills in with the remaining data.

Attach Event Macro

This macro type attaches an event object to a change order, issue, or request.

Example: Use Macros in the Behavior of Category or Area

You can also use macros in the Behavior for Issue and Change categories, and also for the Request/ Incident/ Problem areas. On a Category/ Area detail, select the Workflow tab, Workflow status, Workflow detail. Click Behavior and specify a Conditional-type macro. The macro is executed when a user tries to change the task status value to a new or different value. If the condition is set to false, updating the task status is not allowed.

Note: Use an Attach Event macro to attach an event to a workflow task.

Follow these steps:

1. Type the event name directly in the **Event** field, or click the search icon to select the desired event.
2. Click **Save**.
   The attach event macro is created.

Execute Remote Reference Macro

This type of macro launches an external program on the server.

Follow these steps:

1. Complete the following fields:

   - **Remote Reference**
     The name of the remote reference to the external program you want the macro to launch. Type the remote reference name directly into this field, or click the search icon to select the remote reference.

   - **Parameters to Command**
     Additional parameters required for running the command.

2. Click **Save**.
   The execute remote reference macro is created.

Create Multiple Notification Macro

This macro type lets you send a notification to one or more contacts. You can specify the message to send, the recipients of the message, and the urgency level.

Multiple Notification

The message body of the multiple notification points directly to the table of the object selected. Therefore, when referencing fields on the object table, (CR (Call_Req) for example,) you can reference the field attribute name. If you want to specify the description information of the Call Request ticket, enter the following command:

```
Description: @{description}
```

A QREL (Query Relation) is a relation which contains a list of objects. The list of objects are by an SQL type WHERE clause. You can add the QREL to the description of a multiple notification macro. To use the QREL in the act_log QREL <-- alg, enter the following command in a notification macro:

```
@{act_log.0.description}
```

You can use replacement variables to make notification messages more relevant and dynamic. These replacement variables take the form of @{attribute_path_here} where attribute_path_here is an attribute of some CA SDM object. When the notification is sent, the variable is replaced with the attribute value specified.
A notification (from an activity log or a multiple notification) always has some base context (a ticket or a workflow task). On multiple notification, the Notification macro type field specifies the base object. You use the @{} syntax to reference any attribute on that object.

Example: A Multiple Notification of type Request references any attribute in the 'cr' (Call_Req) object. To include the Request description, specify @{description} (dot-notation is used to follow references to other objects). For example, to include the Request assignee last name: @{assignee. last_name}.

Follow these steps:

1. Type the template name directly in the **Message Template** field, or click the search icon to select the desired template. This template is used to create the notification message.

2. Click **Save**.

3. Choose the appropriate contacts to notify from the following tabs:

   Note: Use the **Update Contacts** button that appears on each tab to search for and select more contacts to notify.

   - **Object Contacts**
     The available organizations, vendors, and configuration items for the selected Object type. For example, you can select Affected End User or Affected End User's Org to notify.

   - **Contacts**
     The individuals who are added to the notification macro, regardless of their association with the ticket.

   - **Contact Types**
     The users who are defined within the notification macro with the same classification, such as analyst or customer.

4. Click **Save**.
   The multiple notification macro is created.

Create a Site-Defined Condition Macro

This type of macro evaluates true and false conditional statements, and can be created by administrators to provide specific behaviors to individual sites.

Site-Defined Condition
The Conditional macro is made up of one or more *atomic* conditions. Each atom tests the value of a single attribute. The Conditional macro uses two atoms, one for Assignee and one for Category. The individual atoms in the Conditional Macro event are connected with a Boolean operator 'AND' or 'OR'. The Conditional Macro Detail shows a list of Atoms, which is read from left to right as follows:

Attribute	Operator	Value	Logical	Translation
Assignee	Equals	Jones	AND	The assignee is Jones and…
Cost	Less than	600	OR	Cost is an integer value less than 600 or…
Group	Empty/NULL		AND	The Group field is blank.

Note: The Logical connectors (AND, OR) connect two atoms. When there are two atoms, Atom A and Atom B, the atom A connector connects the atom. Atom B connector is not used.

Follow these steps:

1. Complete the following fields:
   - **If All Conditions Succeed Return**
     Select the value you want to return if all conditions succeed. Valid values are True or False.
   - **Record Status**
     Select whether the macro is Active or Inactive.
2. Click **Save**.
3. Click **Add Condition** on the **Conditions** tab.
   The **Create New Atomic Condition** page opens.
4. Fill in the following fields as appropriate:
   - **Sequence**
     The order in which the condition is evaluated within the site-defined condition.
   - **Select an Attribute**
     The attribute to be evaluated. Enter the attribute name directly in this field or click the search icon to select the desired attribute.
   - **Choose Operator**
     Select the conditional operator to use in the evaluation. Valid values are: Equals, Does Not Equal, Greater Than, Less Than, Empty/Null, Not Empty/Null.
   - **Select Attribute or Data Value**
     Choose either Attribute or Data Value to be evaluated.
   - **Attribute Value/Data Value**
     The value to be evaluated. Enter the attribute or data value directly into the field, or click the search icon to select the desired value.
5. Click **Save**.
6. Repeat this process until all the desired conditions have been created.
   The site-defined macro is created.

Execute CA IT PAM Action Macro

You can create a macro to initiate a CA Process Automation process. This process definition can be associated with any CA SDM ticket type. The change category, issues category, or request/incident /problem area the ticket is assigned to determines the process definition that is applied to the individual tickets. If a CA Process Automation workflow has been attached to the selected category, the workflow is automatically attached and initiated when the ticket is saved.

Complete the macro description, record status, and the **CA IT PAM** start form and click **Save**.

Create an Event

You can configure events that are attached to objects to execute configured actions. Events are procedures that execute after a certain amount of time has elapsed. For example, an event sends a message to a service desk analyst if a "priority 1" issue is not received within an hour. Other parts of the system use events, for example, Service Types.

You can define events for Requests, incidents, problems, change orders, issues, contacts, configuration items, and global and specific tenants. CA SDM schedules the events execution time that is based on the delay time and workshift.

Create an event and attach a macro to this event. This event is executed after certain time is elapsed. If any macro is attached, an action is performed.

1. Select Events and Macros , Events on the Administration tab.
2. Click Create New.
3. Complete the event fields (see page 1108) and the configuration information fields (see page 1108).
4. Click Save.
5. To add the macro to this event, complete the action information fields (http://wiki.ca.com#actioninformationfields).

   The new event is saved.

Event Fields

- **Object Type**
  Indicates if the event is attached to an issue, request, change order, workflow task, knowledge document, knowledge report card, assistance session, or managed survey.
  This field can only be edited when creating an event. This field is read-only when you want to update the event.
- **Record Status**
  Indicates whether the event is active or inactive. Only active events can be used.

Configuration Information Fields

Complete the following configuration information fields:

- **Delay Time**
  The time after which the event is triggered.
- **Repeat Delay Time**
  The interval of time after which you want the event to be triggered again.
- **Allow Time Resetting**
  Indicates that the desk analyst can change the **Delay Time**. Select this option to use an event as a Service Type event.

- **Work Shift**
  The dates, days, and hours when the service type is in effect.

- **On Done Event Flag**
  The action that is taken once the event is complete.

  - **Repeat Event**
    The event at the specified time interval until the issue is closed.

  - **Save History**
    Records the history of activities that are taken on the event.

  - **No History**
    Do not record any history of the event. The event does not appear in the **Event History** window.

- **Condition**
  Displays the macro (if associated with the event) indicating the condition that is checked for by the event.

- **Text**
  Defines the event configuration. For some action macros, this field is used for a specific purpose. For example, the **Transfer to Event Contact** action macro contains the User ID of the person to whom the ticket can be transferred.

Action Information Fields

Select the actions to be associated with the event as follows:

1. Click the **Action Information** tab.

2. Select one or both of the Set SLA Violation for Actions on True/False Macro check boxes. Selecting these check boxes logs a Service Level Agreement (SLA) violation when a true or false condition is encountered for the event.

   Note: Specify appropriate macros for true or false condition under the action list to log the SLA violations.

3. Click **Update Actions on True**.
   The **Macro Search** page opens.

4. Search for the macros to be performed if the event condition is true.

5. Select the desired macros from the list on the left, and click More (>>).
   The selected macros are added to the list on the right.

6. When all desired macros are in the list on the right, click **OK**.
   The selected macros appear in the **Actions on True Macro List**.

7. Click **Update Actions on False**, and repeat the previous procedure to select the macros to be performed if the event condition is false.

Create a Service Type

You can create a service type that suits your requirements. You can also modify a predefined service type.

Follow these steps:

1. Select **Service Desk**, **Service Types** on the **Administration** tab.
   The **Service Type List** page opens.

2. Click **Create New**.

   The **Create New Service Type** page opens.

3. If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

4. Complete the following fields, as appropriate:

   - **Symbol**
     Defines a unique identifier for the service type. In this example, you assign the symbol as 24_hr_resolution.

   - **Ranking**
     Defines a ranking for the service type. In this example, the hardware request ticket may be associated with multiple service types. The ranking value determines the applicable service type. The service type with low ranking has the highest priority.
     Enter 1.

   - **Workshift**
     Specifies the dates, days, and hours when the service type is in effect. The following rules apply to workshifts:

     - If you apply a workshift to a service type, stop and restart the service for the workshift to take effect immediately.

     - If a workshift for a service type has been specified, but not for an event, the service type workshift is in effect.

     - If a workshift for an event has been specified, but not for a service type, the service type workshift is ignored.

     - If a workshift for the event and service type have been specified, the service type workshift is ignored.

   - **Timezone**
     Specifies the time zone for the service type. This time zone is used for triggering events in the system if the **Use End User's Time Zone** option is not selected.

- **Use End User's Timezone**
  Specifies the timezone of the affected end user to trigger the events.

- **Violation Cost**
  Specifies the cost that is incurred if the service type time limit is violated.

5. Click **Save**.
   The service type is saved.

6. To attach a service type event, select the appropriate tab (Requests, Change Orders, Change Order Tasks, Issues, or Issue Tasks) and click **Add Service Type Event**.
   The **Create New Service Type Event** page opens.

7. Click **Event**.
   The **Event List page** opens.

8. Select one of the existing events from the list.
   The selected or created event is displayed in the **Event** field.

9. Click **Continue**.
   The service type detail page is displayed with the attached event.

Attach the Service Type to an Object

Service types can be associated with various objects such as contacts, organizations, categories, priority codes. According to the example, you attach the service type to the Incident Area, which is Hardware.

Follow these steps:

1. Open the related ticket for which you want to assign an SLA.

2. Click **Hardware** from the **Incident Area** field.
   The **Hardware Update Request/Incident/Problem Area** page opens.

3. Click **Edit**.

4. Click **Service Type**.
   The **Service Type List** page opens.

5. Search for 24_hr_resolution service type that you have created.

6. Click 24_hr_resolution from the search result.
   The **Hardware Update Request/ Incident/ Problem Area** page opens with the updated service type.

7. Click **Save**.
   The service type is attached to the Hardware incident area.

How to Create Service Targets

This article contains the following topics:

- Link a Service Target Template to a Service Type (see page 1114)
- View Ticket Counters and Timers for Service Targets (see page 1114)
- View Service Target Status (see page 1116)

To minimize the SLA violations, you can create a set of service target templates to measure each stage of ticket resolution. Like Service Types, each service target contains a condition and estimate of completion time. However, service targets do not provide an action mechanism.

During the ticket creation, a Service Type assigns one or more service targets to track each stage of the ticket resolution. Each time the ticket changes, the active service targets evaluate the condition. If the condition is met, the ticket and activity log show the actual completion time. When the time exceeds the estimated time, the ticket displays the amount of time by which the target was missed.

Service targets let you do the following actions:

- Verify that tickets of the same Service Type follow the same service targets.
- Monitor whether tickets are closed within the required time frames.
- View information such as the remaining number of minutes before a service target completes.

When creating service target templates, consider the following points:

- Consider the required outcome for meeting the service target. Use an existing Condition or Site-Defined Condition Macro to evaluate ticket data. If necessary, modify or write a new macro to manage the service target.
- Calculate the projected violation and penalty costs based on the SLA agreements.
- Assign at least one service target template to a Service Type.

Follow these steps:

1. Create a service target template (see page 1112) to manage requests, incidents, problems, change orders, or issues.
2. Link the service target template to a Service Type (see page 1114).
3. Assign the service target template detail to a ticket category such as request, incident, problem, change order, or issue tickets.
   At the time of ticket creation, the appropriate template automatically attaches to the ticket based on the Service Type. Each time a user creates a ticket, the status of the service target automatically displays in the Service Type tab.

Create a Service Target Template

You can create a service target template to measure service targets for requests, incidents, problems, issues, or change orders. After you create the template, you can link it to a service type.

Note: If multi-tenancy is installed, specify the tenant in the Tenant field.

Follow these steps:

1. Select **Service Desk**, **Service Target Templates** on the **Administration** tab.
   The **Service Target Template List** page opens.

2. Click **Create New**.
   The **Create New Service Target Template** page opens.

3. Select a ticket type from the **Object Type** field, and click **Continue**.

4. Complete the following fields as appropriate:

   - **Name**
     Defines a descriptive identifier for the service target.

   - **Object Type**
     Identifies the ticket type for this service target.

   - **Target Duration**
     Specifies the maximum amount of time for service target completion in the hh:mm:ss format.

   - **Workshift**
     Specifies the workshift which contains a range of working hours that are used in time calculations for a service target, for example, M-F 08:00-17:00.

   - **Cost**
     Defines information such as the estimated cost associated with missing the service target.

   - **Record Status**
     Indicates whether this target is active or inactive.

   - **Condition**
     Specifies the name of the condition macro or site-defined condition that evaluates the ticket data and determines whether the service target is met.

   - **Required Outcome**
     Specifies a True or False value that indicates whether the service target is complete.

   - **Allow Set Actual**
     Specifies whether to allow users to set the date and time for a service target.

   - **Allow Reset Actual**
     Specifies whether to allow users to reset the date and time for a service target.

5. Click **Save**.
   The service target template is created.

Link a Service Target Template to a Service Type

When you link a service target template to a service type, the targets are automatically attached to a ticket when the service type is assigned. You can only assign a service target template once to a service type. Many different service targets can be linked to a service type.

Follow these steps:

1. Select **Service Desk**, **Service Types** on the **Administration** tab.
   The **Service Type List** page opens.

2. Select a service type.
   The **Service Type Detail** page opens.

3. Select the target tab for the selected object type. For example, if you have created the service target for request, select **Request Targets** tab to manage problem, incident, and request tickets.

4. Click **Link Service Target Template**.
   The **Create New Linked Service Target Template** page opens.

5. You can enter a value directly or click the magnifying glass to search for a service type.

6. Click **Continue**.

7. Make changes to the service target template, if necessary.

8. Click **Save**.
   The service target template is linked to the service type.

View Ticket Counters and Timers for Service Targets

If an analyst assigned a set of service targets to a ticket, you can view the status and deadlines for completing each target.

Follow these steps:

1. On the Service Desk tab, display a list of Incidents, Problems, Requests, Change Orders, or Issues.
   The ticket detail page appears.

2. Click the Service Type tab.
   Additional Service Type information appears at the bottom of the ticket.

3. In the Target column, click the Service Target for additional information.
   The Ticket Counters and Timers section appears near the bottom of the Assigned Service Target Detail page. The Assigned Service Target Detail page displays the following fields:

   - **Name**
     Displays the name of the service target.

- **Target Duration**
  Displays the amount of allotted time to perform the service target. You can only override this value by editing the ticket.

- **Workshift**
  Displays the schedule used for time calculations for the service target.

- **Condition**
  Displays the condition or site-defined condition macro that evaluates the ticket data to determine whether the work can complete within the target time frame.

- **Required Outcome**
  Displays the required result of the condition or site-defined condition Macro.

- **Cost**
  Displays the penalty that incurs for missing the target. This information also displays on the ticket.

- **Target Date/Time**
  Displays the deadline for completing the target. If the ticket is in a Hold status or the service target has been met, this field is blank.

- **Actual Date/Time**
  Specifies the date and time that the condition was satisfied or the user clicked Set Actual.

- **Time Left**
  Displays the amount of remaining time for the service target. A negative value indicates the amount of time that exceeded the target time frame.

- **Allow Set Actual**
  Displays whether you can set the actual time. Yes indicates that you can set the Actual Date/Time of a Service Target. No indicates that you cannot override the Actual Date /Time.

- **Allow Reset Actual**
  Displays whether you can restart the time. Yes indicates that you can reset the Actual Date /Time of a Service Target. No indicates that you cannot reset the Actual Date/Time.

- **Last Modified Date/Time**
  Displays the date that this ticket was last modified.

- **Last Modified By**
  Displays the name of the last person who edited the ticket.

- **Service Type**
  Displays the name of the service type that attached this service target.

- **Service Target Template**
  Displays the name of the service target template that was linked to the service type that was used to create this Service Target.

- **Lock Target Date/Time From Hold Recalculations**
  Locks the Target Date/Time from being automatically updated when the ticket goes on hold or is delayed.

- **Last Start Date/Time**
  Displays the last time the service target timer was started.

- **Ticket Status**
  Displays the value of the Status field of the ticket.

- **Hold Status**
  Displays whether the ticket status has placed the ticket on hold.

- **Last Hold Date/Time**
  Displays the last time the ticket was placed on hold.

- **Hold Count**
  Displays the number of times the ticket was placed on hold.

- **Last Resolved Date/Time**
  Displays the last time the ticket transitioned to a resolved status.

- **Resolved Count**
  Displays the number of times that the ticket changed to resolved status.

- **Last Closed Date/Time**
  Displays the last time the ticket was changed to a closed status.

- **Closed Count**
  Displays the number of times the ticket changed to a closed status.

- **Ticket Open Date/Time**
  Displays the date and time the ticket opened.

- **Ticket Resolved Date/Time**
  Displays the date and time the ticket resolved.

- **Ticket Closed Date/Time**
  Displays the date and time the ticket closed.

View Service Target Status

On an open ticket, you can view the status for each service target. Status information such as Time Left and Violation Cost help you prioritize your work.

Follow these steps:

1. On the Service Desk tab, display a list of Incidents, Problems, Requests, Change Orders, or Issues.
   The respective ticket list displays with the following Service Target information:

- **Service Target**
  Displays the time that the next service target is due.

- **Projected Violation**
  Displays the incurred cost when the service type time limit is violated.

2. Select the ticket you want from the list page.
   The ticket detail page appears.

3. Select the Service Type tab.

> **Note:** Service targets appear on tickets that meet the conditions that the administrator sets up. Priority calculation can be a factor in how target information calculates and displays.

If the ticket meets pre-defined target conditions, the Service Targets List the following information about service targets:

- **Action**
  Sets or resets the Actual Date/Time to the current date and time.

- **Target**
  Specifies the current service target for the ticket.

- **Target Date/Time**
  Specifies date and time when this service target is due. If the ticket is in a Hold status, this value is blank.

- **Actual Date/Time**
  Specifies the time when the target condition was met. If no value appears, the target condition has not been met.

- **Time Left**
  Specifies the amount of remaining time for the service target when the ticket is on hold. If the service target has been met, the Time Left field shows the unused time. A negative value indicates the amount of time that elapsed since the missed target date.

- **Violation Cost**
  Displays the penalty that incurs for missing the target. This information also displays on the ticket.

Service Contracts

This article contains the following topics:

- How to Manage Multiple Time Zones for Service Types (see page 1120)
- Workshifts Setup (see page 1121)

The SLA model includes the Service Contract. The Service Contract defines the SLA for a particular organization, including its Service Types, Request areas, and Issue or Change Categories. These definitions are referred to as *private* Categories and *private* Service Types.

Note: The *private* Categories and Service Types can only be used on tickets where the Service Contract is used.

The Service Contract applicable to a ticket is determined by the ticket's *affected organization*, which is always the Organization of the Affected End User on the ticket (this is the Organization field on a Contact record). Only the Areas or Categories listed on the Service Contract can be selected for the ticket. In addition, the only Service Types that can be applied are the *private* ones listed on the Contract. This helps ensure that the SLAs for one Organization are not accidentally mixed with another's.

A Service Contract also maps Service Types to common reference fields on a ticket, such as Priority and Asset. This mapping associates Service Types with attributes of a ticket. For example, an Organization's contract can assign Service Types to each of the five Priority objects. When a ticket is created with a certain priority, the mapped Service Type is applied.

Categories and Service Types can be defined outside of a Contract and are considered *public*. The public definitions are used when a ticket has no Service Contract. The lack of a Service Contract can occur if the end user has no organization, or the organization's Contract is inactive. A public definition is a helpful backup or default mechanism. Public Service Types are set directly on categories and other reference field objects.

All applicable Service Types are assigned to the ticket. This ensures that all aspects of an SLA are visible and enforced, for example:

- A Printer may have a Service Type that requires a technician to be dispatched within two days.
- A priority object's Service Type may require a callback within one hour.

With both Service Types applied, these required actions are enforced.

Tracking multiple Service Types also helps prioritize tickets. For example, a ticket concerning a broken keyboard is assigned a low priority Service Type. However, if the affected end user is in urgent need of the keyboard, the service priority can be increased.

Note: The SLA model is enforced by default. Past versions of CA SDM applied only a single Service Type to a ticket. The Service Type selection involved finding the highest *ranked* Type among all the possible Service Types. A model using the ranking scheme can still be used by installing the Option 'classic_sla_processing'.

Service Contracts Migration

If CA SDM is installed as a migration, the Option classic_sla_processing is turned ON by default, so your SLA processing can continue as before the migration. This continuation gives you time to create appropriate Service Contracts and eventually deactivate classic_sla_processing.

When building Service Contracts, you do not have to create Service Types, Request Areas, or Categories. You can use the Copy button found on the Service Contract detail to copy existing objects to the Contract.

If the previous installation marked the support_lev field as required for any ticket type, this restriction must be removed. The support_lev field still exists, but is not set in the current model so a required field error results with new tickets. This affects the objects Request (cr), Issue (iss) or Change Order (chg).

Time to Violation

When the SLA model is in use, CA SDM's Time to Violation (TTV) system can help you track and prioritize tickets according to their projected violation time. This system monitors all active tickets and sets the projected violation time for each Service Type. You can report and sort tickets based on their violation time and cost, helping you resolve the most urgent and costly issues first.

The TTV system monitors all active tickets and evaluates their SLA events silently, to determine which events set the SLA violation flag. The events are not executed, but the system looks at the outcome of each event based on the current state of the ticket. If the evaluation results in an action that sets the SLA violation flag, the ticket's attached Service Type is updated with a Time to Violation value; this value is the date/time when the event fires that sets the SLA violation.

Evaluation occurs whenever a ticket is inserted or updated. Because tickets are often updated in rapid succession, the evaluation is delayed for a short period. The delay interval is controlled by the ttv_evaluation_delay Option. After the delay expires, the TTV system evaluates all the SLA events that might set the SLA violation flag.

Each Event has an optional condition and a set of actions (Macros) that start based on the outcome of the condition. To ensure adequate performance, Event template information is cached by the TTV system and is refreshed periodically. Projections made by TTV involving recently updated Event templates may be inaccurate for several minutes.

Note: The TTV projections appear on the Service Type tab of each ticket. The TTV system is activated with the ttv_enabled Option.

Time Zones and Workshifts

To address the complex business demands of automated application execution, CA SDM lets you define as many time zones and workshifts as you want, and to record them for easy reference.

- Time zones identify the time zone where the user, CI, and so forth, are located.
- Workshiftsdefine the period during which event monitoring or the work hours of a service type or SLA are in effect.

Being able to determine a course of action to perform based on when an event occurs can be critical to the proper handling of the event. The time zones and workshifts you define are available for use by any of the CA SDM functions.

Time Zones Setup

Time zone codesdefine the time zone from which a user usually accesses the system (that is, the user' s local time zone) or the time zone in which a CI is located. Business hours are always entered in the time zone of the CA SDM server. This means that business hours can always be compared uniformly.

Time zones are used to manage service types, escalations, and overall response to affected end users based on the ability of CA SDM to present the correct time across multiple time zones. CA SDM automatically adjusts the offset between the time zone where a user is logging in or a CI is located, and the time zone where the server is running. Time zones use the Greenwich Mean Time (GMT) format.

How to Manage Multiple Time Zones for Service Types

CA SDM servers and users can be located in different time zones. The time difference can cause users to miss Service Type expiration dates and times.

To correct the time difference, you can configure CA SDM to display Service Type expiration times in the end-user time zone. If two users in different time zones view the same ticket, each user sees Expiration Time values based on the local computer time zone. However, the Start Time values always reflect the server time zone.

To configure for the end-user time zone, do the following:

1. Create a server code that identifies the server name and time zone.

2. Create or update a Service Type. Set the Use End User Timezone field to Yes.
   A value of Yes causes the Expiration Time to display and update according to each user time zone.

Example: Show Service Type Expiration Dates in Any User Time Zone

In this example, you configure CA SDM to show Service Type expiration dates in any user time zone. The server and user are on separate computers and in different time zones.

To create a server code that identifies the server name and time zone

1. On the Administration Tab of the host server, select Service Desk, Application Code.

2. Click Codes, Servers.
   The Server List displays.

3. Click the Local Host server.
   The Server Name Detail page appears.

4. Set the Time Zone. For example, set the time zone to GMT (EU). The local host name must match the NX_LOCAL_HOST value stored in NX.env for the server

5. Click Save.
   The Host Server uses the new time zone. When the user views a ticket, the Start Time reflects the server time zone.

To create a service type

1. On the Administration Tab, select Service Types.
   The list of Service Types appears.

2. Click Priority 1 Resolution or another Service Type that manages Priority 1 Requests.
   The Update Service Type page displays.

3. Select the Use End User Time Zone check box.

4. Click Save.
   The Service Type record updates.

To view the time zones on the ticket

1. On another computer, open a Request ticket, and set the Priority to 1.

   Note: If you are using Service Targets, set the values in the ticket to cause the target to use Priority 1 Resolution.

2. View the ticket and click the Service Type tab.
   The Start Time reflects the server time zone. The Expiration Time reflects the time on the end-user local computer.

3. Close the page that displays the Request ticket.

4. Change the time zone on the end-user local computer.

5. View the ticket Service Type on the end-user local computer to see the corresponding Expiration Time values based on the user time zone.
   The Expiration Time reflects the new time zone.

Workshifts Setup

Workshiftsidentify the days, dates, and times when an event or schedule is in effect. You can specify days or dates, or days and dates. Specifying a time is optional.

When you are monitoring events for tickets, workshifts define when the event is monitored or, in other words, when the clock is running. For example, using the predefined event P1 Active Issue Notify assignee, if a priority 1 issue is opened at 4:45 PM and the workshift schedule is 9:00 AM to 5:00 PM, the monitored event automatically sends notification to the issue assignee at 9:45 AM the next day.

Note: Workshifts are also used for the purpose of automatically assigning tickets to contacts.

Create a Service Contract

You can create service contracts and map them to contacts, configuration items, and priorities.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. Select Service Desk, Service Contracts on the Administration tab.
   The Service Contract List page appears.
2. Click Create New.
   The Create New Service Contract page appears.
3. Complete the Service Contract fields (see page 1122) as appropriate.
4. Configure the service contract mapping (see page 1123) as appropriate.
5. Click Save.
   The service contract definition is saved and the Service Contract Detail page appears.

Service Contract Fields

The following fields require explanation to create or update a service contract:

- **Client Advocate**
  The person within the company that runs the help desk. This person is the point of contact between the “Customer” company and the “Help Desk” company. This person is a member of the organization that would get special notifications
- **Client Contact**
  This is the contact person that would get notified on tickets/service types/etc.
- **Assigned to Organization(s)**
  Displays the name of an organization assigned to the service contract. If an organization has not been assigned, None appears.
  Add an organization to a service contract by first creating the new service contract. Then, access the Scoreboard tab, select File, Create New Organization and while creating the organization, select the contract previously saved. When you access the service contract, the Assigned to Organization(s) field is populated with the updated organization name.

- **Organization's Service Type**
  If set, this service type is ALWAYS applied to any ticket opened for the organization. This is useful for adding baseline events, notifications or SLA parameters that need to be on every ticket regardless of priority, category, etc. For example, the Client Advocate gets a notification for every ticket opened/closed for the Organization, so they have a general idea of how their customer is doing.

  If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

Service Contract Tabs

The following tabs are available on the Service Contract Detail and Update Service Contract pages:

- **Contacts**
  Allows you to map one or more contacts to the service contract. Also allows you to update a contact's service type. Click Map Single Contact.

- **Groups**
  Allows you to map one or more groups to the service contract. Also allows you to update a group's service type. Click Map Single Group.

- **Config. Items**
  Allows you to map one or more configuration items to the service contract. Also allows you to update a configuration item's service type. Click Map Single CI.

- **Priorities**
  Allows you to map a priority to the service contract. Click Map Priority.

- **Urgencies**
  Allows you to map an urgency to the service contract. Click Map Urgency.

The following tabs appear on the Service Contract Detail page after a new service contract record has been saved:

- **Private_Service_Types**
  Allows you to create a new service type to map to this service contract. Click Add Private Service Type.**Request Areas**

- Allows you to create a new request area or copy an existing request area to map to the service contract. Click Add New Request Area.**Change Categories**

- Allows you to create a new change category or copy an existing change category to map to the service contract. Click Add New Change Category.**Issue Categories**

- Allows you to create a new issue category or copy an existing issue category to map to the service contract. Click Add New Issue Category.

Add an Issue Category to a Service Contract

You can create one or more new issue categories to associate with this service contract.

To create a new issue category for the service contract

1. Select the Issue Categories tab on the Service Contract Detail or Update Service Contract page.
2. Click Add New Issue Category.
   The Create New Issue Category page appears.
3. Fill in the fields as appropriate to define the area.
4. Click Save.
   The issue category definition is saved and the Issue Category Detail page appears, with the name of the associated contract in the Service Contract field.
5. Close the Issue Category Detail page and return to the Service Contract Detail page.
   The new issue category is listed on the Issue Categories tab.

To copy an existing issue category for the service contract

1. Select the Issue Categories tab on the Service Contract Detail or Update Service Contract page.
2. Click Copy Existing Issue Category.
   The Issue Category Search page appears.
3. (Optional) Complete one or more search fields to filter your search.
4. Click Search.
   The Issue Category List page lists the issue categories that match your search criteria.
5. Select the issue category you want to copy.
   The Create New Issue Category page appears with the fields of the copied issue category filled in.
6. (Optional) Update the fields as appropriate for the new issue category.
7. Click Save.
   The issue category definition is saved and the Issue Category Detail page appears, with the name of the associated contract in the Service Contract field.
8. Close the Issue Category Detail page and return to the Service Contract Detail page.
   The new issue category is listed on the Issue Categories tab.

Update a Service Contract

You can edit a service contract record that has already been created.

Note: When you update a service contract, the Private Service Types, Request Areas, Change Categories, and Issue Categories tabs are available on the Service Contract Detail and Update Service Contract pages.

To update a service contract

1. Select Service Desk, Service Contracts on the Administration tab.
   The Service Contracts List page appears.

2. Select the service contract to edit.
   The Service Contract Detail page appears.

3. Click Edit.
   The Update Service Contract page appears.

4. Edit the fields as appropriate.
   See Service Contract Fields (see page 1122) for field definitions.

5. (Optional) Use the controls available on the tabs at the bottom of the page to configure the service contract record.
   See Service Contract Tabs (see page 1123) for more information.

6. Click Save.
   The service contract definition is saved and the Service Contract Detail page appears.

Automatic Closure of Tickets

You can use a configurable setting to allow automatic closure of tickets (requests/incidents /problems, change orders, or issues). When a ticket is set to a Resolved status, the ticket is automatically closed in the number of business hours specified. The Auto Close activity notification sent to the end user displays the number of business hours before the ticket is closed. The number of hours is configurable and tenant-specific. If the status is changed before the configurable number of hours ends, the ticket closure is canceled.

Administrators, can perform the following actions:

- Define an Auto Close ticket setting to control the number of business hours, for the end user, before the ticket is automatically closed.
- Set up an Auto Close activity notification to notify the appropriate contacts when automatic closure is scheduled for a ticket.

If you use multi-tenancy, consider the following:

- The system uses the default public Auto Close setting when a tenant-specific Auto Close setting is not found.
- There is one Auto Close setting for each tenant.

How to Define Auto Close Ticket Settings

You can define the number of business hours before a ticket is closed (all ticket types) as follows:

1. On the Administration tab, select Service Desk, Application Data, Codes, Auto Close.

2. Click Create New on the list page.

3. Complete the following fields on the detail page:

   - **Symbol**
     Defines the system setting name.

   - **Request/Incident/Problem/Change Order/Issue**
     Defines the number of business hours, after the ticket is set to Resolved status, before the ticket is closed. If the status is changed before the number of hours ends, the ticket closure is canceled. 0 (zero) hours indicates that automatic closure is not implemented for the ticket type.

   - **Description**
     Provides a brief description of the record.

   - **Status**
     Indicates if the record is active or inactive.

   The auto close setting is defined.

4. Click Save, Close Window.
   The new setting appears on the Auto Close List page when you redisplay the list.

How to Define an Auto Close Activity Notification

You can change the settings in the default Auto Close activity notification to notify the appropriate contacts when automatic closure is scheduled for a ticket. The activity is valid for all CA SDM ticket types, and include a default notification rule for requests/incidents/problems, change orders and issues.

To define an auto close activity notification, do the following:

1. On the Administration tab, select Notifications, Activity Notifications.

2. Select the Auto Close activity notification on the list page to open it.

3. Update the default Auto Close Notification Rule and specify contacts to receive notification.

4. Click Save, Close window.
   The updated Auto Close activity notification appears in the Activity Notification List when you redisplay the list.

Search Attachments

You can enter search criteria to filter the Attachments List to display only the attachments you want to see. You can also search for individual attachments to view or edit.

Follow these steps:

1. From the Administration tab, select Attachments Library, Attachments.
   The Attachment Search page opens.

2. Complete the search fields. The following fields require explanation:

   Note: All search fields that allow text entry support use of the % wildcard character.

   - **Repository** -- The repository where the file resides.
   - **Status** -- Choose from one of the following values:
     - **Installed** - Attachment is available and in place.
     - **Link Only** - Attachment is a URL link.
     - **Not Installed** - Attachment is not in place. Request has not completed successfully.
     - **Archived** - Attachment is archived.
     - **Not Available** - The attachment could not be found after an archive and purge.
     - **Knowledge File** - Attachment is a text file.

3. Click Search.

   The Attachment List page displays the attachments that match your filter criteria. You can select an attachment to view or edit it.

   Note: If you are using multi-tenancy, a tenant drop-down list appears in the search filter. If you select <empty> in this drop-down list, the search is public.

Create an Announcement

You can use CA SDM to post announcements to users. Announcements help decrease the number of incoming calls and promote increased productivity through proactive resolution of tickets and communication of important information to all affected users. Users can scroll through stored multiple announcements.

Note: Announcements apply to all service desk models.

You can add new announcements and update existing ones. Announcements are part of the reference data function of CA SDM, so by using the access type you can control which contacts can create announcements.

An announcement can specify either or both of the following:

- **Location**
  Specifies a physical location, for example, a city, building, or floor.

- **Organization**
  Specifies an organization ID. When Organization is set for an Announcement, only individuals assigned to that Organization can see the Announcement.

When Location or Organization is set for an announcement, only contacts at that location or organization receive it. Any contact can still see all announcements that are not restricted by location or organization. For example, if neither is set, contacts in every location and organization can see an announcement.

Note: You can specify announcements using the administrative function of the web interface.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Scoreboard, select File, New Announcement.
   The Create New Announcement window opens.

2. Fill in the fields as appropriate. See Announcement Fields (see page 1129) for field definitions.

3. To insert a link to a Knowledge Document in the announcement, click Knowledge Doc.
   The Knowledge Document search page displays.

4. Search for the document you want to include. See Search Knowledge Documents for more information.

5. In the Link Text field, type the text to be used to link to the document.

6. Click Insert Document.
   The HTML code linking to the Knowledge Document is added to the Text field.

7. Click Save to save the announcement.
   The new announcement is added to the right pane of the main window.

Announcement Fields

- **Text** -- Enter the text of the announcement. Click Spelling to perform a spell check of the text you entered. This field is required.
  If you insert a link to a Knowledge Document, the HTML code for that link is displayed in this field.
- **Location** -- The location where the announcement is displayed. Enter the name of the location directly into the field, or click the search icon to search for the location.
- **Internal** -- Select this option if this announcement should only be shown to internal employees.
- **Organization** -- The organization where the announcement is displayed. Enter the name of the organization directly into the field, or click the search icon to search for the organization.
- **Announcement Type** -- Determines the urgency of the announcement and the color of the announcement text displayed in the window. Asterisks are displayed next to the posted date for color blind or visually impaired users.
  The possible values are:
  - **Routine --** Black text. No asterisks.
  - **Advisory** -- Orange text. One asterisk, after the date.
  - **Emergency** -- Red text. Two asterisks, after the date.
- **Status** -- Indicates whether the announcement is active (displayed) or inactive (not displayed).
- **Close Date/Time** -- The date and time to stop displaying the announcement. Enter the date and time in the format mm/dd/yyyy hh:mm AM | PM, or click the calendar icon to select the date and time.

Announcements

This article contains the following topics:

You can use CA SDM to post announcements to users. Announcements help decrease the number of incoming calls and promote increased productivity through proactive resolution of tickets and communication of important information to all affected users. Users can scroll through stored multiple announcements.

Note: Announcements apply to all service desk models.

You can add new announcements and update existing ones. Announcements are part of the reference data function of CA SDM, so by using the access type you can control which contacts can create announcements.

An announcement can specify either or both of the following:

- **Location**
  Specifies a physical location, for example, a city, building, or floor.

- **Organization**
  Specifies an organization ID. When Organization is set for an Announcement, only individuals assigned to that Organization can see the Announcement.

When Location or Organization is set for an announcement, only contacts at that location or organization receive it. Any contact can still see all announcements that are not restricted by location or organization. For example, if neither is set, contacts in every location and organization can see an announcement.

Note: You can specify announcements using the administrative function of the web interface.

View Announcements

Announcements are used to convey important information about the system to the users. Current announcements display in the right pane of the main window when you first login to the system.

To display the Announcements page, choose View, Announcements. To create a new announcement, choose File, New Announcement (refer to for more information).

If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

Create an Announcement

Announcements are used to convey important information about the system to the users.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Scoreboard, select File, New Announcement.
   The Create New Announcement window opens.

2. Fill in the fields as appropriate. See Announcement Fields (see page 1131) for field definitions.

3. To insert a link to a Knowledge Document in the announcement, click Knowledge Doc.
   The Knowledge Document search page displays.

4. Search for the document you want to include. See Search Knowledge Documents for more information.

5. In the Link Text field, type the text to be used to link to the document.

6. Click Insert Document.
   The HTML code linking to the Knowledge Document is added to the Text field.

7. Click Save to save the announcement.
   The new announcement is added to the right pane of the main window.

Announcement Fields

- **Text** -- Enter the text of the announcement. Click Spelling to perform a spell check of the text you entered. This field is required.
  If you insert a link to a Knowledge Document, the HTML code for that link is displayed in this field.

- **Location** -- The location where the announcement is displayed. Enter the name of the location directly into the field, or click the search icon to search for the location.

- **Internal** -- Select this option if this announcement should only be shown to internal employees.

- **Organization** -- The organization where the announcement is displayed. Enter the name of the organization directly into the field, or click the search icon to search for the organization.

- **Announcement Type** -- Determines the urgency of the announcement and the color of the announcement text displayed in the window. Asterisks are displayed next to the posted date for color blind or visually impaired users.
  The possible values are:

  - **Routine --** Black text. No asterisks.

  - **Advisory** -- Orange text. One asterisk, after the date.

  - **Emergency** -- Red text. Two asterisks, after the date.

- **Status** -- Indicates whether the announcement is active (displayed) or inactive (not displayed).

- **Close Date/Time** -- The date and time to stop displaying the announcement. Enter the date and time in the format mm/dd/yyyy hh:mm AM | PM, or click the calendar icon to select the date and time.

Internal Announcement Visibility

You can control whether an announcement is visible to internal users by using the Internal check box on the Create New Announcement page. The View Internal Logs setting of the access type of the logged in user controls whether a user can view items marked as internal.

Specify Announcement Urgency

You can specify the urgency of an announcement record.

To specify announcement urgency

1. Create an announcement or navigate to the Announcement Detail page to edit an existing announcement.

2. Select one of the following values from the Announcement Type drop-down list:

   - **Routine**
     Displays in black text.

   - **Advisory**
     Displays in orange text.

   - **Emergency**
     Displays in red text.

   Click Save.
   The announcement record is color-coded in the Announcements List page.

Auto Assignment

This article contains the following topics:

CA SDM *Auto Assignment* reduces the time that is required to manage tickets by automating the process of assigning them to analysts. This automation can make the tasks that are associated with balancing workloads and coordinating work schedules much more efficient.

You can configure auto assignment to assign tickets that are based on the following factors:

- Which analyst groups work on which tickets or tasks.
- When the work must be done.

The locations catering the affected customers.

- The workload and availability of each analyst.
- The value of an attribute of a configuration item that is associated with the ticket.

Note: Configuration item-based auto assignment (see page 1158) lets you create group-specific assignments for Request/Incident/Problem tickets only. You do not have to implement auto assignment all at once. You can develop a strategy for phasing it in gradually. For example, you can begin by enabling it only for selected ticket types, analyst groups, or locations.

Auto Assignment Relationships

The auto assignment process can involve many CA SDM elements. The element relationships are as follows:

- Areas and categories relate to groups, locations, and workshifts.
- Groups relate to locations and workshifts.

To make the auto assignment easy to administer, all relationships can be maintained from either related element. For example, when relating an analyst group to a change category, you can maintain the association from either the Change Category Detail page or the Group Detail page.

Auto Assignment Methods

The following basic methods let you auto assign tickets:

- **Location-based auto assignment**
  Creates assignments for all ticket types that are based on the following criteria:
  - Areas and categories that are related to groups, locations, and workshifts
  - Groups that are related to locations and workshifts

Note: The Location-based auto assignment is referred to simply as auto assignment.

- **Configuration item-based auto assignment**
  Creates group assignments for request, problem, and incident ticket types that are based on the following criteria:

  - Areas that are related to tickets associated with configuration items
  - Configuration item attributes used to record contact/group information

Location-based auto assignment and configuration item-based auto assignment are exclusive options. This is because you can select only one algorithm for use on a given Request/Incident /Problem Area. Location-based auto assignment and configuration item-based methods both serve to assign tickets when. However, Configuration item-based auto assignment is distinct, because it also reevaluates the assignments for a ticket upon changing the Area or configuration item of a Request /Incident/Problem ticket. If a configuration item-based auto assignment is specified, without successfully generating a group assignment for a ticket, the Area_Defaults option is consulted to determine whether the default Group and Assignee values on the Area should be used to assign the ticket.

Default Group and Assignee

When the auto assignment logic is unable to identify a suitable group or assignee, the ticket is assigned to the default group and assignee. You can specify these defaults in the Group and Assignee fields of the following web interface pages:

- Request/Incident/Problem Area Detail
- Change Category Detail
- Issue Detail

If auto assignment cannot identify a suitable group or assignee and the defaults are not specified, the ticket is left for manual assignment.

Auto Assignment Enablement

Options and controls let you configure auto assignment. You can control whether auto assignment processing occurs as follows:

- For requests, incidents, and problems assigned to that area, use the Auto Assignment Enabled tab on the Request/Incident/Problem Area Detail page.
- For change orders and issues, select the Auto Assignment tab and Auto Assignment Enabled check box on the Change Category Detail page, Issue Category Detail page.

Example: Enable Auto Assignment for a Request/Incident/Problem Area

This example demonstrates how to enable auto assignment for a Request/Incident/Problem area.

1. On the Administration tab, browse to Service Desk, Requests/Incidents/Problems, Areas.
   The Requests/Incidents/Problems Area List page appears.
2. Click the area for which you want to configure auto assignment.
   The Requests/Incidents/Problems Area Detail page appears.

3. Click Edit.
   The Update Requests/Incidents/Problems Area page appears.

4. Select the Auto Assignment tab, and complete the following fields as follows:

   - **Auto Assignment Mode**
     Specifies how auto-assignment occurs. You use the Configuration Item Based option to base the auto assignment on the CI Assignable Attribute value.

     - **Disabled** -- Bases the auto-assignment on the Area Defaults option when it is installed.
     - **Configuration Item Based** -- Bases the auto-assignment on the CI Assignable Attribute value.
     - **Location Based** -- Bases the auto-assignment on the location value.

   - **Assignable CI Attribute**
     Specifies the configuration item attribute to use for the group assignment. You can enter a value directly or click the magnifier to search for an attribute.

5. Click Save.
   The Request/Incident/Problem area is enabled to use default values that are entered automatically on the tickets that are assigned to the area.

Auto Assignment Override

You can use the Auto Assignment Override (autoasg_override) option in the Options Manager to determine if the auto assignment overrides an analyst or a group that is set when a ticket is created.

Other CA SDM features may have set the assignee and/or group before auto assignment obtains control. You can configure your system by setting this option to one of the following values:

- **0**
  Honors the existing assignee and/or group. If the assignee and/or group was set during the creation of the ticket, auto assignment processing does not occur.

- **1**
  Ignores the existing assignee and/or group. Auto assignment processing continues and attempts to find an assignee and/or group.

You can set the Assignee and/or Group in various ways:

- Manually by the Analyst
- Area Defaults and the Assignee set options
- Request Templates
- CA NSM integration

Note: Uninstalling the Auto Assignment Override option causes it to operate in its default mode, which is 0.

Configure Auto Assignment by Location

The Auto Assignment tab allows you to establish a relationship between this location and request areas, change categories, issues categories, and groups. This allows you to assign tickets to eligible members of the group within the location automatically.

Important! You must enable automatic assignment for each request area and category individually. Listing them on the Location Auto Assignment tab does not enable this function.

Follow these steps:

1. On the Location Detail page, click Edit and select the Auto Assignment tab.
2. Click one of the following buttons:
   - Update Request Areas to select request areas for auto assignment.
   - Update Change Categories to select change categories for auto assignment.
   - Update Issue Categories to select issue categories for auto assignment.
   - Update Groups to select groups for auto assignment.

   The Search page for the selected item appears.
3. Enter the search criteria to display the desired items and click Search.

   The Update page appears, listing the items that matched the search criteria.
4. From the list on the left, select the desired items. To select multiple items, hold down the CTRL key while clicking the left mouse button.
5. When you have selected all the items that you want, click the double right-arrow button.

   The selected items move to the Assigned list on the right.
6. Click OK.

   The Location Detail page displays, with the selected items listed on the Auto Assignment tab.

Assignment Controls

Options and controls let you configure the auto assignment. The CA SDM features can affect the assignee, the group fields, or both on a ticket before auto assignment processing occurs. We recommend that you review assignment controls before implementing auto assignment.

Manual Assignment

The analyst can manually select the assignee and/or group while creating a ticket.

Assignee_set Option

By default, CA SDM automatically sets the logged in analyst user as the assignee of the request. An Options Manager option, Assignee_set, lets you control this behavior. This option is typically installed by default.

Iss assignee_set

The Iss assignee_set option automatically sets the logged in analyst user as the assignee of the Issue. It is similar to Assignee_set, except it is for Issues instead of Requests.

Area_Defaults

The Area_Defaults option determines what happens when the request area is specified on a request detail page. This option lets you set the assignee and group whenever the request area changes. The default assignee and group from the request area are used, and this processing occurs before auto assignment processing.

This option is not installed by default.

Note: The Category_Defaults option provides similar functionality for change orders. The Iss_Category_Defaults option provides similar functionality for issues.

Require Assignee and Group Options

Several options are available in Options Manager for controlling the creation of unassigned tickets. These options are global in scope. They affect the creation of all of the indicated ticket types, regardless of whether auto assignment is in effect. If the indicated condition is not satisfied, the new or updated ticket cannot be saved.

The following options control the creation of tickets without an assignee specified:

- **require_change_assignee**
  Application: Change Order Mgr
  Description: Makes the Assignee field of a change order ticket required

- **require_issue_assignee**
  Application: Issue Mgr
  Description: Makes the Assignee field of an issue ticket required

- **require_incident_assignee**
  Application: Request Mgr
  Description: Makes the Assignee field of an incident ticket required

- **require_problem_assignee**
  Application: Request Mgr
  Description: Makes the Assignee field of a problem ticket required

- **require_request_assignee**
  Application: Request Mgr
  Description: Makes the Assignee field of a request ticket required

The following options control the creation of tickets without a group specified:

- **require_change_group**
  Application: Change Order Mgr
  Description: Makes the Group field of a change order ticket required

- **require_issue_group**
  Application: Issue Mgr
  Description: Makes the Group field of an issue ticket required

- **require_incident_group**
  Application: Request Mgr
  Description: Makes the Group field of an incident ticket required

- **require_request_group**
  Application: Request Mgr
  Description: Makes the Group field of a request ticket required

- **require_problem_group**
  Application: Request Mgr
  Description: Makes the Group field of a problem ticket required

Templates

You can use templates to set the values on a new request, change order, or issue. Templates can affect assignee and group fields.

CA Network and Systems Management Interface

When CA NSM and CA SDM are integrated and you are creating requests from CA NSM events, the user_parmsparameter in writer rule definitions is passed to the Text API. The CA SDM writer process (tngwriter) defines its own replacement parameters for changing the text before sending it to the Text API. The keyword LOG_AGENT is added to the end of the input to set the log_agent for the request.

Note: You must update the Text_API.cfg file for all additional fields that are passed from CA NSM Alert Management Systems to CA SDM. This file is used for integrations with web services, email, and AHD.DLL.

How Auto Assignment Assigns Tickets

This article contains the following topics:

Auto-assignment assigns tickets as follows:

1. The initial save operation of a new ticket invokes auto assignment.
   If an area or category is not configured for auto assignment, processing stops.

2. Auto assignment determines whether Autoasg_override is installed.
   If it is not installed and the ticket has an assignee or group, processing stops.

3. If work shifts are related to the ticket, the open date is evaluated to determine the inclusion of a ticket.
   If a work shift does not include the ticket, processing stops. Auto assignment attempts to assign the default group and assignee.

4. Auto assignment determines whether any groups are related to the ticket.
   If no groups are related, processing stops, and auto assignment attempts to assign the default group and assignee.

5. Auto assignment filters any groups with work shift, where the open date is outside the time frame of the work shift. Groups without a work shift bypass filtering.

6. The following processing occurs for locations that are related to the ticket:

   - If this ticket is a request, and it has a configuration item:
     The location of the configuration item is matched against the locations that are related to the request area. If no match occurs, processing stops, and auto assignment attempts to assign the default group and assignee. Otherwise, the customer location is matched against the locations that are related to the area or category. If no match occurs, processing stops, and auto assignment attempts to assign the default group and assignee.

   - If locations are associated with the request area or category:
     Suppose that locations are associated with the request area and the configuration item (during request auto assignment processing), or the customer has no location. Then auto assignment stops processing.

7. Auto assignment filters the groups that have related locations that do not match the configuration item location (for requests only) or customer location. If no groups remain, processing stops, and auto assignment attempts to assign the default group and assignee.

8. Auto assignment creates a list of analysts from each of the remaining eligible groups.

9. Unavailable analysts are filtered.

10. The remaining analysts are checked for Work Schedules. Available analysts that have Work Schedules are filtered when the open date is not within their work schedules.

11. If no analysts remain, processing stops and auto assignment attempts to assign the default group and assignee.

12. All the remaining analysts are ranked according to the number of active tickets that are assigned to them.

13. The analyst (and associated group) with the least number of active tickets is assigned to the ticket. If a tie occurs, the first analyst that occurs in the group is selected.

How Auto Assignment Assigns Workflow Tasks

Auto Assignment assigns workflow tasks as follows:

1. Auto assignment is invoked when the status of a workflow task changes to pending. If the workflow template that the workflow task was created from is not enabled for auto assignment, processing stops. If the parent change order category or Issue category is not enabled for auto assignment, processing stops.

2. Auto assignment checks to determine if Autoasg_override is installed. If not installed and the task has an assignee or group, processing stops.

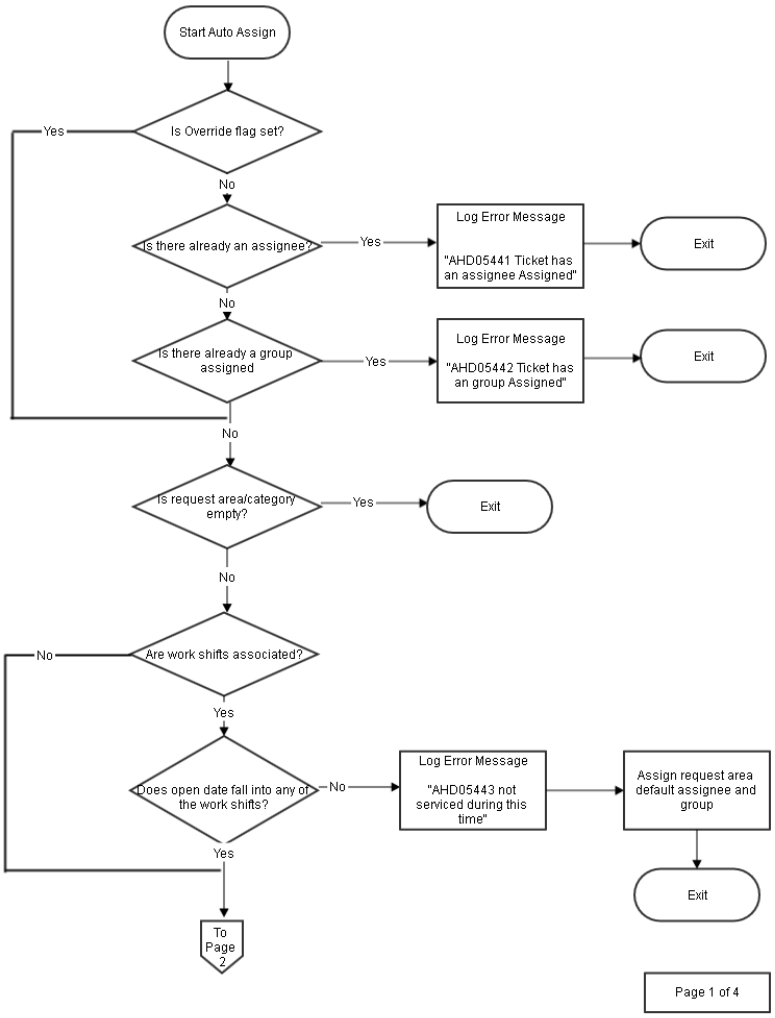
3. The workflow template that the workflow task was created from is checked to see if any contacts are associated with it. If there are no contacts, processing stops.

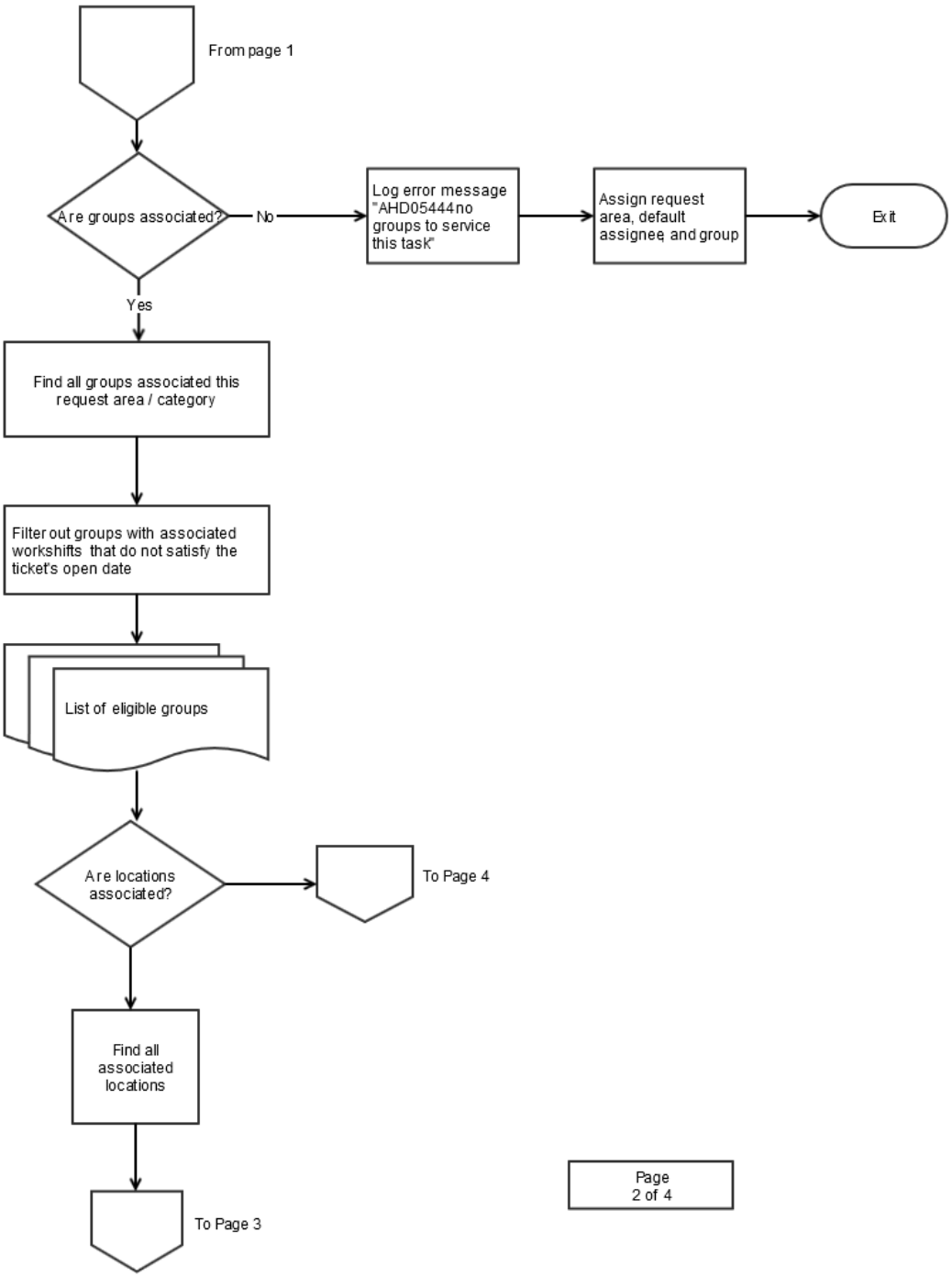
4. Auto assignment builds a list of contacts that are members of the groups that are currently associated to the workflow template. The workflow template must be the template from which the workflow task was created. Any contacts in this list that are groups are filtered out.

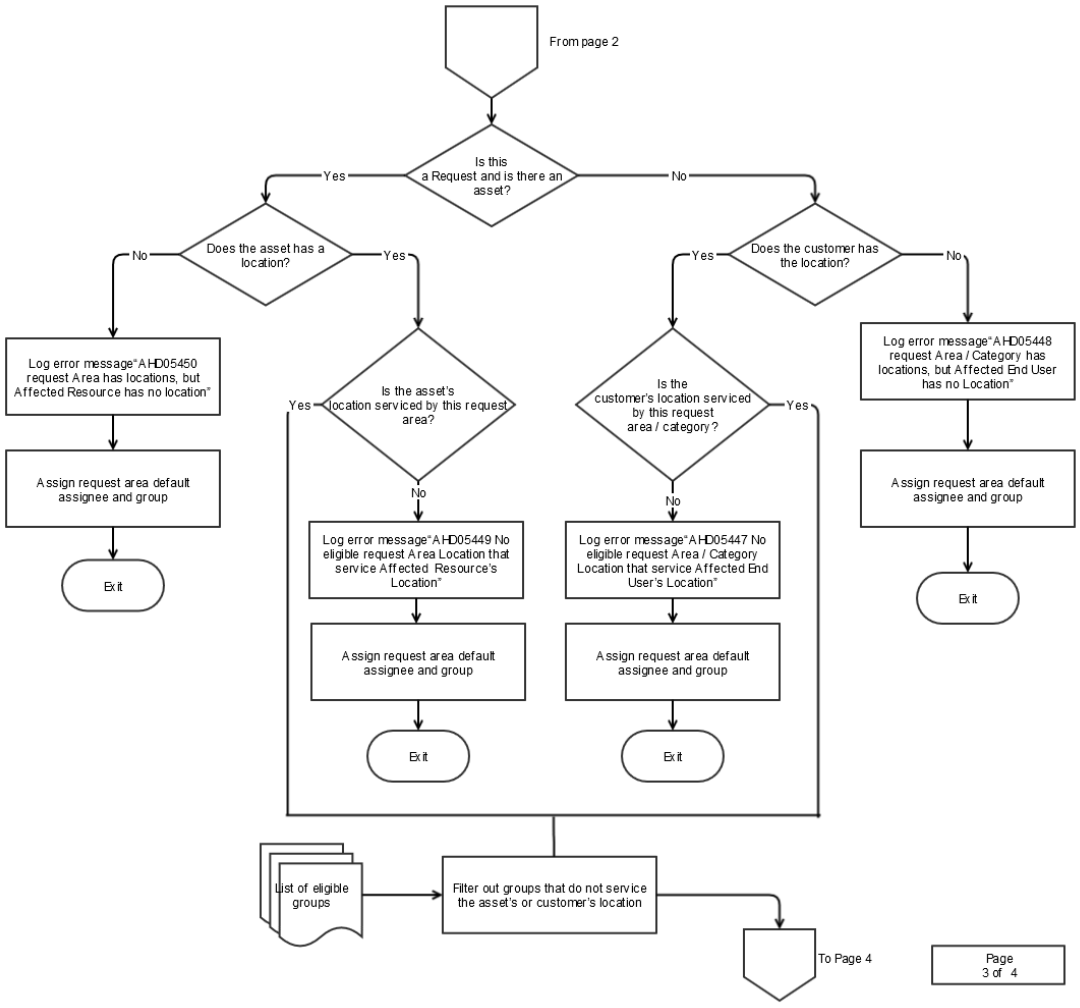
5. All of the remaining contacts are ranked according to the number of active change order tasks or the corresponding issue tasks.

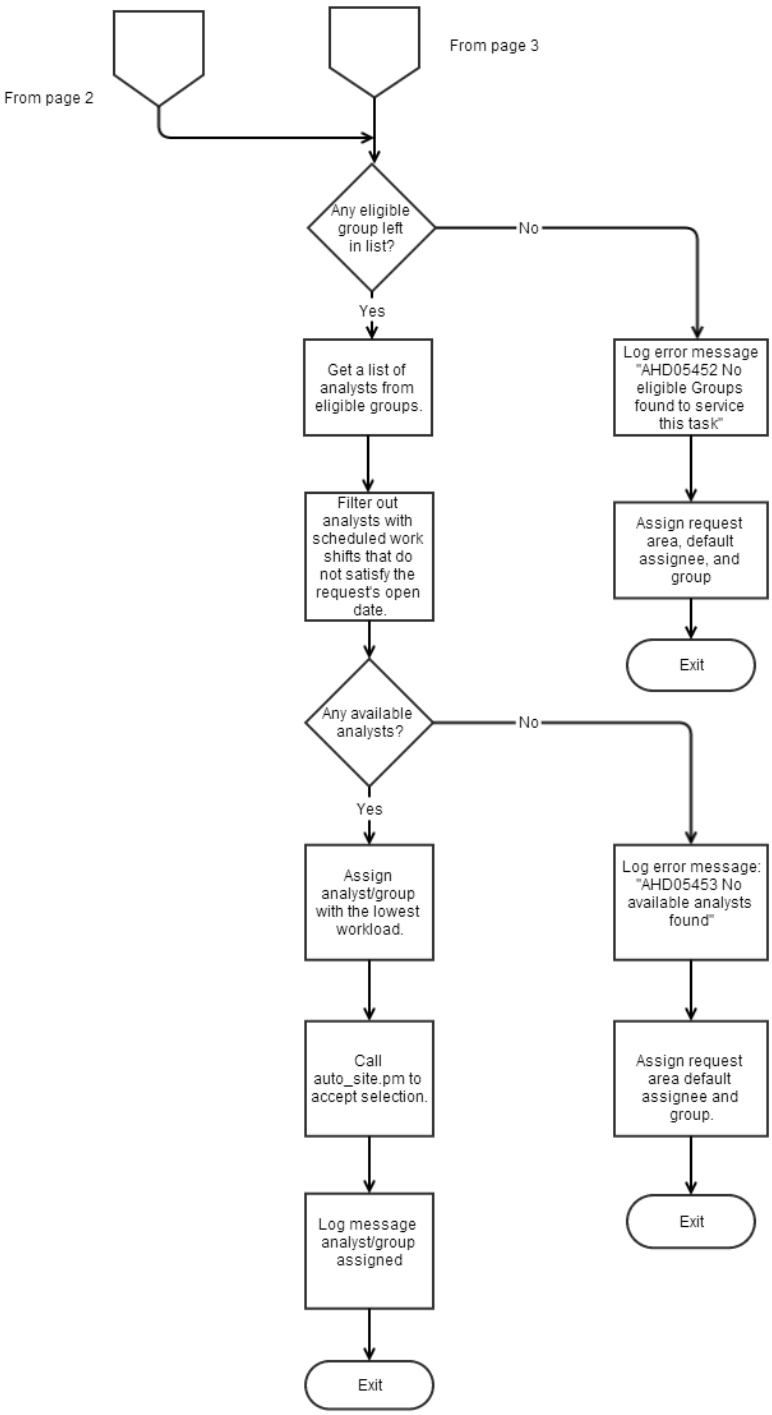
6. The contact and associated group with the least number of active tasks is assigned to the task.

Ticket Process Flow Diagram

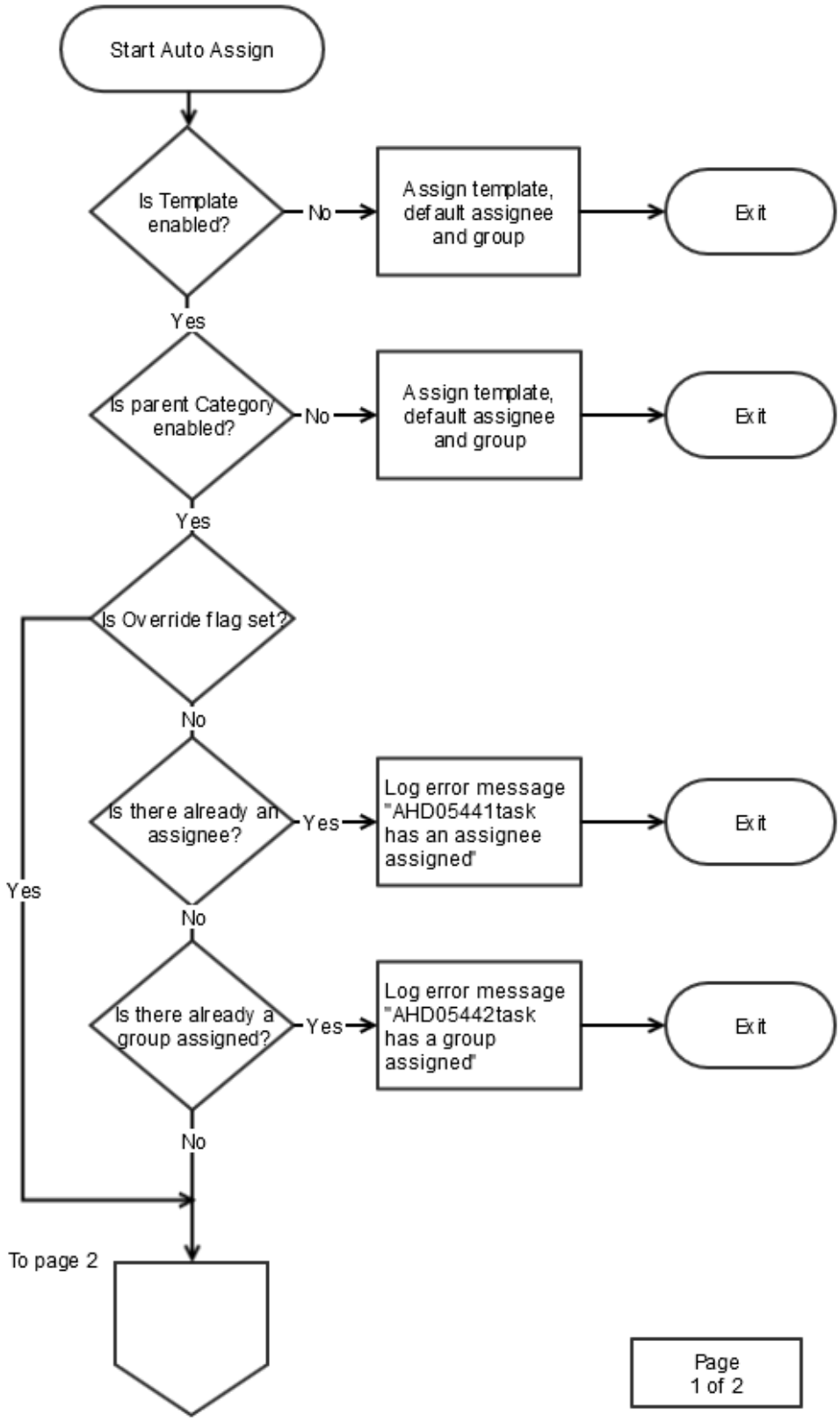


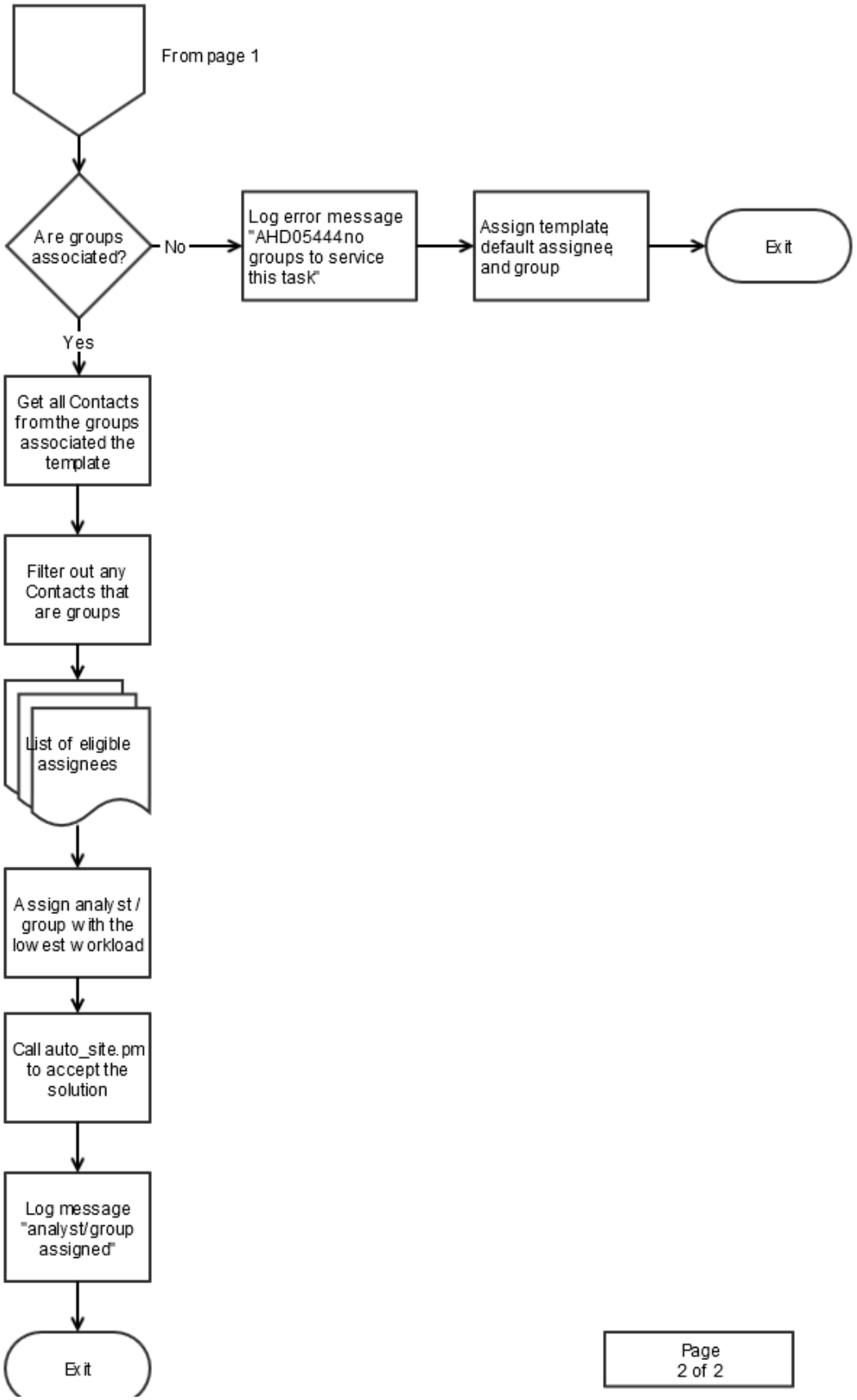

From page 1
Are groups associated?
No
Log error message "AHD05444 no groups to service this task"
Assign request area, default assignee, and group
Exit
Yes
Find all groups associated this request area / category
Filter out groups with associated workshifts that do not satisfy the ticket's open date
List of eligible groups
Are locations associated?
To Page 4
Find all associated locations
To Page 3
Page 2 of 4


From page 2
Is this a Request and is there an asset?
Yes
No
Does the asset has a location?
No
Yes
Does the customer has the location?
Yes
No
Log error message"AHD05450 request Area has locations, but Affected Resource has no location"
Assign request area default assignee and group
Exit
Is the asset's location serviced by this request area?
Yes
No
Log error message"AHD05449 No eligible request Area Location that service Affected 'Resource's Location"
Assign request area default assignee and group
Exit
Is the customer's location serviced by this request area / category?
Yes
No
Log error message"AHD05447 No eligible request Area / Category Location that service Affected End User's Location"
Assign request area default assignee and group
Exit
Log error message"AHD05448 request Area / Category has locations, but Affected End User has no Location"
Assign request area default assignee and group
Exit
List of eligible groups
Filter out groups that do not service the asset's or customer's location
To Page 4
Page 3 of 4

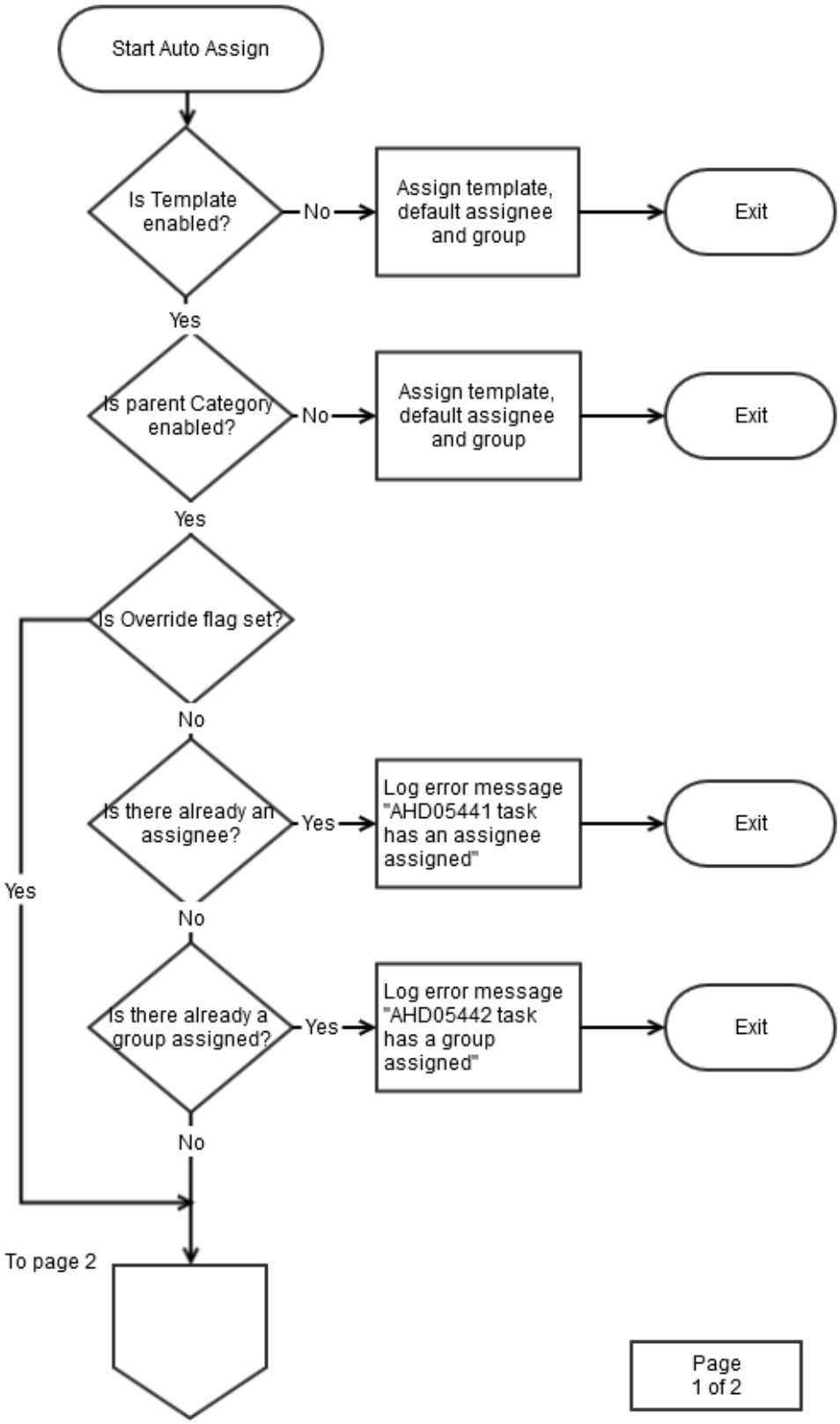

From page 2
From page 3
Any eligible group left in list?
No
Yes
Get a list of analysts from eligible groups.
Log error message "AHD05452 No eligible Groups found to service this task"
Filter out analysts with scheduled work shifts that do not satisfy the request's open date.
Assign request area, default assignee, and group
Exit
Any available analysts?
No
Yes
Assign analyst/group with the lowest workload.
Log error message: "AHD05453 No available analysts found"
Call auto_site.pm to accept selection.
Assign request area default assignee and group.
Log message analyst/group assigned
Exit
Exit
Page 4 of 4

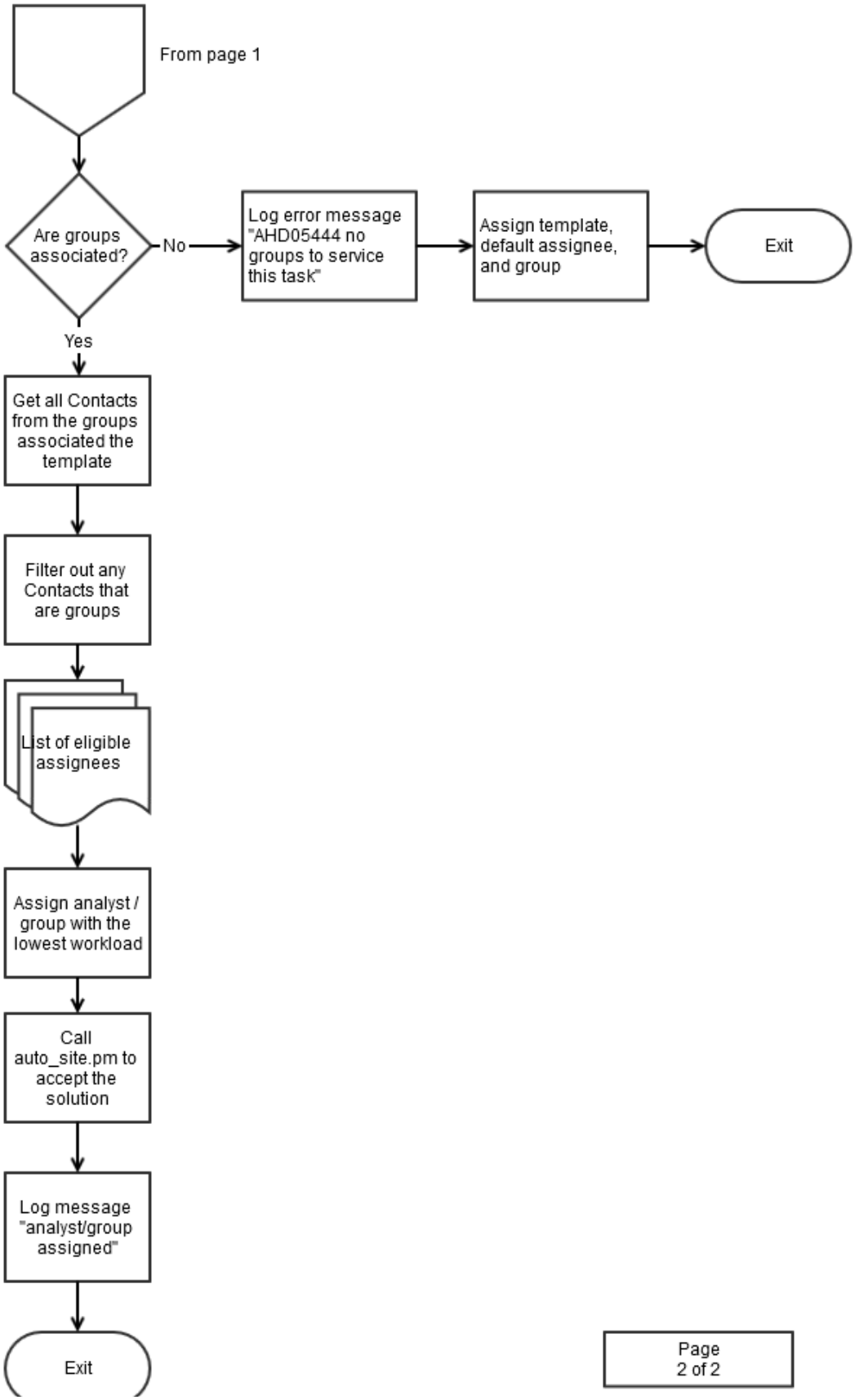
Workflow Process Flow Diagram

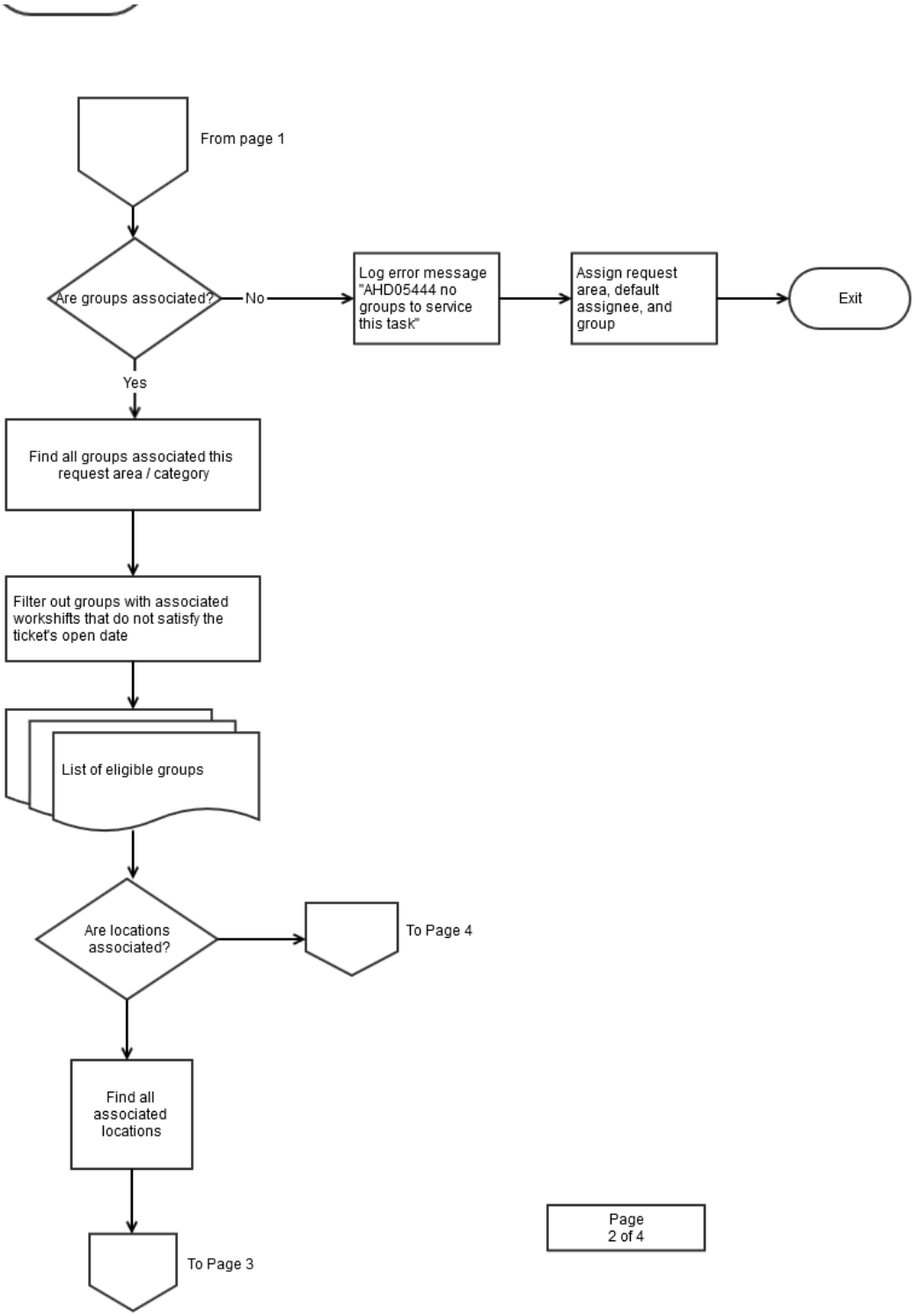

Start Auto Assign
Is Template enabled?
No
Assign template, default assignee and group
Exit
Yes
Is parent Category enabled?
No
Assign template, default assignee and group
Exit
Yes
Is Override flag set?
No
Is there already an assignee?
Yes
Log error message "AHD05441task has an assignee assigned"
Exit
Yes
No
Is there already a group assigned?
Yes
Log error message "AHD05442task has a group assigned"
Exit
No
To page 2
Page 1 of 2

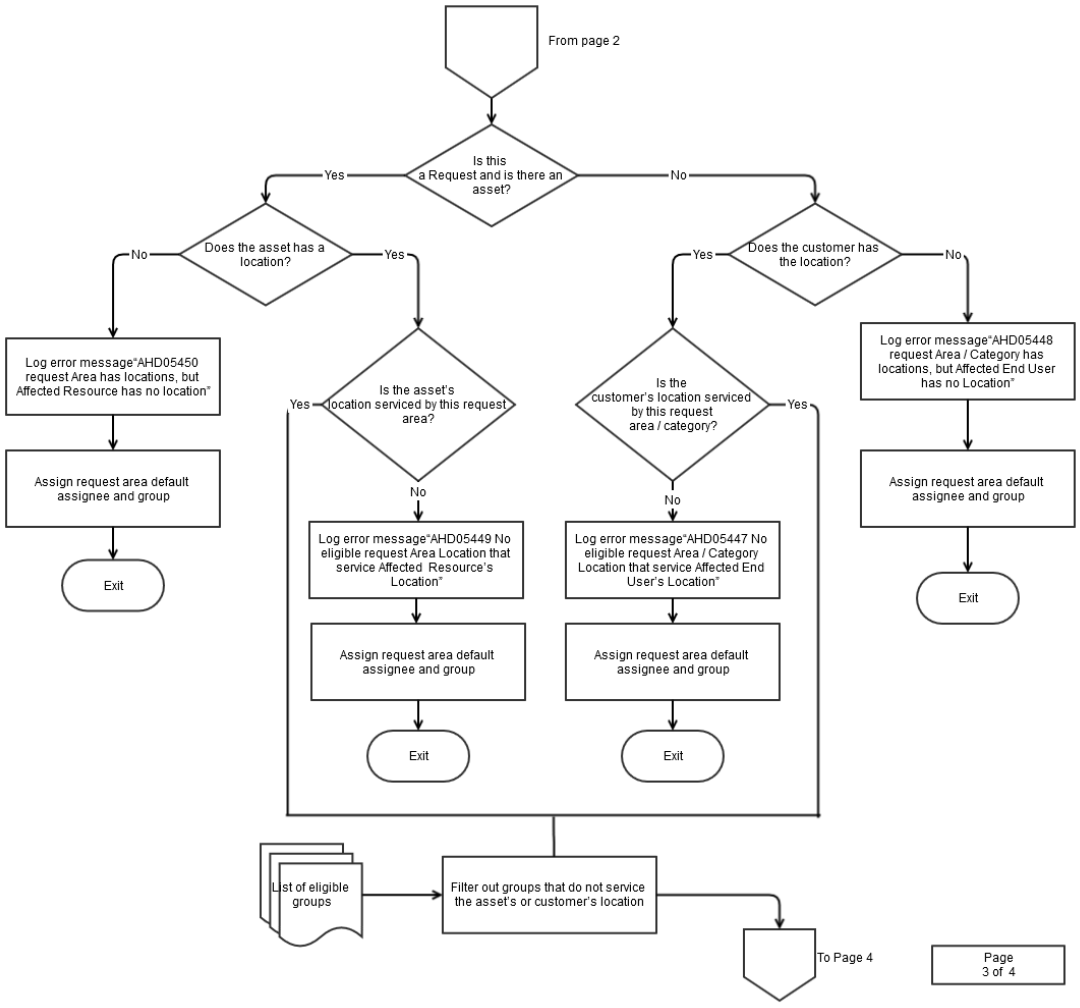

From page 1
Are groups associated?
No
Log error message "AHD05444 no groups to service this task"
Assign template default assignee and group
Exit
Yes
Get all Contacts from the groups associated the template
Filter out any Contacts that are groups
List of eligible assignees
Assign analyst / group with the lowest workload
Call auto_site.pm to accept the solution
Log message "analyst/group assigned"
Exit
Page 2 of 2

How Auto Assignment Assigns Tickets - Flow Diagram


Start Auto Assign
Is Template enabled?
No
Assign template, default assignee and group
Exit
Yes
Is parent Category enabled?
No
Assign template, default assignee and group
Exit
Yes
Is Override flag set?
No
Is there already an assignee?
Yes
Log error message "AHD05441 task has an assignee assigned"
Exit
Yes
No
Is there already a group assigned?
Yes
Log error message "AHD05442 task has a group assigned"
Exit
No
To page 2
Page 1 of 2


From page 1
Are groups associated?
No
Log error message "AHD05444 no groups to service this task"
Assign template, default assignee, and group
Exit
Yes
Get all Contacts from the groups associated the template
Filter out any Contacts that are groups
List of eligible assignees
Assign analyst / group with the lowest workload
Call auto_site.pm to accept the solution
Log message "analyst/group assigned"
Exit
Page 2 of 2


From page 1
Are groups associated?
No
Log error message "AHD05444 no groups to service this task"
Assign request area, default assignee, and group
Exit
Yes
Find all groups associated this request area / category
Filter out groups with associated workshifts that do not satisfy the ticket's open date
List of eligible groups
Are locations associated?
To Page 4
Find all associated locations
To Page 3
Page 2 of 4



How to Begin Implementing Auto Assignment

This article contains the following topics:

Follow these guidelines to begin implementing auto assignment for selected analyst groups and analysts:

1. Identify one or more areas or categories for which you want to enable auto assignment.

   Note: To review your site area and category configurations, examine the settings in the CA SDM web interface.

2. By default, auto assignment is disabled. Enable it only for the areas and categories (see page 1154) where you want to use it.

3. Build the relationships between an identified area or category and the analyst groups (see page 1155) that can be assigned tickets through that area or category.

4. Mark individual members of the analyst (see page 1155) groups as available.

Areas and Categories

Note: When you configure areas and categories, consider setting default groups and assignees (see page 1134).

To configure the auto assignment of request, incident, and problem tickets, use the following options in the Auto Assignment tab of Request/Incident/Problem Area Detail page:

- Update Groups
- Update Locations
- Update Workshifts

Note: The check box for enabling auto assignment is also on the Auto Assignment tab of each of these pages. It is visible only while the page is in edit mode.

The following pages on the interface provide the same controls for configuring auto assignment of change orders and issues:

- The Change Category Detail
- The Issue Category Detail

Analyst Groups

To configure auto assignment you must, at a minimum, define the relationships between analyst groups and areas or categories. Assignees are chosen from groups that meet *all* of your specified auto assignment criteria. If no additional constraints are defined, tickets are auto assigned to the group member with the fewest active tickets.

If no groups are associated with an area or category, the default group and assignee are assigned. If these defaults are not defined, the ticket is left for manual assignment.

You can maintain the relationships between groups and areas or categories on the area or category detail page.

Alternatively, use the following options to maintain the same relationships on the Auto Assignment tab of the Group Detail page:

- Update Request Areas
- Update Change Categories
- Update Issue Categories
- Update Locations

Analysts

Fields on the Analyst Detail page help determine whether the analyst is eligible for auto assignment.

Analysts are eligible for auto assignment only if they are marked as available.

The Analyst Detail page provides an Available check box that enables auto assignment.

Consider allowing analysts to control their own auto assignment availability. You can monitor analyst availability by using stored queries.

Note: The Available check box is not considered during auto assignment of workflow tasks.

The Work Schedule field allows analysts to have tickets auto-assigned only during their scheduled workshift. Analysts that are marked as available and are without work schedule are eligible for auto assignment at any time. However, no other constraints must result in an ineligible status.

Stored Queries

Two stored queries are provided for monitoring the availability of analysts. The CA SDM managers can add the following queries to their Scoreboard:

- **Available Analysts** -- Analysts that are marked as available for auto assignment
- **Unavailable Analysts** -- Analysts that are marked as unavailable for auto assignment

How to Auto Assign Tickets to a Group and Not to Contacts Within the Group

Auto assignment assigns tickets to contacts that have the Available option selected in the contact record. However, you can auto assign incidents/issues/change orders/requests to a group and not to contacts within the group. The NX_AUTOASG_GROUP_ONLY option controls the auto assignment behavior for groups. You install this option to auto assign the tickets to the group instead of individual contacts. NX_AUTOASG_GROUP_ONLY is not available on the web interface, you install it from the command prompt.

Follow these steps:

1. Verify that your CA SDM installation is at a minimum level of Release 12.9 Cumulative 2 patch.
2. Open the command prompt on any CA SDM server.
3. Run the following command:

   ```
   pdm_options_mgr -c -s AUTOASG_GROUP_ONLY -v 1 -a pdm_option.inst
   ```

   By default, new options that you add to the nx.env file are not saved after you run pdm_configure. You can save the changes permanently by specifying the -t option as follows:

   ```
   pdm_options_mgr -c -s AUTOASG_GROUP_ONLY -v 1 -a pdm_option.inst -t
   ```

   The commands update the following files in CA SDM with the new option:

   - Windows -- NX_ROOT/NX.env and NX_ROOT\pdmconf\nx.env.nt.tpl
   - UNIX/Linux -- NX_ROOT/pdmconf/NX.env.tpl
4. Open the NX.env file in the CA SDM installation folder and search for the variable @NX_AUTOASG_GROUP_ONLY=1. Typically, the variable is found at the end of the file.
5. Open the file nx.env.nt.tpl present under NX_ROOT/pdmconf and search for the @NX_AUTOASG_GROUP_ONLY=1 option.
6. Restart the CA SDM Daemon Server service.
   CA SDM auto assigns the tickets to the group only.
7. Restart the CA SDM servers (see page 866).

Auto Assignment by Location

If your service area is large and it consists of many locations that service different customer communities. You can use location as a factor in your auto assignment configuration as follows:

- **Location Assigned to an Area or Category** -- If you assign a location to an area or a category, tickets are auto assigned only when a matching location is found. For example, a request ticket is auto assigned if there is an eligible analyst at the following locations:
  1. The affected asset location.
  2. The affected customer location.

If the affected asset or customer has no specified location, the request is assigned to the default group and assignee. If these defaults are not defined, the request is left for manual assignment. You can use the area or category detail pages to maintain relationships between locations and areas or categories.

- **Location Assigned to a Group** -- When a location is associated with a group, only members of that group are eligible for auto assignment of tickets. Further, only the tickets that pertain to the location of the member can be assigned. You can use group detail pages to maintain relationships between groups and locations.

To maintain location relationships with areas, categories, or groups, use the following options on the Auto Assignment tab of Location Detail page:

- Update Request Areas
- Update Change Categories
- Update Issue Categories
- Update Groups

Examples: Use Location in Auto Assignment Configuration

The following are examples of how you can use location in your auto assignment configuration:

- **Auto assign tickets only at a specified location** -- Tickets from other locations receive the default group and assignee, or are left for manual assignment. For example, you can have many users at your company headquarters, and smaller groups of users at regional offices. An analyst group located at the headquarters services their local users, while mobile analyst groups visit the regional offices. You can configure auto assignment of tickets to the headquarters analysts only, and manually assign tickets to the mobile analysts.
- **Auto assign tickets by user or asset location** -- You can restrict auto assignment eligibility to analyst groups at locations that match the affected user location, or the affected asset location. For example, your organization can have many offices, but only the groups that are located in a particular office handle tickets for the office. You can relate each group to appropriate areas or categories *and* to the appropriate location. The auto assignment logic selects eligible analysts only from groups at the correct location.

Auto Assignment by Workshift

You can constrain auto assignment by relating an area or category to a workshift. The workshift determines the timeframe within which tickets are eligible for auto assignment. Tickets opened outside the workshift are assigned to the default group and analyst, or left for manual assignment.

You can also use workshifts to control group and analyst eligibility for assignment:

- If you assign a work schedule to a group. Analysts in that group are eligible for auto assignment only to tickets opened during their work schedule.

> **Note:** The workshift for a group is specified in the Work Schedule field of the Group Detail page.

- If you assign a work schedule to an individual analyst. The analyst is eligible for auto assignment only to tickets opened during that work schedule.

> **Note:** The workshift for an analyst is specified in the Work Schedule field of the Analyst Detail page.

When a ticket is created, the group that meets the assignment eligibility criteria is identified. Within the group, the analyst with the fewest active tickets is identified. If an appropriate analyst is not identified, the ticket is assigned to the default group and assignee. If these defaults are not defined, the ticket is left for manual assignment.

For workflow tasks associated with change orders or issues, auto assignment uses a simpler selection strategy. Assignees are selected from the groups that are associated with workflow templates. Workflow task assignees can be of any contact type except group. When a task changes to pending status, the contact that has the fewest change order or issue workflow tasks is selected. To prevent unwanted results, if the parent change order category or issue category is disabled for auto assignment, tasks are not assigned automatically. Workflow tasks may encompass individuals external to service desk. So, relying on them to reflect their availability with the available flag is not recommended.

You can use the area or category detail pages to relate a workshift to an area or category. Or, you can use the following controls on the Workshift Detail page:

- Update Request Areas
- Update Change Categories
- Update Issue Categories

Examples: Use Workshifts in Auto Assignment Configuration

The following examples show how you can use workshifts in your auto assignment configuration:

- **Auto assign tickets to the shift on duty** -- Suppose that your service desk operates 24 hours per day and you have tickets about network outage problems. You may want to configure auto assignment of such tickets to the shift on duty when the ticket is opened.
- **Allow auto assignment only during a specified shift** -- You may want to restrict further auto assignment of tickets in some areas or categories. For example, if analysts are on duty only during day shift, you may auto assign application problems only during the day shift.

Configuration Item-Based Auto Assignments

Configuration item-based auto assignment lets you create group-specific assignments that apply to specific scenarios. You can specify that for a particular Request/Incident/Problem area, the value of a configuration item attribute controls the assignment of the ticket.

Configuration item-based and location-based auto assignments are exclusive options because you can select only one algorithm for use. Configuration item-based and location-based auto assignment modes both serve to assign tickets. However, configuration item-based auto assignment is distinct, because it also reassigns tickets after changing the Request/Incident/Problem Area.

Example: Request/Incident/Problem Area Assigns Tickets to a Group

Suppose that you configure the Network Area to assign configuration item-based auto assignments using the network_contact_uuid attribute as the Assignable CI Attribute value. Tickets that are opened for the Network Area are assigned automatically to the group that is specified for Network Operations in the corresponding CI. If no CI is associated with the ticket, the Network Operations value of the CI is blank, or a group is not specified, the ticket is not assigned. In such cases, the system acts in accordance with the Option Manager option, Area Defaults, and assigns the ticket using the Group and Assignee fields of the Category.

How Configuration Item-Based Auto Assignment Works

Request/Incident/Problem tickets must specify the following for configuration item-based auto assignment to occur:

- A configuration item and an Area.
- The Area must have the Auto Assignment option set to Configuration Item Based.

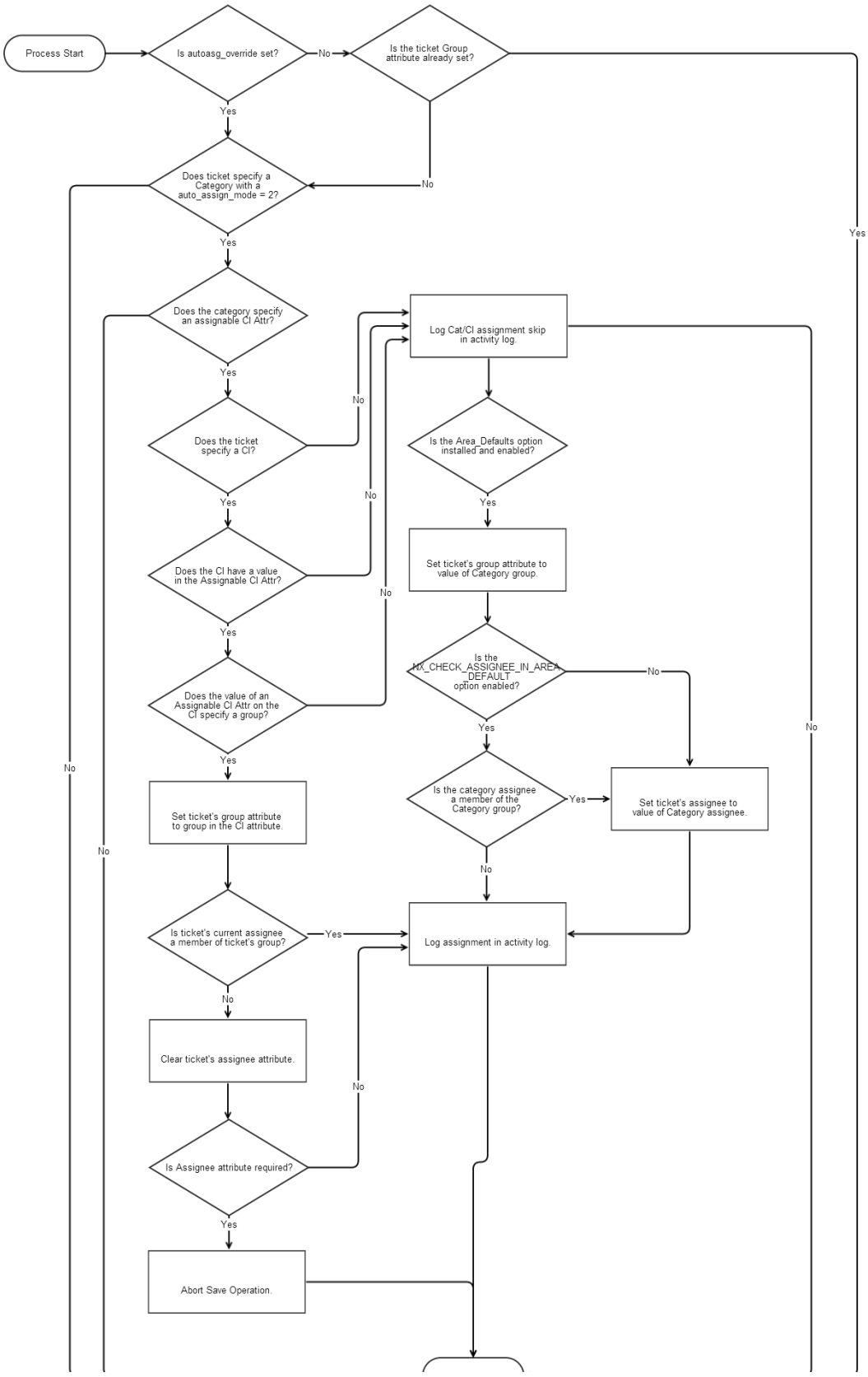
When an analyst creates and assigns a ticket to this Area, or changes the Area on an existing ticket, CA SDM examines the Assignable CI Attribute field of the Area. CA SDM uses the value of Assignable CI Attribute as the name of an attribute and then attempts to find an identically named attribute on the configuration item that is associated with the ticket. If the attribute on the configuration item includes a group, the ticket is assigned to that group.

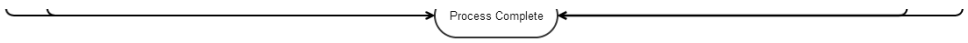
The following diagram describes the process for configuration item-based auto assignment in more detail:

1. CA SDM checks for the following:
    a. Is the autoasg_override option set?
    b. Does a ticket specify an Area with its Auto Assignment auto_assign_mode=2?
    c. Does the category specify an assignable CI attribute?
    d. Does the ticket specify a configuration item?
    e. Does the configuration item have an assignable CI attribute value?
    f. Does the value specify a group in the CI attribute?
    g. Is the assignee of the ticket a member of the ticket group?
2. When the answers are positive for all questions in the previous step, CA SDM sets the group attribute of the ticket to the group attribute of the CI, and logs the assignment in the activity log.

Note: The diagram shows how Configuration Item-Based Auto Assignment uses the NX_CHECK_ASSIGNEE_IN_AREA_DEFAULTS variable to determine if the Area option is enabled. NX_CHECK_ASSIGNEE_IN_AREA_DEFAULTS is a variable in the NX.env file, which is located in the $NX_ROOT\ directory.

3. CA SDM assigns the ticket to the group.


Process Start
Is autoasg_override set?
No
Is the ticket Group attribute already set?
Yes
Does ticket specify a Category with a auto_assign_mode = 2?
No
Yes
Does the category specify an assignable CI Attr?
Yes
Log Cat/CI assignment skip in activity log.
Does the ticket specify a CI?
No
Yes
Is the Area_Defaults option installed and enabled?
Yes
Does the CI have a value in the Assignable CI Attr?
No
Yes
Set ticket's group attribute to value of Category group.
Does the value of an Assignable CI Attr on the CI specify a group?
No
Yes
Is the NX_CHECK_ASSIGNEE_IN_AREA_DEFAULT option enabled?
No
Yes
Set ticket's group attribute to group in the CI attribute.
Is the category assignee a member of the Category group?
Yes
Set ticket's assignee to value of Category assignee.
No
Is ticket's current assignee a member of ticket's group?
Yes
Log assignment in activity log.
No
Clear ticket's assignee attribute.
Is Assignee attribute required?
No
Yes
Abort Save Operation.
No
No
No
Yes



Enable Configuration Item-Based Auto Assignments

Configuration item-based auto assignment lets you create group-specific assignments that apply to specific scenarios. You can specify that for Request/Incident/Problem tickets opened for a particular Area, the value of an attribute of the configuration item associated with the ticket controls its assignment. Configuration item-based auto assignment reassigns tickets whenever the Request /Incident/Problem Area of a ticket or configuration item changes.

Note: The Options Manager autoasg_override option controls the circumstances under which auto assignment takes place. When you set this option to 1, CA SDM ignores any existing assignee and group settings and auto assigns tickets in all cases. If you want CA SDM to auto assign tickets only if they are not already assigned, set the option value to 0.

Follow these steps:

1. On the Administration tab, browse to Service Desk, Request/Incident/Problems, Areas.
   The Request/Incident/Problem Area List appears.

2. Click the area to edit.
   The Area Detail page appears.

3. Click Edit.
   The Update Area page appears.

4. Select the Auto Assignment tab, and complete the fields as follows:

   - **Auto Assignment Mode**
     Specifies how auto-assignment occurs. You use the Configuration Item Based option to base the auto assignment on the CI Assignable Attribute value.

   - **Assignable CI Attribute**
     Specifies the configuration item attribute to use for the group assignment. You can enter a value directly or click the magnifier to search for an attribute.

   Click Save.
   Auto assignment is enabled. CA SDM performs configuration item-based auto assignments using the attribute that you specified in the Assignable CI Attribute field.

Activity Logging

Auto assignment logs information as events in the ticket's activity log. The success or failure of auto assignment is logged, and any anomalies that may have occurred during processing.

Enable Activity Logging for Additional Attributes

Activity logs display changes attribute values of objects. Objects such as all ticket types, classic workflow tasks, Surveys, Contacts, and Configuration Items feature activity logging. You can enable activity logging for additional attributes In WSP.

Note: You can view activity log simple attributes, including strings, integers, date, duration, and SREL types. You cannot view activity logs for list types, such as QRELs and BRELs.

Follow these steps:

1. Open WSP and start the Schema Designer.
2. Select the table that you want to modify, and add additional attributes.
3. For each attribute, add +AUDITLOG() to the site-defined UI_INFO field.

   Important! When you add the AUDITLOG flag, you *must* also remove the val_fieldupdate_site() function to prevent duplicate activity logs.

4. Save and publish the schema
5. Open WSP again and add the new attributes to the appropriate detail forms.
6. Open CA SDM and define an Activity Association for the additional attributes.
7. Test your changes.
   For example, open a previously-saved instance of the object and modify the affected attributes to verify that the appropriate activity logs appear.

Auto Assignment Tracing

In a complex auto assignment implementation, auto assignment may not make the decisions that were expected. Tracing can be enabled to help you understand the processing flow. Tracing is normally turned off but when turned on, numerous messages are written to the stdlog files in $NX_ROOT\log that describe the various decisions made by auto assignment.

Use caution when implementing this in a high-volume installation, as the number of messages generated could cause the log files to grow and eventually wrap. On very active systems, performance degradation may occur. Tracing is controlled with the pdm_logstat utility. The parameters used by this utility are case-sensitive. Be sure to enter them as shown.

To turn tracing on, run the following command on each CA SDM the server:

```
pdm_logstat  -f auto.pm milestone
```

To turn off tracing, run the following command on each CA SDM the server:

```
pdm_logstat  -f auto.pm
```

Create a Stored Query

CA SDM supports use of stored queries to produce two kinds of data:

- Scoreboard Queries let you configure the web interface scoreboard by adding counter fields for items of interest.
- KPI Queries let you retrieve historical information for a specified time period on the value of a counter for use in web-based reporting.

Stored queries apply to all service desk models. Stored queries are not intended to bring users to a new page.

Administrators define the stored queries that are available to users. You can use the predefined stored queries that are installed with CA SDM, or define your own. You can define stored queries by using the administrative function of the web interface.

Consider the following information about stored query definitions:

- A valid stored query clause is integrated into an appropriate SELECT statement and passed to the underlying DBMS engine for processing. To develop the SELECT statements, see the object definition files in the following directories:
  - Windows: installation-directory\bopcfg\majic directory
  - UNIX: $NX_ROOT/bopcfg/majic directory
- Stored queries use the object and attributes statements for building the SQL WHERE clause instead of the field names at the database level.
- CA SDM does not support Cartesian product joins for stored queries. To help ensure that your stored query does not produce a Cartesian product join, enter the following command appropriate for your system.
  - Windows: bop_cmd -f *installation-directory*\bopcfg\interp\bop_diag.frg "check_queries()"
  - UNIX: bop_cmd -f $NX_ROOT/bopcfg/interp/bop_diag.frg "check_queries()"

  Update any queries that are flagged as a result to avoid Cartesian product joins.
- The URL stored query is an option offered while creating stored queries. The URL stored query runs a query and returns numerical results that only work with Knowledge Management.

Stored queries are supported for the following:

- **Scoreboard Queries** -- Allow you to configure the Web Interface scoreboard by adding counter fields to monitor items of interest.
- **KPI Queries** -- Allow you to retrieve historical information for a specified time period on the value of a counter for use in web-based reporting.

- **Automated Policy Queries** -- Allow you to retrieve information about the documents that are flagged for correction and promoted to publication or retirement during the various stages of the document lifecycle.

You can create stored queries for use in configuring the Scoreboard, or defining KPIs, or both.

Note: When you save a stored query, validation testing is performed on parameters. If you attempt to save a stored query with an invalid parameter (for example, datespan @cnt, @root) the save fails and an error message appears.

Follow these steps:

1. Click CA SDM, Application Data, Stored Queries on the Administration tab.
   The Stored Query List appears.

2. Click Create New.
   The Create New Stored Query page appears.

3. Complete the stored query fields (see page) as appropriate.

4. Click Save.
   The Create Stored Query Detail page displays your entries.

Stored Query Fields

You can use the fields on the Stored Query pages to define and edit query definitions.

Note: If you are using multi-tenancy, a tenant column appears on the list page.

The following fields require explanation:

- **Code**
  Defines a unique identifier for the stored query.

- **Scoreboard Usage**
  Specifies whether the query is available for configuring the Scoreboard.

- **KPI Usage**
  Specifies whether the query is available for configuring a KPI

- **Record Status**
  Specifies whether the stored query is active or inactive.

- **Type**
  Specifies the type of CA SDM object for which the stored query produces data (Contact, Request, Change Order, and so on).

- **Label**
  Defines the text string to be displayed on the Stored Query List page.

- **Where Clause**
  The SQL WHERE clause for the query. A WHERE clause includes a comparison predicate, which restricts the number of rows returned by the query.

Manage Roles

Contents

Roles are the primary records that control CA SDM security and user interface navigation. Each role defines a focused view of the system by exposing only the functionality necessary for users to perform the tasks typically assigned to the role they perform within their business organization.

A user's default role determines the system view that is presented upon login. Users with multiple role assignments can switch from one role to another to see different views of the system without having to log out and log back in again.

Predefined Roles

You can use the predefined roles in their default configuration, modify them to meet your business requirements, or create new roles.

The following table describes the predefined roles installed with CA SDM. These roles are designed to align with ITIL v3 best practices, and thereby reduce the amount of site-specific modifications required to bring your IT organization into ITIL compliance.

CA SDM only supports ITIL, and the CA SDM documentation is ITIL-oriented. For more information, see ITIL Configuration.

Role Type	Role Name	Description
End Users	Configuration Viewer	Performs basic CI viewing and research tasks from inside your organization.
	Customer	Performs basic self-service tasks from outside your organization.
	Employee	Performs basic self-service tasks from inside your organization.

Role Type	Role Name	Description
Analysts	Configuration Analyst	Performs tasks within the configuration item life cycle process and second-line CMDB support within your organization.
	Customer Service Representative	Supports users external to your organization, most often customers.
	Knowledge Analyst	Performs tasks within the knowledge management life cycle process.
	Level 1 Analyst	Provides first-line support within your organization.
	Level 2 Analyst	Provides second-line support within your organization, which requires more advanced subject matter expertise.
	Support Automation Analyst	Provides first-line support within your live assistance environment.
	Vendor Analyst	Supports a limited segment of your IT environment from outside your organization, such as vendor-specific hardware.
Managers	Change Manager	Manages the change order process, but typically not the analysts who work on change order tickets.
	Customer Service Manager	Manages Customer Service Representatives and the external support process.
	Incident Manager	Manages the incident process, but typically not the analysts who work on incident tickets.
	Knowledge Manager	Supervises Knowledge Analysts, knowledge document reassignments and escalations, and day-to-day knowledge administration.
	Problem Manager	Manages the problem process, but typically not the analysts who work on problem tickets.
	Service Desk Manager	Handles escalations and supervises Level 1 Analysts. Also may manage overall service desk operations.
Administrators	Administrator	Performs administrative tasks throughout your CA SDM and Knowledge Management implementation. This role typically installs, configures, and integrates the products.
	Configuration Administrator	Performs administrative tasks related to your CA CMDB implementation. This role typically administers CMDB and configuration item infrastructure and data structures.
	Knowledge Management Administrator	Configures and monitors knowledge management settings.
	Service Desk Administrator	Performs administrative tasks on data and processes, such as creating and updating categories, contacts, service types, root causes, and so on.
	Support Automation Administrator	Performs administrative tasks related to your Support Automation environment, such as configuring queues and analyst tool permissions.

Role Type	Role Name	Description
	System Administrator	Performs administrative tasks related to your CA SDM implementation, configuration and adaptation, such as setting options, configuring integrations and modifying web forms.
	Tenant Administrator	Performs multi-tenancy administrative tasks specific to a particular tenant or supporting organization.

Create a Role

Roles are the primary records that control security and user interface navigation. Each role defines a focused view of the system by exposing only the functionality necessary for users to perform the tasks typically assigned to the role they perform within their business organization.

Predefined roles are provided that are designed to align with ITIL v3 Best Practices and thereby reduce the amount of site-specific customization required to bring your IT organization into ITIL compliance. You can use the predefined roles in their default configuration, modify them to meet your business requirements, or create new roles.

Administrators can create roles to meet site-specific business requirements.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. Select Security and Role Management, Role Management, Role List on the Administration tab.
2. Click Create New.
3. Complete the following fields:
   - **Code**
     Specifies the code that identifies the role to the system.

     Note: After you save the record, this field value cannot be changed.

   - **Record Status**
     Indicates whether the role is Active or Inactive.
   - **Default?**
     Indicates whether this role is the default role.
   - **Customization Form Group**
     Specifies a predefined or custom form group.

- **Preferred Document**
  Specifies the document used by this role for entering tickets into the system.

Click Save.
The role definition is saved and the Role Detail page appears.

4. Update the information in the role tabs (see page).

Role Tabs

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

The following tabs are available on the Role Detail and Update Role pages:

- **Authorization**
  Allows you to define the authorization level assigned to the role. Complete the following fields as appropriate:

  - **Grant Level**
    Specifies the access permission that users assigned to this role can grant to others. The grant level is used to determine which access types a user can grant to another user. You can assign an access type to the contact record of another user only if the access level of the access type you are attempting to assign is ranked the same as or lower than the grant level for your own access type. These levels are ranked as follows:

    - Admin (highest)
    - Analyst
    - Cust/Emp
    - None (lowest)

  - **View Internal Logs?**
    Allows users assigned to this role to view internal log files.

  - **Data Partition Name**
    The name of the data partition assigned to this role. Data partitions are subsets of the database with restricted access to data records, based on their content. You restrict that access by defining a set of constraints for each data partition.
    Enter the data partition name directly into the field, or click the search icon to search for a data partition name.

  - **Override Contact Data Partition?**
    Select this option if you want the data partition defined for the access type to override the data partition defined on the contact record. This option can help prevent conflicts from arising between data partitions specified on the contact records and data partitions specified on the role record.

- **Multi-Tenancy Settings**
  The following options apply to systems where multi-tenancy is enabled:
  Update Public (Service Provider only)
  Select this option if you want users that are assigned to this role to update data for all tenants and non-tenanted data.
  Tenant Access
  Select the tenant or tenant group that you want users assigned to this role to be able to read. If you select Single Tenant, you can enter the name of the tenant that you want this role to read. You can assign the following associations to roles:

  - **Same As Tenant Access (Tenant Write Access Only)**
    Sets Tenant Write Access to be the same as the Tenant Access setting. Default for Tenant Write Access and only valid for Tenant Write Access.

  - **All Tenants**
    Removes tenant restrictions. CA SDM allows a user in a role with this access to view any object in the database (read access) or create and update (write access) any tenanted object in the database. When users with All Tenant access create an object, CA SDM requires that they select the tenant of the new object.

  - **Single Tenant**
    Sets a role's tenant access to a named tenant. When this option is selected, a second field appears on the web UI that allows selection of a specific tenant. CA SDM restricts a user in a role with this access to view (read access) or create and update (write access) only those objects associated with the named tenant. This selection is valid for either Tenant Access or Tenant Write Access.

  - **Tenant Group**
    Sets a role's tenant access to a user-defined or system-maintained tenant group. When the Tenant Group option is selected, a second field appears on the web UI that allows selection of a specific tenant group. CA SDM restricts a user with the role to view (read access) or create and update (write access) only those objects associated with one of the tenants in the group. When a user with tenant group access creates an object, CA SDM requires that they select the tenant for the new object. This selection is valid for either Tenant Access or Tenant Write Access.

  - **Contact's Tenant**
    Sets a role's tenant access to the tenant of the contact using it. CA SDM restricts a user in a role with this access to view (read access) or create and update (write access) only those objects associated with their own tenant. This selection is valid for either Tenant Access or Tenant Write Access.

  - **Contact's Tenant Group (Analyst Only)**
    Sets an analyst's role access to the tenant group that the analyst works with, as specified on the analyst's contact record. If the user with the role is not an analyst, this selection has the same effect as Contact's Tenant. It is valid for either Tenant Access or Tenant Write Access.

  - **Contact's Subtenant Group**
    Sets a role's tenant access to the Subtenant group of the contact using it. CA SDM restricts a user in a role with this access to view (read access) or create and update (write access) only those objects associated with their own Subtenant group. This selection is valid for either Tenant Access or Tenant Write Access.

- **Contact's Supertenant Group**
  Sets a role's tenant access to the Supertenant group of the contact using it. CA SDM restricts a user in a role with this access to view (read access) or create and update (write access) only those objects associated with their own Supertenant group. This selection is valid for either Tenant Access or Tenant Write Access.

- **Contact's Related Tenant Group**
  Sets a role's tenant access to the Related Tenants Group of the contact using it. CA SDM restricts a user in a role with this access to view (read access) or create and update (write access) only those objects associated with their own Related Tenants Group. This selection is valid for either Tenant Access or Tenant Write Access.

All users can view public data, regardless of their current role's access rights. The Update Public check box controls whether a service provider user in the role has the authorization to create or update public data. Tenant users (users belonging to a tenant other than the service provider) cannot update public data, regardless of their role.

- **Tenant Write Access**
  Select the tenant or tenant group that you want users assigned to this role to be able to create and update. If you select Single Tenant, an additional field displays where you can enter the name of the tenant you want this role to access.

  Note: Either the Tenant Access or Tenant Write Access fields can be set to Contact's Tenant Group to reference the Analyst's Tenant Group on the Contact Detail page. If a user that is not an Analyst, or an Analyst with no Analyst's Tenant Group defined, uses a role with this access, their access is Contact's Tenant.

- **Support Automation Access**
  Defines the appropriate Support Automation access for this role.

- **Function Access**
  Allows you to define the role's access to each functional area.

- **Web Interface**
  Allows you to configure the web interface for the role by defining the web pages and online help content the users can access. Complete the following fields as appropriate:

  - **Web User Interface Type**
    The kind of Web Interface that used to present the product features. Most of the predefined roles use the Analyst interface. The Customer and Employee roles are assigned a restricted interface type because they are not allowed access to analyst, management, and administrative functionality.

  - **Web Initial Form**
    The initial web form that appears for this role.

    Important! This must be set to menu_frames_role.htmpl in order for role-based functionality to be active. Changing the name of this form to anything else negates the role-based functionality.

- **Help View**
  The name of the help set that appears for this role. Enter the name of the help set directly or click the search icon to select the help set from a list.

  Note: The list of available help sets is based on the web user interface type selected in the role. Only active help sets belonging to that interface type are available for selection. If you do not select the web user interface type before selecting the help view, no help sets are available for selection.

- **Knowledge Management**
  Allows you to specify the Knowledge Management privileges for the role. Fill in the following fields as appropriate:

  - **Open Issue/Request**
    Allows the role to open an issue and request.
  - **Open Issue/Request based on Document**
    Allows the role to open an issue and request based on a Knowledge Document.
  - **Bypass Approval Process**
    Allows the role to bypass the knowledge approval process.
  - **Change Approval Process Template**
    Allows the role to change the approval process template.
  - **Add, Edit, Copy and Paste Categories**
    Allows the role to manage Knowledge Categories.
  - **Delete Multiple Categories and Documents**
    Allows the role to delete parents and child categories and documents.
  - **Delete Category**
    Allows the role to delete a Knowledge Category.
  - **Create Document**
    Allows the role to Create a Knowledge Document.
  - **Create Document with Attachments**
    Allows the role to create a document with attachments.

    Note: If this option is disabled, the Attach File and Attach File from Library buttons do not appear for that role.

  - **Delete Knowledge**
    Allows the role to delete knowledge documents, forums and files.

- **View Forum**
  Allows the role to view forums.
- **Create Forum**
  Allows the role to create a forum.
- **Reply Forum**
  Allows the role to reply to a forum.
- **Edit Forum**
  Allows the role to edit a forum.
- **View File**
  Allows the role to view files.
- **Edit File**
  Allows the role to edit files.
- **View External Repository**
  Allows the role to view the external repository.
- **View Related Tickets**
  Allows the role to view related support tickets.
- **Add Bookmark**
  Allows the role to add bookmark to My Bookmarks.
- **Use Preferences**
  Allows the role to use preferences.
- **Allow Export**
  Allows the role to export knowledge packages.
- **Allow Import**
  Allows the role to import knowledge packages.

- **KT Document Visibility**
  Allows you to specify which document statuses the role is allowed to view (for example, draft, retired, and published).
- **Tabs**
  Allows you to define the tabs that appear when a user assigned to this role is logged in.

Important! Include *only* tabs that contain forms that are in the form group assigned to the role you are creating or editing. For example, assigning the Customer tab or Employee tab to the Administrator role causes an error when users attempt to access that tab. Including more tabs than your browser window can display causes some tabs to be inaccessible to the user.

Note: The role's form group is specified in the Customization Form Group field on the Role Detail page, and is also displayed in the Form Group column on the Role List page.

- **Report Web Forms**
  Allows you to define the report web forms that are available to this role.

- **Go Resources**
  Users can search for items in by a number, name, or ID. In the upper right-hand corner of the main window, there is a drop down list containing the searchable record types. These searchable record types are referred to as "go" resources. Allows you to specify which record types appear in the Go drop-down list for the role.

How to Implement a Custom Role

For many sites, the predefined roles are sufficient. There may be situations, however, when you want to create a custom role and tailor it to meet site-specific business needs within your organization.

The following process outlines the tasks required in implementing a new role. The example shown here describes how you might implement a role for a small group of analysts tasked with reviewing and authorizing change order tickets.

Follow these steps:

1. Create a new role record using the following field values:
   - **Role Name**
     Change Analyst
   - **Code**
     chg_anal
   - **Customization Form Group**
     Analyst
   - **Preferred Document**
     Incident
2. Select Service Desk Analyst in the Data Partition field on the Authorization tab.
3. Select the Modify in the Change Orders field on the Function Access tab.
4. Enter the following values on the Web Interface tab:
   - **Web User Interface Type**
     Analyst
   - **Help View**
     Change Analyst
5. Select the following tabs:
   - Reports tab - Change Analyst

- Service Desk tab - Change Analyst
- Change Calendar tab

6. Select the following reports on the Report Web Forms tab:
   - Active Change Orders Aging by Priority for Status
   - Active Change Orders at Weeks End
   - Change Orders by Failed Service Type for Change Categories
7. Add the Change Order resource on the Go Resources tab.
8. Create a custom help set named Change Analyst that includes all content appropriate for the new role.
   For more information, see Create and Publish a Help Set (see page).
9. Create the following custom tabs using features appropriate for the new role:
   - Reports tab - Change Analyst
   - Service Desk tab - Change Analyst
10. Create a custom menu tree that includes all nodes appropriate for the new role.
    For more information see How to Implement a Custom Menu Tree (see page 1178).

Switch Roles

Roles define the system functionality each user can access. Depending on your assigned role, a specific set of menus, tabs, and toolbar controls are presented when you log in in the Web Interface client. For example, administrative roles have access to the Administration tab, while analyst and manager roles typically do not.

Some users are allowed to access multiple roles, enabling them to switch from one view of the system to another. If you are assigned multiple roles, you can switch between them at any time without having to log out and back in again.

Follow these steps:

1. Select the desired role from the Role drop down list in the upper right corner of the main page of the Web Interface.
2. Click Set Role.

   The Web Interface and available functionality change to match the new role setting.

Create Help Sets

Help sets are the collections of online help topics available to users depending on their role assignments and current role setting. If you log in using the Administrator role, for example, you can view the online help topics included in the Administrator help set. If you switch to the Employee role, you can view the Employee help set.

Each predefined role has a corresponding predefined help set. You can create custom help sets for any custom roles you might define.

You can create custom help sets for any custom roles you might define.

Follow these steps:

1. Select Security and Role Management, Role Management, Help Sets on the Administration tab.

2. Click Create New.

3. Complete the following fields:

   - **Help Set Name**
     The unique name of this help set.

   - **Interface Type**
     The interface type of the help set (such as Analyst, Employee, or Customer).

   - **Record Status**
     Indicates whether the help set is Active or Inactive.

   - **File Name Prefix**
     The prefix you want to attach to the help files generated for this help set. Do not include spaces in the name.

     Note: Assign a prefix that allows you to identify the files belonging to this help set. For example, you may want to use ANAL for an analyst's help set prefix.

   - **Internal**
     This is automatically set to NO for user-defined help sets. The value in this field cannot be changed.

4. Click Save.

5. Click Define Content and select the content you want to include in the help set.

6. **Important!** Some topics are required, and are included in your new help set regardless of whether you select them. For example, the CA SDM home page and other front matter topics are always included. Also, nested topics are dependent on their container topics. Container topics are included automatically if you include any of their nested topics. For example, if you select the "Use the Scoreboard"

topic, the container topic "Navigate CA SDM" is included when you publish the help set. If you edit the contents of an existing help set by adding or removing topics, you may not see your content changes reflected in the help set's table of contents until you clear your browser cache. See your browser documentation for information on how to clear the cache

7. Click OK.
   The Selected Help Update window closes and the content is listed on the Contents tab.

8. Click Publish.
   This generates the help set by packaging the selected topics into a help system you can display in a web browser.

9. Wait a few moments for the publishing process to complete; then select View, Refresh on the menu bar.
   The View Help button becomes active.

10. Click View Help.
    The custom help set appears in your default web browser.

How to Manage Roles Using Menu Trees

Contents

You can manage roles using the menu trees, implementing a custom menu tree, and copying a menu tree.

Menu Trees

Menu trees are the hierarchical listings of nodes (menu tree resources) that are displayed in the navigation pane on the left-hand side of the main web interface window. Menu tree resources define the items users can access from the menu tree. A menu tree resource consists of a name, description, and a URL fragment or HTMPL filename used by the web engine that controls the web page displayed.

A role can have a menu tree, which provides nodes for access to many functional areas of the system. For example, the predefined Administrator role has a menu tree that includes nodes to the System and Role Management administration features, Service Desk administration features, and many others.

For roles that include a menu tree, the menu tree provides access to a specified set of resources that provide access to functional areas of the system.

CA SDM provides predefined menu trees for the following roles:

- Administrator (admin_tree)

- CA CMDB Administrator (cmdb_adm_tree)
- Knowledge Management Administrator (kt_adm_tree)
- Knowledge Manager (kt_mgr_tree)
- Support Automation Administrator (sa_admin_tree)
- Service Desk Administrator (sd_adm_tree)
- System Administrator (sys_adm_tree)
- Tenant Administrator (tn_admin_tree)

You can edit the Name, Record Status, and Description fields of the predefined menu tree records, but you cannot modify them by adding or removing their menu tree resources.

To produce a custom a menu tree, you can create new menu tree record or copy and modify one of the predefined menu trees.

Note: The non-modifiable Internal field on each menu tree record indicates whether the menu tree can be modified. A value of YES in the Internal field indicates a predefined menu tree, which cannot be modified. A value of NO indicates a site-defined menu tree, which can be modified. The Customize Menu button appears only on menu tree detail records with an Internal field value of NO.

When you attach a menu tree to a tab, it becomes available for all roles that have access to that tab.

How to Implement a Custom Menu Tree

For many sites, the predefined menu trees are sufficient. There can be situations, however, when you want to configure a role by implementing a custom menu tree for it.

In most cases, it is easier to start with a copy of a predefined menu tree and then add, remove, or reorganize nodes within the hierarchy. Alternatively, you can create a menu tree and construct an all new hierarchy of nodes.

You can use either of the following methods to make custom menu tree available to a role:

- Replace the menu tree in the web form (Start Page) for the tab that shows the original admin_tree.
- Create a web form and attach the new web form with the new menu tree to a tab.

Follow these steps:

1. Copy one of the predefined menu trees.

Note: Make a note of value you enter in the Code field.

2. Create a web form using the following field values:
   - **Type:** HTMPL
   - **Resource:**

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMPL=admin_main_role.htmpl+KEEP.tree_code=menu_tree_code
```

   Note: Specify the value of the code for the menu tree you created in Step 1 for menu_tree_code. The admin_main_role.htmpl code uses the value of the KEEP. tree_code variable as its menu tree.

3. Create a tab record using the following field values:
   - **Starting Page:** The web form you created in Step 2
   - **Menu Bar:** Administration

   Note: Administration is a generic menu bar used by many roles; it is not role-specific.

4. Assign the tab you created in Step 3 to the role you want to have access to the custom menu tree.
5. Log out of CA SDM and log back in again.
   The Administration tab displays your custom menu tree.

Copy a Menu Tree

You can copy an existing menu tree to use as a starting point for a modified menu tree.

Follow these steps:

1. Select Security and Role Management, Role Management, Menu Trees on the Administration tab.
   The Menu Tree List page appears.
2. Click the Menu Tree to copy.
   The Menu Tree Detail page appears.
3. Click File, Copy.
   The Create New Menu Tree page appears.

4. Complete the following fields:

   - **Menu Tree Name**
     (Required) Specifies the name you assign that identifies this menu tree.

   - **Code**
     (Required) Specifies the code that identifies the menu tree to the system. After the code is defined, it cannot be changed.

   - **Record Status**
     Indicates whether this menu tree is active or inactive.

   - **Description**
     Describes the menu tree. The description can be used to give additional details about the menu tree and the roles that use it.

   Click Save.
   The Menu Tree Detail page for the new menu tree appears.

5. Click Customize Menu.
   A copy of the original menu tree appears.

6. Modify the menu tree as you want.

Create and Format a Menu Tree

You can create and format menu trees, based on one of the default menu trees provided.

Follow these steps:

1. Select Security and Role Management, Role Management, Menu Trees on the Administration tab.

2. Click Create New. The following fields require explanation:

   - **Menu Tree Name**
     (Required) The name you assign that identifies this menu tree.

   - **Code**
     (Required) The code that identifies the menu tree to the system. Once the code is defined, it cannot be changed.

   - **Record Status**
     Indicates whether this menu tree is active or inactive.

3. Click Save.

4. Click Customize Menu.
   A form appears, allowing you to modify the menu tree. At this point, the menu tree contains only a top node with the text you entered as the menu tree name.

5. Right-click the node in the menu tree and select Create New Node.
   The following fields require explanation:

   - **Node Name**
     Enter a name for the node. This is the name that appears in the menu tree.

   - **Description**
     Enter a description for the node. This description can be used to further define the purpose of the node.

   - **Resource**
     Enter the resource name directly in the field, or click the search icon to select the resource from a list. The menu tree resource determines the action to perform when the user selects the node from the menu tree.

6. Repeat steps 4 and 5 as many times as necessary to create the set of nodes you want to appear in the menu tree.

7. Click Save.
   The menu tree definition is saved and the Menu Tree Detail page appears.

Create a Menu Tree Resource

Menu tree resources are the items users can access from the left pane of one of the tabs. A menu tree resource consists of a name, its description, and a URL fragment or HTMPL filename used by the web engine that controls the web page displayed.

You can create your own menu tree resources to configure the user access points available from the left pane of a tab.

Follow these steps:

1. Select Security and Role Management, Role Management, Menu Tree Resources on the Administration tab.

2. Click Create New.

3. Fill in the following fields and click Save:

Name

The name displayed in the menu tree in the left pane of the tab. This is a required field.

Status

Indicate whether the resource is active or inactive. This is a required field.

Description

The description of the resource. The description can be used to further define the purpose of the resource.

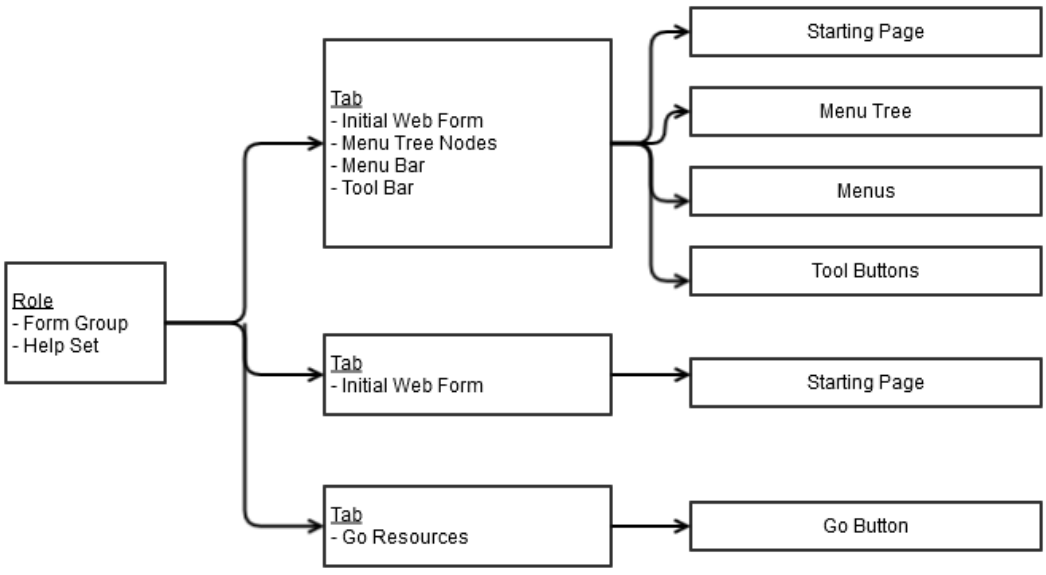
Resource

The action performed when the user selects the resource from the menu tree. This can be the name of the form that is displayed or the search operation that is performed.

How Role-Based Navigation Works

Contents

Each user's view of the web interface is defined by a role. Users with multiple role assignments can switch to multiple web interface views. The following diagram shows how roles interrelate with other objects to produce a role-based presentation of the user interface:



Create a Tab

A tab is a graphical display entity that links to a role in order to present features to the users of that role. When a user logs in to the system, the main window displays the tabs assigned to the user default role.

Tabs define major subdivisions in the web interface main window. Each tab is configured to expose an appropriate set of user interface features to the role or roles that use it.

All roles must have at least one tab. You can associate one or more tabs with a role. Each tab has a sequence number that controls its display order in the main window. If only one tab is associated with a role, the tab starting page is displayed and not the tab.

You can configure tabs to include the following kinds of display features:

- A starting page (default web form) that is displayed when a user selects the tab. The starting page is a required element of all tabs. You can assign only one starting page to each tab.

  Note: You can configure a starting page to display graphical reports from Business Object, which enables users to generate reports at run time. For more information, see CA Business Intelligence Reporting documentation.

- A menu bar, which presents drop-down lists of commands, such as File, View, and Search commands. The menu bar is optional. You can assign only one menu bar to each tab.

- A toolbar, which presents tool buttons for easy access to frequently used menu commands. The toolbar is optional.

CA SDM provides several predefined tabs. You can assign the predefined tabs to a role, modify the predefined tabs, and create custom tabs.

Important! Do not assign more tabs than your browser window can display; doing so causes tabs with higher sequence numbers to extend beyond the window viewable display area and make them inaccessible to the user.

Important! Include only tabs that contain forms that are included in the form group that is assigned to the role you are creating or editing. For example, do not assign the Customer tab or the Employee tab to the Administrator role; doing so causes an error when users attempt to access that tab. The role form group is specified in the Customization Form Group field on the Role Detail page, and is also displayed in the Form Group column on the Role List page. For a list of the web forms in each form group, see Form Groups.

You can create your own tabs to display on the main page. You can then define the tabs that display when users of different roles log into the system.

Follow these steps:

1. Select Security and Role Management, Role Management, Tabs on the Administration tab.
2. Click Create New.
3. Fill in the tab fields (see page) as appropriate and click Save.

Tab Fields

Code

The code that identifies this tab to the system. After you save the tab record, the code cannot be changed.

Record Status

Indicates whether the tab is active or inactive.

Display Name

The name of the tab that is displayed to users.

Starting Page

The initial web page that appears in the main window when a user selects this tab. The starting page and menu bar must belong to the same form group. Defining a tab with a starting page and a menu bar that belongs to different form groups causes an error when users access the tab.

Menu Bar

The menu bar that appears in the main window when a user selects this tab.

Predefined Tabs

The following table shows the predefined tabs that are assigned to each role. The tabs are listed in sequence number order, indicating their left-to-right position in the window.

Note: In many cases, there are multiple versions of tabs with the same display name. For example, the Service Desk tab for the Administrator role provides full access to CA SDM functionality, while the Service Desk tab for the Change Manager role is more focused on change orders.

Role	Tabs
Administrator	Service Desk tab with full menu and scoreboard Knowledge tab Administration tab with full menu tree Reports tab - Administrator Change Calendar tab CA CMDB tab Support Automation tab
Change Manager	Reports tab - Change Manager Service Desk tab - Change Manager Change Calendar tab
Configuration Administrator	CA CMDB tab Administration tab - Configuration Administrator

Role	Tabs
Configuration Analyst	CA CMDB Scoreboard - Configuration Analyst
Configuration Viewer	CA CMDB Scoreboard - Configuration Viewer
Customer	Customer tab
Customer Service Manager	Service Desk tab - Customer Service Manager Knowledge tab Reports tab - Customer Service Manager
Customer Service Representative	Service Desk tab - Customer Service Rep Quick Profile tab Knowledge tab
Employee	Employee tab
Incident Manager	Reports tab - Incident Manager Service Desk tab - Incident Manager Knowledge tab
Knowledge Analyst	Service Desk tab - Knowledge Analyst Knowledge tab Knowledge Management Schedule Knowledge Report Card tab Reports tab - Knowledge Analyst
Knowledge Manager	Service Desk tab - Knowledge Manager Knowledge tab Knowledge Management Schedule Administration tab - Knowledge Manager Knowledge Report Card tab Reports tab - Knowledge Manager
Knowledge Management Administrator	Administration tab - Knowledge Administrator
Level 1 Analyst	Service Desk tab - Level 1 Analyst Quick Profile tab Knowledge tab
Level 2 Analyst	Service Desk tab - Level 2 Analyst Knowledge tab Change Calendar tab
Problem Manager	Reports tab - Problem Manager Service Desk tab - Problem Manager Knowledge tab
Service Desk Administrator	Administration tab - Service Desk Administrator
Service Desk Manager	Reports tab - Service Desk Manager Service Desk tab - Service Desk Manager Knowledge tab Change Calendar tab
Support Automation Administrator	Service Desk tab - Level 1 Analyst Support Automation tab Support Automation Admin Quick Profile tab Knowledge tab
Support Automation Analyst	

Role	Tabs
	Service Desk tab - Level 1 Analyst Support Automation tab Quick Profile tab Knowledge tab
System Administrator	Administration tab - System Administrator
Tenant Administrator	Administration tab - Tenant Administrator
Vendor Analyst	Service Desk tab - Vendor Analyst

Create a Web Form

Web forms define the pages that appear in the CA SDM web interface.

There are four web form types:

- Business Object Report URL
- HTMPL page
- GO resource
- Custom (for example, a URL for a third-party web page)

Administrators can create web forms to be the starting pages for tabs, reports to display on tabs, "go button" resources, or another URL.

Follow these steps:

1. From the Administration tab, navigate to Security and Role Management, Role Management, Web Forms.
   The Web Forms List page displays.

2. Click Create New.
   The Create New Web Form page displays.

3. Complete the following fields:

   - **Web Form Name**
     (Required) Specifies the name that identifies the web form.

   - **Record Status**
     Indicates whether this form is active or inactive.

   - **Code**
     (Required) Specifies the code that identifies the web form to the system. After the code is defined, it cannot be changed.

     Note: This field specifies the web_form_name on the Properties tab for a multiframe form in Web Screen Painter.

- **Type**
  Specifies one of the following types of web form that you are creating:
  - **HTMPL page** -- Displays a web page to use as the starting page for one of the custom tabs you create.
  - **Report** -- Specifies a CA SDM report that displays on any tab.
  - **Go Resource** -- Specifies a "Go Button" resource.
  - **Other** -- Accesses any other external Web page through URL.
- **Description**
  Describes the web form. Use this description to further identify this web form, where it displays, and its purpose.
- **Resource**
  Specifies the code that calls the web form. This code can be command line code or a URL.
  Example: Open a simple htmpl form "menu_tab_dflt.htmpl":

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMPL=menu_tab_dflt.htmpl
```

Click Save.

Form Groups

Form groups define the sets of CA SDM web interface pages that are available to a role. Each role has one form group. Users can display only the web pages that are included in the form group that is assigned to their role.

Each interface type has an associated form group, a set of HTMPL files that define the pages displayed to the users.

CA SDM provides the following predefined form groups:

- Analyst
- Customer
- Employee
- ITIL

You can use the predefined form groups in their default configuration, modify the predefined form groups, and create new form groups using Web Screen Painter. You can view a listing of the HTMPL filenames included in each predefined form group.

Create a Menu Bar

A menu bar is a user interface element that displays a horizontal list of menus in the web interface main window. Each menu contains a drop-down list of options or commands. You can define custom menu bars for any custom roles you might create. Menu bar records specify the HTMPL form that controls the menu items that the menu bar can access.

Note: To define the functionality of the menu bar, you must use the Web Screen Painter application. For information about configuring the functionality of a predefined or custom menu bar, see the *Web Screen Painter Online Help*.

The following table lists the predefined menu bars and identifies the predefined tabs that use them.

Menu Bar	Associated Tabs
Administration	Administration tab - Configuration Administrator Administration tab - Knowledge Administrator Administration tab - Knowledge Manager Administration tab - Service Desk Administrator Administration tab - System Administrator Administration tab - Tenant Administrator Administration tab with full menu tree
CA CMDB	CA CMDB tab with full menu and scoreboard
Change Calendar	Change Calendar tab
Knowledge	Knowledge tab Knowledge Management Schedule
Service Desk	Service Desk tab with full menu and scoreboard
Service Desk-Change Manager	Service Desk tab - Change Manager
Service Desk-Cust Service Mgr	Service Desk tab - Customer Service Manager
Service Desk-Cust Service Rep	Service Desk tab - Customer Service Rep
Service Desk-Incident Manager	Service Desk tab - Incident Manager
Service Desk-Knowledge Analyst	Service Desk tab - Knowledge Analyst
Service Desk-Knowledge Manager	Service Desk tab - Knowledge Manager
Service Desk-Level 1 Analyst	Service Desk tab - Level 1 Analyst
Service Desk-Level 2 Analyst	Service Desk tab - Level 2 Analyst
Service Desk-Problem Manager	Service Desk tab - Problem Manager
Service Desk-Service Desk Mgr	Service Desk tab - Service Desk Manager
Service Desk-Vendor Analyst	Service Desk tab - Vendor Analyst
Support Automation-Analyst	Support Automation tab - Support Automation Analyst

You can create your own menu bars to control the access to system functionality for your user-defined roles.

Follow these steps:

1. From the Administration tab, navigate to Security and Role Management, Role Management, Menu Bars.
2. Click Create New.
3. Fill in the menu bar fields (see page) as appropriate.
4. Click Save.

Menu Bar Fields

Code

The code that identifies this menu bar to the system. Once the code is defined, it cannot be changed. This is a required field.

Record Status

Indicates whether the menu bar is Active or Inactive.

HTMLP Name

The name of the HTMPL form that contains the menu bar definition. The menu bar is actually designed using the Web Screen Painter.

Go Resources

The *Go* button provides an easy means of locating a particular record.

Go resources are a type of web form. If a role has associated Go resources, when a user logs in with that role the Go button appears in the upper-right corner of the main CA SDM window and in all popup windows. The Go button has two associated fields in the user interface:

- A drop-down list for selecting the type of record to search for (for example, Change Order)
- A text box for entering a value to identify a particular record (for example, 135 to locate Change Order 135)

By assigning Go resources to a role, you can specify the kinds of records users in that role can search for. For example, the predefined Administrator role has the following Go resources:

- Change Order
- Document by ID
- Incident
- Issue
- Knowledge
- Problem

- Request
- User by ID
- User by Name
- User by Phone

Toolbars

Toolbars extend the functionality of menu bars by adding the capability to display one or more tool buttons to the right of the menus.

Tool buttons appear as icons on the toolbar. Clicking a tool button gives the user easy access to frequently used menu options or commands.

Note: You can use the Web Screen Painter application to define the functionality of the toolbar. For more information, see Using the Web Screen Painter (WSP) (see page 1898).

Create a Functional Access Area

Functional access areas define the role level access to ticket records and other system components. The usp_functional_access_type table defines the area and the usp_functional_access_level tables describe user access.

Name	Code Name	New
Administration	admin	No
Incident/Problem/Request	call_mgr	No
Change Order	change_mgr	No
Inventory	inventory	No
Issue	issue_mgr	No
Knowledge Document	kd	No
Notification	notify	No
Reference	reference	No
Security	security	No
Announcement	announcement	Yes
Incident/Problem/Request Reference	call_mgr_reference	Yes
Incident/Problem/Request Template	call_mgr_template	Yes
Change Order Template	change_mgr_template	Yes
Change Order Reference	change_reference	Yes
Configuration Item	ci	Yes
Configuration Item Common Readonly	ci_common_ro	Yes

Configuration Item Reference	ci_reference	Yes
Contact	contact	Yes
Group	group	Yes
Issue Template	issue_mgr_template	Yes
Issue Reference	issue_reference	Yes
Location	location	Yes
Multisite Administration	multisite_admin	Yes
Multisite Reference	multisite_reference	Yes
Notification Reference	notification_reference	Yes
Organization	organization	Yes
Prioritization	prioritization	Yes
Service Level	service_level	Yes
Site	site	Yes
Stored Query	stored_queries	Yes
Support Automation	sa	Yes
Survey	survey	Yes
Tenant Admin	tenant_admin	Yes
Timezone	timezone	Yes
Workflow Reference	workflow_reference	Yes
Workshift	workshifts	Yes

When you add a functional access area, the existing roles automatically have Modify access. You can review and change the access levels to grant the appropriate authority.

Follow these steps:

1. On the Administration tab, select Security and Role Management, Functional Access.

2. Click Create New.
   The Create New Functional Access List page appears.

3. Complete the functional access area fields as appropriate. The Code field defines the CA SDM or site-defined object name. Objects can only map to one functional access area. However, one functional access area can manage multiple objects.

4. Click Save.
   The Functional Access Detail page appears.

5. Apply access levels to one (see page 1193) or more (see page 1191) roles.

Apply Access Levels to Many Roles

For a functional access area, you can set the access levels for every role to save time. Instead of using Role Management, you update the functional access area with the appropriate role access levels.

Follow these steps:

1. On the Administration tab, select Security and Role Management, Functional Access.
2. Click the name of the function area.
3. On the Roles Tab, click Edit in List.
4. Review and update each role as appropriate. The following access levels are available:
   - **None**
     Denies the role access to the function object.
   - **View**
     Grants read-only capability to the function object.
   - **Modify**
     Grants read/write access to the function object.
5. Continue selecting roles and choosing access levels.
6. (Optional) Click Change All.
7. Click Save.
   The changes for the roles apply immediately.

Example: Change the Access Levels for the Announcement

This example shows you can role access levels for the Announcement functional access area.

1. On the Administration tab, select Security and Role Management, Functional Access.
   The Functional Access Detail page appears.
2. Click Announcement.
3. On the Roles Tab, click Edit in List.
4. Select Level 2 Analyst.
5. Select View from the Access Level.
   The Access Level for the Level 2 Analyst role highlights with the value of View.
6. Select Configuration Analyst.
7. Select Modify from the Access Level.
   The Access Level for the Configuration Analyst highlights with the value of Modify.
8. Click Save.
   A message confirms the change.
9. Log in as a Level 2 Analyst role.

10. Select View Announcements.
    The Announcements page appears.

11. Click an announcement.
    A message reminds you that as a Level 2 Analyst, you can only view announcements.

12. Set the Role to Configuration Analyst.

13. Select View Announcements.
    The Announcements page appears.

14. Click an announcement.
    The Update Announcement page appears. As a Configuration Analyst, you can modify announcements.

Apply an Access Level to a Role

You can use Role Management to change the way users access the user interface. When you change the access levels for a role, the user interface shows only objects, pages, and menu items based on the access level. For example, if a role can no longer create contacts, the File menu omits New Contacts.

Follow these steps:

1. On the Administration tab, select the Security and Role Management, Role Management, Role List.

2. On the Role List, right-click the role name and select Edit from the short-cut menu.

3. Click Edit in List on the Function Access tab.

4. Click a function name.
   The row highlights.

5. Update the functional access areas with the following access levels as appropriate:

   - **None**
     Denies the role access to the function object.

   - **View**
     Grants read-only capability to the function object.

   - **Modify**
     Grants read/write access to the function object.

6. Click Save.
   A message confirms the change. The role can immediately use the functional access area at the specified access level.

7. Verify the access level, by logging in as the role and checking menus, page options, and buttons.

Example: Grant the Level 2 Analyst Role Modify Access to Tickets

This example shows how the user interface changes when you grant a Level 2 Analyst access to modify tickets.

1. On the Administration tab, select the Security and Role Management, Role Management, Role List.
   The Role List appears.

2. Right-click Level 2 Analyst and select Edit from the short-cut menu.

3. Click Edit in List on the Function Access tab.

4. Select Incident/Problem/Request Reference.

5. Select Modify on the Access Level.
   The access level updates to Modify.

6. Click Save and log out.
   A message confirms the change.

7. Log in as a Level 2 Analyst role.

8. Select Search, Incidents.

9. Click Search and open an incident.
   The Incident Detail page includes an Edit in List button. As a Level 2 Analyst, you can modify the ticket.

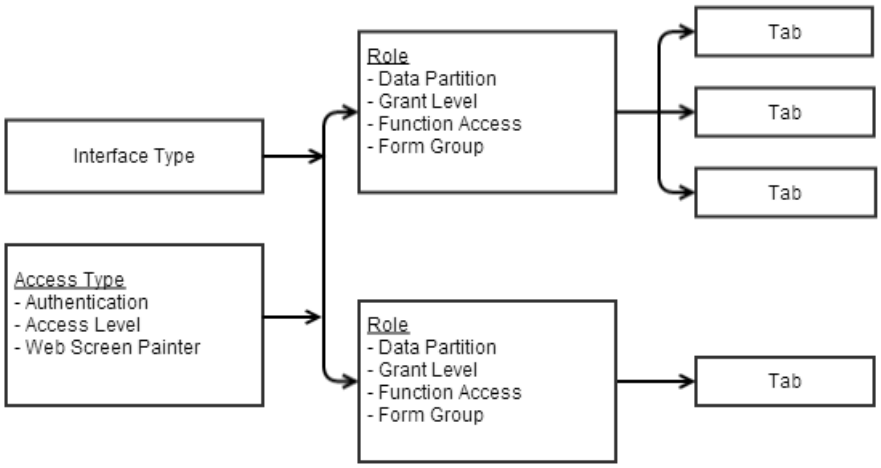
Role-Based Security

This article contains the following topics:

Access types and roles are the primary components you use to control CA SDM security.

The following diagram shows an overview of how roles interrelate with other system objects to provide role-based security.

Note: For more information about other aspects security, see Security (see page 1002).



How Access Types Work

Each access type for a user controls the following aspects of system behavior:

- How CA SDM performs web authentication when the user logs in
- The access level for the user
- Whether the user can modify web forms or the database schema using Web Screen Painter
- Which roles are available to the user

You can associate an access type with a contact by selecting the access type while creating or updating the contact record.

Note: The following table lists the predefined access types, identifies their linked roles, and gives a brief description.

Access Type	Linked Roles	Description
Administration	Administrator (default) Configuration Administrator Employee Level 2 Analyst Service Desk Administrator	Provides the highest level of security access to all key administration roles. Used during implementation and ongoing administration. **Note:** The Administration access type is preconfigured to allow administrators to switch to any of the linked roles. For example, to see a different view of the system, administrators can switch to the Employee role without having to log out and log in again.

Access Type	Linked Roles	Description
	System Administrator Tenant Administrator	
Customer	Customer	Provides highly restricted access to *external* customers who use the self-service view.
Employee	Employee	Provides highly restricted access to *internal* employees who use the self-service view. Used to create new incident and update incident pages.
IT Staff	Configuration Analyst Employee Level 2 Analyst (default) Knowledge Analyst Knowledge Management Administrator Knowledge Manager	Provides analyst-oriented access to users who work within your IT organization but are not actual members of the support team. This access is designed specifically for users who need access to Knowledge Management.
Knowledge Management	Configuration Administrator Configuration Analyst Configuration Viewer Employee Knowledge Analyst Knowledge Management Administrator (default) Knowledge Manager Level 2 Analyst	Provides administrative access tailored to users who administer Knowledge Management features.
Process Management	Change Manager Configuration Analyst Employee Incident Manager (default) Level 2 Analyst	Provides access tailored to users who perform key process management roles.

Access Type	Linked Roles	Description
	Problem Manager Service Desk Manager	
Service Desk Management	Customer Service Manager Configuration Analyst Employee Level 1 Analyst Level 2 Analyst Service Desk Manager (default)	Provides access tailored to users who manage IT support or external customer support functions (typically front-line support supervisors).
Service Desk Staff	Configuration Analyst Configuration Viewer Customer Service Representative Employee Level 1 Analyst (default) Level 2 Analyst	Provides access tailored to users who perform support tasks. Access is focused on those users that perform frontline support.
Support Automation Admin	Support Automation Administrator	Provides access to users that perform Support Automation administration.
Support Automation Analyst	Support Automation Analyst	Provides access to users that provide live assistance to end users.
Vendor Staff	Vendor Analyst	Provides highly restricted access to external vendors, who work only on items directly related to their product (for example, a particular brand of hardware).

Role Records

You can assign roles to an access type, or directly to a user contact record. If a role assignment conflict occurs, the contact role assignments take precedence.

Each role record must be configured with the following components:

- One form group
- One user interface type
- Function access settings
- One or more tabs
- One help set

The following optional components can also contribute to each role definition:

- Menu trees
- Scoreboards
- Menu bars
- Toolbars
- One data partition
- Knowledge Management access
- Support Automation access levels
- Report web forms
- Go resources

Data Partitions

Data partitions are subsets of the CA SDM database that enable you to control access at the record level. You can associate a data partition to a role to control access to tickets and other records accessible through the web interface.

For information about working with data partitions, see How to Set Up the Data Partition (see page 1281).

Configuring User Accounts

Contents

Configure the user accounts to set up contacts, contact types, groups, special handling types, LDAP data authentication, and communication.

Contacts

An important part of establishing a working service desk is defining the users who are going to access it. In CA SDM, users are named *contacts*, and you can perform several tasks to set up and manage them:

- Set up contacts manually.
- The Organize contacts into groups that define areas of responsibility.
- Create contact types to organize your CA SDM contacts into logical groupings.
- Import LDAP user information into a CA SDM contact record.
- Assign a contact to a role to define the accessible system functionality.
- Assign a special handling type, such as Very Important Person (VIP), to a contact.

Contact Definitions

Everyone who uses CA SDM must be defined as a contact. The contact record of a user defines the user information that the system needs as follows:

- **Basic Identification**
  Defines basic identification, such as the name of a user and contact type. The Contact name is used as the primary identifier when selecting a contact or filling in contact information in other contexts.
- **Login**
  Defines login information, such as the user ID and in some cases, a PIN field to use as a password that verifies the user upon login. The user ID is used to identify the user in the contact table for authentication purposes and for determining the access types assigned to the user. Depending on your security configuration, another field such as the contact ID, can be specified as the PIN field. The user can use the PIN as login password.
- **Security**
  Defines the access type that is assigned in their contact record or by a default access type, depending on how you set up the security for your system. In addition, the access type of a user can be assigned based on their membership in an LDAP Directory group.
  The user access type determines all aspects of security, including authentication, web interface they can view, and what product functionality they can access.
  Security management is a feature of the web interface.
- **Service Type**
  Determines the level of service a user receives. A service type defines the level of service a user can receive. The Service Level Agreements (SLAs) are negotiated with CA SDM customers. Service types serve as the mechanism for CA SDM to implement SLAs. As an Administrator, you can use service type to set up SLAs using the web interface.

- **Automatic Assignment**
  Defines automatic assignment information, such as work shift and availability (used for analyst contact types only). You can set up analyst contacts to determine if they are eligible for automatic assignment. The Automatic assignment is valid only for requests, and is defined as part of the request area definition. Automatic Assignment is also linked to the groups to which the analyst belongs.

- **How to Send Users Notification Messages**
  Defines the notification information of a contact for the following:

- - Various email addresses and telephone numbers to be used for notification

  - Method to be used for the notifications with different urgency levels

  - work shifts during which notifications are received
    The notification delay calculation takes the Contact Time Zone into account. If the Contact Time Zone is not set, the server time zone is used, instead. Using the server time zone may result in notifications firing at times, perceived to be outside the Work shift settings.
    Organizational information (such as location, organization, and department) lets you group contacts based on the organization to which they belong. For example, associating a contact with a location links the contact to a physical address and also helps in determining automatic assignment. The organization can be assigned a service type, making it easier to manage SLAs by organization rather than by individual contacts.

- **Groups to which a User Belongs**
  Organizes contacts into groups that represent specific areas of responsibility within your service desk. You can set up and can define contacts using the web interface.

Groups

A group is a collection of contacts that share a common area of responsibility. In CA SDM, groups are implemented using the predefined group contact type, making a group just a special type of contact. A group has the same basic information as a contact, with the important additional feature that groups are one of the keys to automatically assigning requests. You can associate request areas, locations, and a work shift with a group. These attributes are used to determine if and when the contacts in the group can accept the automatic assignment of a request.

Working with Special Handling Types

This article contains the following topics:

You can define special handling types that identify contacts who require special attention. You can use the special handling types that CA Service Desk Manager provides or create your own types. You can view and locate tickets that specify an affected end user who requires special attention. For example, analysts can browse the V.I.P. folder on the Scoreboard to identify tickets that specify a VIP as the affected end user.

The following examples are contacts that special handling types can identify:

- Very Important Persons (VIPs) such as executives
- Customers with support renewal in process
- Customers with disabilities requiring special handling or equipment
- Visitors
- Contacts suspected of misusing or abusing system resources

When one or more special handling types are assigned to a contact, tickets that specify the contact in the Affected End User field show an alert banner, icon, or both. You can use ticket fields and special handling types to track tickets, and distinguish between two related but possibly distinct contact types. For example, a VIP (Affected End User) has an assistant (Requestor) acting on their behalf. When the Affected End User is a contact assigned to a VIP special handling type, an analyst can prioritize tickets more accurately.

How to Configure Special Handling Contacts

To configure special handling contacts, do the following steps:

1. Create special handling types (see page).
2. Associate a contact to any number of special handling types (see page 1201). Similarly, a specia handling type can have many contacts.
   A contact that is associated with one or more Special Handling types is visually distinguished in the Contact Detail form and the Quick Profile browser using a banner at the top of each page. This banner displays the alert icon and alert text for each Special Handling type that is assigned to the contact.
   Additionally, any tickets that identify the contact as the Affected End User are indicated as follows:
   - Alert Icons and Alert text appear in a banner at the top of the ticket detail form.
   - Alert Icons appear in the ticket list.
   - The Scoreboard includes a V.I.P. folder and subfolders for each ticket type. The V.I.P. subfolders include tickets for affected end users who are VIP special handling contacts.

     Note: The V.I.P. Scoreboard folder displays for analyst roles.

Associate a Contact to a Special Handling Type

You can assign a special handling type to a contact to alert analysts about tickets that affect end users with special requirements, such as for a visually impaired person or a contact that poses a security risk.

To associate a contact to a special handling type, perform the following:

Follow these steps:

1. On the Contact Detail page, select the Special Handling tab.
   The Associated Special Handling List tab lists special handling types that are associated with the contact.

2. Click the Update Contact's Special Handlings button.
   The Search filter appears.

3. Search for the special handling type that you want to associate to the contact.
   The Special Handlings Update page appears.

4. Select one or more handling types from the left column and use the move button (>>) to move the types to the right column. Click OK.

   Note: You can remove an association from a contact by using the move button (<<) to move the type from the right column to the left column. You can click the search icon to search for the value you want.

   The contact is associated to a handling type.
   CA SDM displays the following depending on the handling type, when a ticket specifies the contact in the Affected End-User field:

   - An alert banner appears on the Contact Detail for the affected end user on a ticket.
   - Alert text appears as a banner at the top of the ticket detail page and in the Quick Profile.
   - Ticket lists highlight the contact row and show an alert flag.
   - A V.I.P. folder appears in the Scoreboard for analyst roles. The folder contains all tickets that are associated with contacts (Affected End Users) that have a VIP special handling type.

Special Handling Types Options

This article contains the following:

Create a Special Handling Type

You can associate contacts to special handling types. This association lets you easily view and locate contacts that require special attention, for example, to identify tickets in a list that specify Very Important Person (VIP), vision that is impaired, or visitor as affected end users. You can create special handling types and can associate them to contacts.

To create a special handling type, perform the following:

Follow these steps:

1. On the Administration tab, select Service Desk, Application Data, Codes, Special Handling Types.
   The Special Handling List page appears.

2. Click Create New.
   The Create New Special Handling page appears.

3. Complete the fields (see page) as appropriate, and click Save.

4. Click Update Special Handling Members.
   The Contact Search page appears.

5. Complete the search fields as appropriate and click Search.

6. Select one or more contacts from the Contacts column and use the move button (>>) to move the contacts to the Special Handling column. Click OK.

   Note: You can remove a contact from an association by using the move button (<<). Move the contact from the right column to the left column.

   The special handling type is created and it is associated with contacts.

7. Click Close Window.

Edit a Special Handling Type

You can edit special handling types that you can use to associate to contacts. For example, you can add contacts (members) to a special handling type.

To edit special handling types, perform the following:

Follow these steps:

1. On the Administration tab, select Service Desk, Application Data, Codes, Special Handling Types.
   The Special Handling List page appears and lists special handling types.

2. Click a name link.
   The Special Handling Detail page appears.

3. Click Edit.
   The Update Special Handling page appears.

4. Edit the fields (see page) as appropriate.

5. Select the Special Handling tab, and click Update Special Handling Membership.
   The Special Handling Search page appears.

6. Complete the page fields as appropriate, and click Search.
   The Special Handling Update page appears.

7. Use the move controls (>> and <<) to add or remove special handling type associations. Click OK.
   The special handling type is updated.

8. Click Save.
   The special handling type is updated.

Special Handling Types Fields

The following fields require explanation:

- Name
  Specifies the name of the special handling type, for example, VIP, Visually Impaired, Visitor, and so on.

- **Icon**
  Specifies the URL for the icon graphic that displays with the alert banner, for example, icon\visitor_icon.jpg, to display an alert banner. If you do not specify an icon URL, no alert icon appears on the ticket detail page. The format of the URL is http[s]://*server_name*:*server_port* /CAisd/img/icon_file. For example:

  ```
  http://server_name:8080/CAisd/img/glasses.gif
  ```

- **Escalate Urgency**
  Uses the special handling type to escalate the corresponding ticket priority.

- **Auto-Display Notes**
  Indicates whether the contact notes (ca_contact.comments) automatically display in an alert banner following the alert text banner when the affected user of the ticket is associated with the special handling type.

- **Alert Text**
  Specifies the text to display in an alert banner, for example, Visitor. If you do not specify text, no alert text or highlighting appears on the ticket detail page.

- **Description**
  Describes the special handling type, such as Very Important Person.

Add an Icon to a Special Handling Object

You can add an icon to a special handling object to identify the object. The icon file is located in the NX_ROOT/bopfg/www/wwwroot/img folder.

To add an icon to a special handling object, perform the following:

Follow these steps:

1. On the Administration tab, select Service Desk, Application Data, Codes, Special Handling Types.
   The Special Handling List page appears and lists special handling types.

2. Click a name link.
   The Special Handling Detail page appears.

3. Click Edit.
   The Update Special Handling page appears.

4. Specify the URL in the Icon field and click Save. The format of the URL is http[s]://*server_name*:*server_port*/CAisd/img/*icon_file*. For example:

   ```
   http://server_name:8080/CAisd/img/glasses.gif
   ```

   Note: The filename can be case-sensitive depending on the web server used. If the case is incorrect, the icon is not displayed.

   The special handling icon is added.

How to Identify Tickets for Special Handling Contacts

Special handling contacts are contacts that require special attention, for example, security-risk monitoring, a visitor badge, or requiring special equipment. You can identify tickets for which the affected end user is a contact that requires special attention. For example, you can identify tickets in a list that specify Very Important Person (V.I.P.), vision that is impaired, or visitor as affected end users.

To identify tickets for which the affected end user is a special handling contact, perform the following:

- Navigate the Scoreboard to ticket lists.
  Special handling contact rows are highlighted and show an alert flag.

- As an analyst, navigate the Scoreboard to the V.I.P. folder.
  The V.I.P. folder includes subfolders for each ticket type. The subfolders include tickets for affected end users who are VIP special handling contacts.

- Navigate the Scoreboard, open ticket Details, and click Quick Profile for the affected end user on a ticket.
  An alert banner appears on the page to identify contacts with special handling types.

  Note: An alert icon also appears if an alert icon is associated with the special handling type.

- Browse the Administration tab and open Contact Details.
  An alert banner appears on the page to identify contacts with special handling types.
  Note: An alert icon also appears if an alert icon is associated with the special handling type.

List Special Handling Types

You can list special handling types that you can use to associate to contacts.

To list special handling types

1. On the Administration tab, select Service Desk, Application Data, Codes, Special Handling Types.
   The Special Handling List page appears, lists special handling types, and corresponding information (see page).

2. (Optional) Click a name link.
   Details about the special handling type appear.

Contact Types

Contents

Contact types are used to categorize CA SDM users into logical groupings based on how they use the system. For example, some of the many contact types that are predefined by the system are analyst, customer, and group. These predefined contact types meet the needs of most CA SDM implementations; however, if your circumstances require it, you can modify the predefined contact types and create contact types. When you define users as contacts, you can associate a contact type with each one. You can base notification on contact type, which allows you to send a notification message to all contacts of a particular type.

You can select users based on contact type in various contexts. For example, most list and selection windows that display contacts have a search field where you can select a contact type as a search criterion.

Determine Behavior Based on Contact Type

The contact *type* determines which contacts display (and have permission) in different situations. For example, when you manually assign any type of ticket, such as a request or an issue, the field to specify the assignee requires that the person you specify have a contact type of analyst. If you choose to select a contact from a selection list for this field, only contacts with the type of analyst display in the selection list. Entering a contact with a different type displays the analyst search screen only.

Note: An important feature of the contact type is in the implementation of groups of contacts through the predefined group contact type.

How to integrate CA SDM with LDAP

Contents

Configure LDAP Options

You can configure CA SDM to access LDAP directory data.

Follow these steps:

1. Manually install LDAP options using the Web Interface Options Manager.

   Note: The options necessary for basic LDAP integration are identified as required in the Description column in the following table. Options identified as optional are features you can add only if all the required options are installed. The values you specify when installing these options are written to the $NX_ROOT/NX.env file.

2. Restart the CA SDM service.
   The changes take effect.

Manage LDAP Servers Using the LDAP Configuration Utility

You can use the LDAP Server utility to manage multiple LDAP servers. You can perform the following tasks by using the utility:

- Add a new LDAP server.
- Delete an LDAP server that you no longer want to use.

- View LDAP server details.
- Restart LDAP virtual database.

Important! In an advance availability configuration, run the utility on the background server. After you add a new LDAP server, restart the CA SDM services on all the standby servers.

Follow these steps:

1. (Optional) To specify the domain name of the default LDAP server, execute the following command:

   ```
   pdm_options_mgr -c -a pdm_option.inst -s LDAP_DOMAIN -v
   <Default_LDAP_DomainName>
   pdm_options_mgr -c -a pdm_option.inst -s LDAP_DOMAIN -v
   <Default_LDAP_DomainName> -t
   ```

   Configure the default LDAP server domain name in the following cases:

   - CA EEM server is configured with multiple Microsoft Active Directory domains.
   - Default LDAP server and any other LDAP server configured with CA SDM have the same user details.

   After the configuration is complete, the default LDAP users must log in to CA SDM in the format domain_name\userid.

2. Open the windows command and navigate to the location $NX_ROOT/bin.
3. Run the following command:

   ```
   pdm_perl pdm_ldap_config.pl
   ```

4. Based on the task that you want to perform, select the appropriate option.

Option	Default Value	Description
ldap_domain		Required for configuring mulitple LDAP servers. Specifies the domain name of the LDAP server.
default_ldap_tenant		Required for multi-tenancy installation. Specifies the default tenant assignment for contacts imported from LDAP. You must use the tenant UUID when setting the Option Value field. You can get the tenant UUID from a database query. For example, "SELECT * FROM ca_tenant".
ldap_enable	Yes	Required. Enables LDAP integration with CA SDM.
ldap_host		Required. Specifies the LDAP database server host name or IP address.

Option	Default Value	Description
ldap_port	389	Required. Specifies the LDAP server port number.
ldap_dn		Required. Specifies the LDAP server logon distinguishedName. **Example**: CN=Joe, CN=Users, DC=KLAND, DC=AD, DC=com If the LDAP server supports anonymous binds, this value can be empty.
ldap_pwd		Required. Specifies the password for LDAP server logon distinguishedName. If the LDAP server supports anonymous binds, this value can be empty.
ldap_search_base		Required. Specifies the starting point for searches in the LDAP schema tree: (UNIX) You must specify a starting container. For example: CN=Users, DC=KLAND, DC=AD, DC=com (Windows) You do not have to specify a container. You may start at the top of the schema tree. For example: DC=KLAND, DC=AD, DC=com
ldap_filter_prefix	(&(objectClass=user)	Specifies the prefix applied to an automatically generated filter when searching for LDAP users. This variable has been superseded by the ldap_user_object_class option. It is not available in Options Manager, but can be set manually in the NX.env file.
ldap_filter_suffix	)	Specifies the suffix applied to an automatically generated filter when searching for LDAP users. This variable has been superseded by the ldap_user_object_class option. It is not available in Options Manager, but can be set manually in the NX.env file.
ldap_user_object_class	person	Required. Specifies the value of the LDAP objectClass attribute applied to an automatically generated filter when searching for LDAP users.
ldap_enable_group	Yes	Optional. Enables CA SDM access type assignment based on LDAP group membership.
ldap_group_object_class	group	Required only if the ldap_enable_group is installed. Specifies the object name applied to an automatically generated filter when searching for groups.
ldap_group_filter_prefix	(&(objectClass=group)	Specifies the prefix applied to an automatically generated filter when searching for LDAP groups. This variable has been superseded by the ldap_group_object_class option. It is not available in Options Manager, but can be set manually in the NX.env file.
ldap_group_filter_suffix	)	Specifies the suffix applied to an automatically generated filter when searching for LDAP groups. This variable has been superseded by the ldap_group_object_class option. It is not available in Options Manager, but can be set manually in the NX.env file.
ldap_enable_auto	Yes	Optional. Enables auto generation of contact records from LDAP data.
ldap_sync_on_null	Yes	Optional. Overwrites existing CA SDM contact attributes with null data if the corresponding LDAP user attribute contains a null value.
ldap_service_type	Active Directory	Optional. Use this option if the CA SDM operating environment is Windows and the LDAP directory is *not* Active Directory (for example, eTrust or Novell). On UNIX operating environment, "Non AD" functionality is used only if this option is *not* installed. If it is installed, the service type is set to Active Directory.
	No	

Option	Default Value	Description
ldap_enable_tls		Optional. Specifies whether Transport Layer Security (TLS) is enabled during LDAP processing.

Verify LDAP Integration

After you have installed the necessary LDAP options, CA SDM users can import LDAP data on a case-by-case basis, eliminating the need to fill in all the contact attribute fields manually.

To verify that you can search for and import LDAP records

1. Select File, New Contact from LDAP on the Service Desk tab.
   The LDAP Directory Search window appears.

2. Specify filter criteria, and then click Search. For example, you could enter b% in the Last Name field to retrieve a list of the LDAP user entries with last names that begin with the letter B.

   Note: If your LDAP directory contains thousands of entries and you do not filter your search, your request attempts to retrieve *all* of the LDAP user records. This can cause the request to time-out and return zero records.

   Search results matching your filter criteria are displayed.

3. Select an entry.
   The Create New Contact window appears, populated with imported LDAP attribute values.

4. Click Save.
   The contact record is created.

To verify that you can update a contact using LDAP data

Note: Before performing this procedure, for test purposes you may want to use whatever LDAP editing tool you have available to change one or more attribute values in the entry you used for the previous procedure. You can verify that the contact is updated with the latest LDAP data.

1. Select Search, Contacts on the Service Desk tab.
   The Contact Search window appears.

2. Specify filter criteria to search for a contact that has a corresponding LDAP user entry. For example, you could search for the contact you created in the previous procedure.
   Search results matching your filter criteria are displayed.

3. Select the contact you want to update with LDAP data.
   The Contact Detail page appears, populated with the CA SDM contact information.

4. Click Edit.
   The Contact Update page appears.

5. Click Merge LDAP.
   The LDAP Entry List page displays a list of any LDAP user entries that correspond with the selected CA SDM contact.
   To search the LDAP directory for other entries, you can click Show Filter, specify filter criteria, and then click Search.

   Note: If your LDAP directory contains thousands of entries and you do not filter your search, your request attempts to retrieve *all* of the LDAP user records. This may cause the request to time-out and return zero records.

6. Click the LDAP entry of interest.
   The LDAP Detail page displays the attribute values for the selected entry. Verify that you have selected the correct entry for the contact you want to update, then click Close Window.

7. On the LDAP Entry List page, right-click the entry that best matches the contact you want to update, and then select Merge into Contact.
   The Contact Update page reappears, populated with the current LDAP attribute values. If the LDAP data has changed since you created or last updated the contact, the changes are reflected in the contact attribute fields.

   Note: If you have installed the ldap_sync_on_null option, and the LDAP entry contains null values for any attribute fields that correspond to contact attributes that currently contain values, the values in the contact record are overwritten with null values when you save the contact data.

8. Click Save on the Contact Update page.
   The contact is updated with the corresponding LDAP data.

Create a Contact

A contact is a person who uses your system regularly, such as an analyst or customer. After you have created the business structure and groups, you create contacts and map them to their respective location and organization.

You can create contacts using the following ways:

Create a Contact Using Data From LDAP

If your installation is configured to access a Lightweight Directory Access Protocol (LDAP) server such as Microsoft Windows Active Directory and has the necessary options installed, you can create and update contacts using data from the LDAP database. This method makes it easy to synchronize contacts with network user data.

Note: Administrators can configure automated synchronization of contacts with LDAP data.

Follow these steps:

1. Select File, New Contact from LDAP from the menu bar of the Service Desk tab.
   The LDAP Directory Search page appears.

2. (Optional) Complete one or more of the following filter fields to limit the LDAP Entry list to the records of interest:

   - **Last Name**
     Specifies the last name of the user as it appears in the LDAP directory. For example, you could enter b% in the Last Name field to retrieve a list of the LDAP user entries with last names that begin with the letter B.

   - **First Name**
     Specifies the first name of the user as it appears in the LDAP directory.

   - **Middle Name**
     Specifies the middle name of the user as it appears in the LDAP directory.

   - **User ID**
     Specifies the user name for logging in to the system.

3. Click Search.
   The LDAP Entry List page displays the records that match your search criteria.

   Note: To see the information contained in an LDAP record without creating a contact, right-click the record of interest and select View. The LDAP Entry Detail page appears.

   All fields on the LDAP Entry Detail page are self-explanatory except for the following:

   - **User ID**
     Specifies the ID the user enters to log in to the system.

- **Distinguished Name**
  Specifies the fully qualified LDAP login name. For example, CN=Joe, CN=Users, DC=KLAND, DC=AD, DC=com.

4. Click the LDAP entry to create a contact.
   The Create New Contact page appears and is partially populated with LDAP information.

5. Enter additional information (see page) as necessary.

6. Click Save.
   The contact record is saved and the Contact Detail page appears. The following buttons are now available for configuring the contact:

   - **Update Environment** -- Displays the Configuration Item/Asset Search window for the contact or organization, where you can specify search criteria for the assets you want to consider. When you click Search, the Environment Update window is displayed, where you can add and remove assets for this contact or organization.

     Update Groups -- Displays the Group Search window, where you can specify search criteria for the groups you want to consider for this contact. When you click Search, the Groups Update window is displayed, where you can add and remove groups for this contact.

Create a Contact Automatically

You can configure CA SDM to create a contact automatically from a corresponding LDAP user record whenever a new user logs in to CA SDM.

To enable this feature, install all of the required LDAP options plus the ldap_enable_auto option.

The contact record is automatically created as follows:

1. If a user logging in to CA SDM does not yet have a contact record, but the user's login name exists in an LDAP record, the LDAP data is automatically imported and a contact record is created.

2. The automatically created contact record inherits the defaultaccess type security settings.

3. The contact can then be assigned an access type explicitly, or the access type can be assigned based on the user's membership in an LDAP Group.

This process is completely transparent to the user, appearing as any other login session.

Create Contacts Manually

If you do not want to use an active directory such as LDAP for your contacts information, you can create the contacts manually in CA SDM.

Note: If multi-tenancy is enabled, select the appropriate tenant from the drop-down list.

Follow these steps:

1. Select File, New Contact from the menu bar on the Scoreboard.
   The Create New Contact window opens.

2. Complete the contact fields (see page) .

3. Click Save.
   The contact information is saved.

Contact Fields

Tenant

Specifies the tenant that is associated with the contact (for multi-tenancy installations).

Contact ID

Specifies a unique identifier for the contact. If the default user authentication is being used, the value in this field is used as the password when the user logs in.

User ID

Specifies the user name of the contact. The contact uses this value to log in to the system.

Service Type

Specifies the level of support that is received by the contact.

Data Partition

Specifies the data partition for this contact. This value determines the records that this contact can access.

Access Type

Specifies the access type. The access type determines the system functions the contact can access.

Available

Indicates whether the contact is available for ticket assignments.

Confirm Self-Service Save

Indicates whether the contact receives a confirmation when saving a record from the self-service interface.

Analyst's Tenant Group

(Analyst Contact Type Only) Specifies the tenant group that the analyst is responsible for.
To configure the contact, use the following controls available on the tabs.

Notification

Defines the contact information and method for notifying the contact.

- Select the notification method from the drop-down list (Email, Notification, Pager_Email, xMatters/Email, xMatters/Notification, and xMatters/Pager_Email) that you want to use for each message urgency level for this contact.

  Note: CA SDM supports only one notification method at a time. If you are using Email, then you cannot use Notification at the same time. This applies to all out of the box notification methods like Email, Notification, Pager_Email, xMatters/Email, xMatters /Notification, and xMatters/Pager_Email.

  Note: CA SDM Administrators must update the notification method manually in the contact details page if the xMatters and CA SDM integration is disabled. For more information, see Create a Notification Method (see page 834) and Options Manager xMatters (see page 1303).

- Select the workshift that is valid for each notification urgency level.

For example, you may assign a Regular workshift (five-day week, eight-hours a day) to the normal level notification, but a 24 hour workshift to the emergency level notification.

Address

Specifies the location of the contact.

Organizational Info

Specifies the functional or administrative organization, department, cost center, or vendor information of the contact.

Environment

Specifies the environment of the contact, such as equipment, software, and services.

Groups

Assigns a contact to a group (a collection of contacts with a common area of responsibility).

Roles

Assigns the contact to one or more roles.

Service Contracts

Displays any service contracts that have been associated with the contact.

Special Handling

Lists the special handing contacts and lets you search for and associate a contact to a special handling type, such as a visitor or security risk type.

Event Log

Lists events that are associated with the contact, such as self service and knowledge activities.

Activities

Lists the activity log for the contact.

Merge Contacts Using LDAP

You can synchronize existing contacts with the current LDAP data.

Follow these steps:

1. Select Search, Contacts on the Scoreboard.

   The Contact Search page appears.

2. Fill in the filter fields as desired (or leave all filter fields blank to see a listing of all contacts), then click Search.

   The Contact List page appears.

3. Click the contact you want to edit.

   The contact's Detail page appears.

4. Click Edit.

   The contact's Update page appears.

5. Click Merge LDAP.

   The LDAP Entry List page appears. If the contact you are editing has a corresponding LDAP record, it appears on this page.

6. Click the LDAP entry.

   The LDAP Detail page appears.

7. Click Close Window after you have verified that the LDAP Detail page contains the data for the correct user.

8. Right-click the entry on the LDAP Entry List page for the contact you are updating and select Merge Into Contact.

9. Click Save on the contact's Update page.

Assign Access Type Using LDAP Groups

Assign Access Types values to contacts automatically with a Lightweight Directory Access Protocol (LDAP) server.

Note: To enable this feature, install the ldap_enable_group and ldap_group_object_class options.

Follow these steps:

1. Select Security and Role Management, Access Types on the Administrator tab.
2. Select the Access Type you want to associate with an LDAP Group. For example, select Administration.
   If the ldap_enable_group option is installed, the LDAP Access Group field appears on the Web Authentication tab.

   Note: If an LDAP Group is already associated with the selected Access Type, a link to the LDAP Group Detail appears. Click the link for a read-only description of the LDAP Group and a listing of its members.
3. Click Edit on the Access Type Detail page to associate an Access Type with an LDAP Group.
4. Click the LDAP Access Group link.
5. (Optional) Enter filter criteria to limit the search to the LDAP groups of interest.
6. Select the LDAP Group that you want to associate with this Access Type.
7. Click Save.
   Association of the selected LDAP Group with the Access Type is complete.

Attribute Mapping

CA SDM contact record attribute values are synchronized with LDAP user attribute values based on the attribute mapping definitions in the $NX_ROOT/bopcfg/majic/ldap.maj file.

The following excerpt from ldap.maj illustrates mapping. Attribute names in the left column (id) are the CA SDM contact attribute names. The center column (distinguishedName) contains the corresponding LDAP attribute names.

```
    id               distinguishedName              STRING 512;
last_name          sn,pzLastName                    STRING ;
first_name         givenName,pzFirstName            STRING ;
middle_name     initials,pzMiddleName            STRING ;
userid               uid,sAMAccountName,pzUserName     STRING ;
phone_number    telephoneNumber,pzWorkPhoneNumber STRING ;
```

If an SREL (a single relationship or foreign key in another database table) exists on CA SDM, the contact attribute value is synchronized with the corresponding LDAP value. If the SREL does not exist, it is not created automatically during LDAP synchronization processing.

Note: By default, attribute mapping is configured for the Microsoft Active Directory LDAP schema. If necessary, you can change the mapping by using a mod file.

How to Modify Attribute Mapping

You can change the default attribute mapping.

To change the default attribute mapping, do the following steps:

1. Navigate to $NX_ROOT/site/mods/majic and open the mod file.
2. Use MODIFY statements in the mod file as follows.
   - MODIFY statements must always be stated first in the file.
   - Following the MODIFY statements, any additional fields that are not in the ldap.maj file should be stated using the syntax shown in the following example.
   - If you define a field that contains a hyphen character in the attribute name, you must enclose the name in single quotes; otherwise, when you build the mod file, the attribute fails with a syntax error. For example, the following attribute name must be enclosed in single quotes:

     ```
     c_nx_string1 'swsd-secret-question' STRING ;
     ```
3. Save and close the mod file.
4. Restart the CA SDM service.

   Important! The web engine does not start if there is a discrepancy in the syntax or case.

   Your changes take effect.

Example: Use MODIFY Statements

The following example shows how to modify two existing fields and add a new field.

```
//
// Map CA SDM userid attribute to ADAM Userid
//
MODIFY ldap userid cn ;
```

```
MODIFY ldap middle_name middleName ;
OBJECT ldap LDAP {
ATTRIBUTES LDAP_Entry{
contact_num employeeNumber STRING ;
};
} ;
```

How CA SDM Uses LDAP Data to Communicate

Lightweight Directory Access Protocol (LDAP) is a network communications protocol for querying and modifying directory services running over a TCP/IP network. An LDAP directory is a tree structure that contains entries for managing users, groups, computers, printers, and other entities on a network.

CA SDM can be configured to access an LDAP directory, which allows you to use LDAP data in several ways:

- Synchronize contacts with LDAP user records. Synchronization can occur in the following ways:
  - **At login** -- When a user logs in to the product, if an LDAP record exists for that user but a corresponding contact record does not exist, a contact record is automatically created based on the LDAP information.
  - **New Contact** -- When you manually create a contact record, you can select an LDAP record and can merge its attribute values with their corresponding fields in the new contact record.
  - **Batch Update** -- You can run batch jobs to automate the processes of importing and updating contact records with information from the corresponding LDAP records.

    Note: Synchronization with LDAP is a one-way process. The LDAP data can be used to create and update contacts, but the product does not support updates to the LDAP directory.
- Assign CA SDM access types that are based on LDAP group membership.
- Implement an alternative method of performing CA SDM authentication.

The ldap_virtb component provides LDAP integration functionality on the following servers depending on your CA SDM configuration, regardless of operating system type:

- Conventional: Primary or secondary server.
- Advanced Availability: Background or application server.

Note: The $NX_ROOT/bopcfg/majic/ldap.maj file specifies the mapping between LDAP attributes and contact record attributes.

Important! CA SDM requires that LDAP records have an entry in the last name field in order to facilitate search, view, and import the LDAP data.

Important! CA SDM supports *paged searching*, which searches all records in your LDAP directory. Paged searching also enables you to import new contact records or sync existing contact records from any number of LDAP records. These capabilities are limited, however, if you are using Sun Java System Directory Server or Novell eDirectory because these LDAP servers do not support paged searching. In that case, you can only search, import, and sync with the number of LDAP records specified by NX_LDAP_MAX_FETCH. For more information about paged searching, see NX.env File.

Access Type Assignments From LDAP Groups

You can configure CA SDM to assign access type values to contacts automatically, based on LDAP group membership. With automatic access type assignment enabled, if an LDAP user record that was used to create a contact belongs to an LDAP group that is associated with one of the CA SDM access types, then the contact is automatically assigned that access type. Otherwise, the contact inherits the default access type.

To enable automatic access type assignment, you must install the ldap_enable_group and ldap_group_object_class options.

For more information, see Configure LDAP Options (see page 1207).

LDAP Authentication

You can use LDAP to authenticate users logging in to CA SDM. The LDAP authentication is available when the CA EEM authentication component is integrated with CA SDM, which replaces the default validation that is performed by the host operating system. The LDAP authentication is only applicable when CA EEM is configured to use an external LDAP directory and you have selected OS authentication for an user validation type in an access type record.

When a CA EEM feature is activated, login requests are checked with the CA EEM server. A log in request is granted only if the following occurs:

- The specified user ID matches a CA SDM contact record.
- The user ID matches a user profile in CA EEM.
- The user ID and password combination is successfully validated by CA EEM.

Note: For more information about using CA EEM for authentication and to move authentication module to external server, see How to Move the Authentication Module to an External Server (see page 864). Also, see Assign Access Type Using LDAP Groups (see page 1216).

Transport Layer Security

You can configure CA SDM to use Transport Layer Security (TLS) during LDAP processing. TLS, a secure communications protocol, is the successor of Secure Socket Layer (SSL v3) security. You install the ldap_enable_tls option to enable TLS.

Important! If this feature is enabled, all communications between CA SDM and the LDAP server are encrypted. If this feature is *not* enabled, all data communications (including the administrative login and password that is used to access the LDAP server) are sent in clear text.

Note: For information about configuring TLS, refer to your LDAP server and operating system documentation. Manually install the LDAP options using the Web Interface Options Manager. For more information, see Configure LDAP Options (see page 1207).

Create Contacts in Batch Mode Using LDAP Data

This article contains the following topics:

Batch Import Contacts Using LDAP Data

You can run the pdm_ldap_import command-line utility to create CA SDM contacts in batch mode using LDAP data.

Note: In addition to creating contacts, pdm_ldap_import updates existing contacts if they are not synchronized with their corresponding LDAP entries. You can use the pdm_ldap_sync batch process to update existing contacts, but not create ones.

When you import contacts using LDAP data, restart the CA SDM services if you encounter the following error:

pdm_ldap_import: Method got_record in Ldap_Group_Catcher failed (LDAP agent not found).

pdm_ldap_import has the following syntax:

```
pdm_ldap_import -n "domain_name" -l "ldap_where_clause" [-c "contact_where_clause"] [-
u "userid"]
```

- **-n *"domain_name"***
  Specifies the LDAP directory domain name from where you want to import contacts to CA SDM. If you do not specify the domain name, CA SDM retrieves the data using the default LDAP domain name.

- **-l "*ldap_where_clause*"**
  Specifies the userids of LDAP records to be searched. Replacement variables are indicated with the '?' character. For example, for *userid = ?*. The default value is *userid = ?*. In this special case, id is mapped to the contact attribute ldap_dn.
  Note: Use the keywords as defined in the *ldap.maj* file. You can also search by using the memberOf = 'group_dn' syntax.

- **-c "*contact_where_clause*"**
  (Optional) Specifies how to determine whether the contact record already exists. If the contact record does not exist, a new contact record is inserted. If the contact record does exist and is not synchronized with the current LDAP data, the contact record is updated.

- **-u "*userid*"**
  (Optional) Specifies the login name under which the pdm_ldap_import program runs.

Note: You can use wildcards with pdm_ldap_import to specify multiple records.

Examples: Batch Imports Using LDAP Data

This example imports a single LDAP record for userid jsmith11 from the LDAP directory with the domain name example.com:

```
pdm_ldap_import -n "example.com" -l "userid = 'jsmith11'"
```

This example imports all LDAP records with a userid that begins with the letter C from the LDAP directory with the domain name example.com:

```
pdm_ldap_import -n "example.com" -l "userid = 'c%'"
```

This example imports all LDAP User records in the directory from the LDAP directory with the domain name example.com:

```
pdm_ldap_import -n "example.com" -l "userid = '%'"
```

Batch Import Contacts by Date and Time

You can configure the pdm_ldap_import utility to import LDAP records that were created before or after a specified date and time. To enable this functionality, create an ldap.mod file with the following content:

```
OBJECT ldap {
  ATTRIBUTES LDAP_Entry {
```

```
    whenCreated whenCreated STRING ;
  };
};
```

This adds the *whenCreated* attribute to the LDAP object.

The rules for filtering records using the whenCreated attribute are as follows:

- Use only the >= or <= operator.
- Specify *all* characters for the date/time value, including the Z. Place a 0 in any location you do not wish to explicitly state (for example, the time of day).
- Place the date/time specification at the beginning of the filter; do not use leading 0s at the beginning of the string.
- Do not include the leading century. For example, to specify the year 2008, use 08.

Note: Single quotation marks must surround the date/time value.

Example: Using the whenCreated Attribute to Import LDAP Entries

The following example uses the whenCreated attribute to import LDAP entries created after 3/11 /2008.

```
Pdm_ldap_import -l "whenCreated >= '080312000000Z'"
```

Example: Using the whenCreated Attribute to Search for LDAP Records

The following example uses the whenCreated attribute with pdm_ldap_test to search for LDAP records created after 3/11/2008.

```
pdm_ldap_test.exe -f "whenCreated>=080312000000Z" -a whenCreated
Starting ldap_test.exe...
LDAP Directory Type    : active directory
Service Desk Platform    : windows
Search Base    : DC=kirklandsd,DC=ca,DC=com
Search Filter    : (&(objectClass=person)(whenCreated>=080312000000Z))
Administrator Username    : CN=Administrator,CN=Users,DC=kirklandsd,DC=ca,DC=com
Administrator Password    : **********
LDAP Host    : gecko.kirklandsd.ca.com
LDAP Port    : 389
LDAP API Version    : 3
DN: CN=aixmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
        whenCreated(17)(0): 20080312035327.0Z
DN: CN=hpmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
        whenCreated(17)(0): 20080312035425.0Z
DN: CN=sunmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
        whenCreated(17)(0): 20080312035726.0Z
3 Total LDAP records found...
```

Batch Import Summary and Log Data

The pdm_ldap_import command maintains a detailed log of all activity of each run. The ldap_logging.0-n log file is located in the $NX_ROOT/log directory.

The following is an example of the summary data pdm_ldap_import returns at the command line:

```
pdm_ldap_import Starting...
pdm_ldap_import Summary:  Processed(21) Updated(1) No Matches(7) New Contacts(11)
Multiple Matches(0) Empty Filter(2) Errors(0)
pdm_ldap_import Complete...
```

The following table describes the summary data.

Status	Count	Description
Processed	21	The number of CA SDM contacts with corresponding LDAP entries.
Updated	1	The number of contact records that were updated because the corresponding LDAP entry contained different information
No Matches	7	The number of CA SDM contact records with no corresponding LDAP entries.
New Contacts	11	The number of new contact records that were created based on corresponding LDAP entries
Multiple Matches	0	The number of LDAP entries with multiple matching contact records, as defined by the ldap_search_base option
Empty Filter	2	The number of LDAP entries that cannot be used to generate a valid search filter
Errors	0	The number of LDAP entries that encountered an error during processing. For example, LDAP records that do not contain a value in a field required by CA SDM (such as Last Name) are counted as failures and cannot be imported.

Batch Update Contacts Using LDAP Data

You run the pdm_ldap_sync utility to update contact records in batch mode using LDAP data.

Important! This utility overwrites the existing tenant of the LDAP contact defined in CA SDM. If you want to retain the tenant value, you must modify NX.env by adding the NX_RETAIN_TENANT_VALUE variable manually, and set it to "yes". If this variable is set to "no", missing, or not set properly, the utility overwrites the tenant information.

Note: The pdm_ldap_sync utility synchronizes existing contacts with corresponding LDAP entries, but does not create contacts. You can use the pdm_ldap_import batch process to create contacts.

pdm_ldap_sync has the following syntax:

```
pdm_ldap_sync -n "example.com" -l "ldap_where_clause" [-c "contact_where_clause"] [-u "userid"]
```

- **-n *"domain_name"***
  Specifies the LDAP directory domain name from where you want to import contacts to CA SDM. If you do not specify the domain name, CA SDM retrieves the data using the default LDAP domain name.

- **-l "ldap_where_clause"**
  Determines how to search for matching LDAP records. Replacement variables are indicated with the '?' character. For example, for *userid = ?*, the default value is *id = ?*. In this special case, id is mapped to the Contact attribute ldap_dn.

- **-c "contact_where_clause"**
  (Optional) Determines which contacts are used when searching for matching LDAP records.
  Default: "ldap_dn IS NOT NULL"

- **-u "userid"**
  (Optional) Specifies the userid under which pdm_ldap_sync runs.

Note: You can use wildcards with pdm_ldap_sync to specify multiple records.

Examples:

This example establishes a baseline of contact records that have a corresponding LDAP record:

```
pdm_ldap_sync -n "example.com" -l "userid = ?" -c ""
```

This example uses the default parameters to update all contacts that have an LDAP distinguishedName:

```
pdm_ldap_sync -n "example.com"
```

This example updates a single contact:

```
pdm_ldap_sync -n "example.com" -l "userid = ?" -c "userid = 'jsmith11'"
```

Batch Update Summary and Log Data

The pdm_ldap_sync command maintains a detailed log of all activity for every run. The ldap_logging.0-n file is located in the $NX_ROOT/log directory.

The following is an example of the summary data pdm_ldap_sync returns at the command line:

```
pdm_ldap_sync Starting...
pdm_ldap_sync Summary:  Processed(21) Updated(1) No Matches(7) No Changes(11)
Multiple Matches(0) Empty Filter(2) Errors(0)
pdm_ldap_sync Complete...
```

The following table describes the summary data:

Status	Count	Description
Processed	21	The number of CA SDM contacts with corresponding LDAP entries
Updated	1	The number of LDAP entries with information different from their corresponding CA SDM contact record
No Matches	7	The number of CA SDM contact records with no corresponding LDAP entries.
No Changes	11	The number of LDAP entries with information identical to their corresponding CA SDM contact record
Multiple Matches	0	The number of LDAP entries with multiple matching contact records in CA SDM, as defined by the ldap_search_base option
Empty Filter	2	The number of LDAP entries that cannot be used to generate a valid search filter
Errors	0	The number of LDAP entries that encountered an error during processing

Test Connections to LDAP Directories

This article contains the following topics:

Use the pdm_ldap_test command-line utility to test the connection to an LDAP directory, ensure that the search options are correctly configured, and test the TLS configuration.

By default, pdm_ldap_test uses the parameter settings that are entered in the $NX_ROOT/NX.env file when you install, edit, or uninstall LDAP options. To override the defaults, you can specify parameters at the pdm_ldap_test command line.

To see the available parameters for this command, enter the following command:

```
pdm_ldap_test -h
```

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

Verify Connection to LDAP Server

To verify the connection to the LDAP server, run pdm_ldap_test without parameters:

```
pdm_ldap_test
```

Successful Connection to LDAP Server

If the connection is successful, you receive output similar to the following:

```
Starting pdm_ldap_test...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(myserver.mycontroller.xyz.com,389): (Success)
ldap_bind_s(Administrator) (Success)
LDAP API Verion 3
```

View Search Parameters

To verify that the search parameters are correctly configured, run pdm_ldap_test without parameters:

```
pdm_ldap_test
```

Successful Search

When your search is successful, you see output similar to the following:

```
DN: CN=John A. Smith,CN=Users,DC=COMPUTERTEST
       c(2)(0): US
       displayName(14)(0): John A. Smith
       mail(14)(0): account02@mycompany.com
       givenName(4)(0): John
       initials(1)(0): a
       distinguishedName(38)(0): CN=John a.
Smith,CN=Users,DC=COMPUTERTEST
       objectGUID(3)(0): 314738
       pager(12)(0): ###-111-1111
       postalCode(5)(0): 11111
       SAMAccountName(7)(0): account02
       sn(6)(0): Smith
       telephoneNumber(12)(0): ###-342-6265
       userPrincipalName(16)(0): account02@COMPUTERTEST
DN: CN=Mike Johnson,CN=Users,DC=COMPUTERTEST
       displayName(10)(0): Mike Johnson
```

```
       givenName(4)(0): Mike
       distinguishedName(34)(0): CN=Mike
Johnson,CN=Users,DC=COMPUTERTEST
       objectGUID(12)(0): 312328
       SAMAccountName(7)(0): account03
       sn(5)(0): Johnson
       userPrincipalName(16)(0): account03@COMPUTERTEST
```

Determine which Attribute Names have Values

Use the -a "*" parameter and the -f parameter with the pdm_ldap_test command to determine which attributes are defined for LDAP User or Group records. This test is useful for seeing if there are LDAP attributes that you want to map to Contact attributes, and to verify that a particular attribute has a value and should be available when creating or updating Contact records.

The following example shows output from an iPlanet directory:

```
pdm_ldap_test -a "*" -f sn=Account_1000001
2 LDAP records found...
DN: cn=Account_1000001,ou=200K_Plus,o=SmartLabs
   sn(15)(0): Account_1000001
   objectClass(13)(0): inetOrgPerson
   objectClass(20)(1): organizationalPerson
   objectClass(6)(2): Person
   objectClass(18)(3): ndsLoginProperties
   objectClass(3)(4): Top
DN: cn=Account_1000001,ou=2_Plus,o=SmartLabs
   mail(28)(0): ThisIsTheMailingAddressField
   uid(13)(0): Login_1000001
   givenName(17)(0): GivenNameOfPerson
   sn(15)(0): Account_1000001
   objectClass(13)(0): inetOrgPerson
   objectClass(20)(1): organizationalPerson
   objectClass(6)(2): Person
   objectClass(18)(3): ndsLoginProperties
   objectClass(3)(4): Top
```

The following example shows output from Active Directory:

```
Ldap_test  - a "*"  - f (&(sn=Brown)(initials=A))"
1 LDAP records found...
DN: CN=John A. Smith,CN=Users,DC=mycontroller,DC=xyz,DC=com
   objectClass(3)(0): top
   objectClass(6)(1): person
   objectClass(20)(2): organizationalPerson
   objectClass(4)(3): user
   cn(16)(0): John A. Smith
   sn(5)(0): Brown
   givenName(7)(0): John
   initials(1)(0): A
   distinguishedName(55)(0): CN=John A. Smith,CN=Users,DC=mycontroller,DC=xyz,DC=com
   displayName(16)(0): John A. Smith
   memberOf(52)(0): CN=Domain Admins,CN=Users,DC=mycontroller,DC=xyz,DC=com
```

```
   sAMAccountName(7)(0): smijo04
   userPrincipalName(25)(0): smijo04@mydomain.xyz.com
   objectCategory(63)(0): CN=Person,CN=Schema,CN=Configuration,DC=mycontroller,DC=xyz,
DC=com
```

Narrow Your Search

Use the -f parameter with the pdm_ldap_test command to specify a filter to be added to the base filter for narrowing the search criteria. You must use appropriate LDAP syntax and LDAP schema attribute names in your filter. Surround your filter with double quotation marks and use parenthesis to clarify the order of operator precedence.

For example, use the following command to search for all records where sn=Account_10001:

```
pdm_ldap_test  - f "(sn=Account_10001)"
```

The pdm_ldap_test utility supports the following equality operators:

Equality Operator	Description
=	equal to
<=	less than or equal to
>=	greater than or equal to
~=	like

The pdm_ldap_test utility supports the following Boolean operators:

Boolean Operator	Description
&	AND
|	OR
!	NOT

The AND and OR operators affect each set of parenthesis () in the search filter. The NOT only affects the first set of parenthesis. Always place these operators *before* the search filters to be operated on, rather than between them. They can be applied to any number of filters, as shown in the following examples:

```
"(&(sn=Brown)(initials=A)) "
"(|(sn=Brown)(sn=Smith))"
"(!sn=Brown)"
```

Error Messages for Failed Connections to LDAP Directories

This article contains the following topics:

Failed Connection Server Down or Incorrect Name or Port

If the connection fails because the server is down or you specified an incorrect LDAP server name or port, you receive output similar to the following:

```
Starting pdm_ldap_test...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(junk,389): (Success)
ldap_bind_s(Administrator) (Server Down)
```

Failed Connection Invalid LDAP_DN or LDAP_PWD

If the connection fails because you specified an incorrect LDAP_DN or LDAP_PWD, you receive output similar to the following:

```
Starting pdm_ldap_test...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(myserver.mycontroller.xyz.com,389): (Success)
ldap_bind_s(junk) (No Such Object or Invalid Credentials)
```

Failed Search Invalid SEARCH_BASE

If the search fails because you have an invalid SEARCH_BASE, you receive output similar to the following:

```
Starting pdm_ldap_test...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabsx
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)

ldap_bind_s() (Success)
LDAP API Verion 3
ldap_search_st() (No Such Object or Referral)
```

Failed Search SIZELIMIT_EXCEEDED, TIMEOUT

The search can fail with a SIZELIMIT_EXCEEDED or TIMEOUT message if you specify a filter that does not sufficiently narrow the search. Most LDAP Servers limit the size of the result set returned from a search request. If you exceed this limit, you receive a SIZELIMIT_EXCEEDED message. If your search request takes longer than the default timeout of 20 seconds, the LDAP server times out your request and you receive a TIMEOUT error message similar to the following:

```
Starting pdm_ldap_test...
LDAP service type=edirectory
Service Desk platform=windows
```

```
Using search base=o=SmartLabsx
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)
ldap_bind_s() (Success)
LDAP API Verion 3
ldap_search_st() (TIMEOUT or SIZELIMIT_EXCEEDED)
```

Failed Search 0 Records Returned

The search may fail because your default filter is not correct. If pdm_ldap_test returns zero (0) records, always check the Using filter line, which is the base filter generated by the LDAP_FILTER_PREFIX and LDAP_FILTER_SUFFIX, or the LDAP_OBJECT_CLASS options:

```
Starting pdm_ldap_test...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabs
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)
ldap_bind_s() (Success)
LDAP API Verion 3
ldap_search_st() 0 records
```

Configuration File Modification

When you install the CA SDM web interface, a sample web engine configuration file (*web.cfg*) is installed that you can modify to suit your needs. The *web.cfg* file itself contains helpful comments that you can read by viewing the file. You can open the *web.cfg* file from the appropriate directory:

- (Windows) %NX_ROOT%\bopcfg\www\
- (UNIX) $NX_ROOT/bopcfg/www/

> **Note:** Some additional configuration variables, such as charset, are also available in Options Manager. These are accessible using the Administration tab in the web interface.

AllowInactiveSrelEntry
Specifies whether a record can be saved when it references inactive records in a reference table.

- When this property is omitted or set to zero, inactive reference table entries (such as request status or change category) are not included in drop-down selects, and cannot be specified for lookup or hierarchical search fields.
- When this property is set to 1, the inactive flag is ignored in reference table entries.

Regardless of the setting of this flag, records already containing a reference to an inactive reference table entry can be saved without changing the reference; the flag affects only new field values.

AnnouncementLength
Specifies the maximum number of announcements to display on the opening screen for both customer and analyst interfaces. CA SDM begins the display with the most recent announcement, continuing for the number of announcements specified by this parameter. Users of the analyst interface can view additional announcements by selecting Announcements from the Search menu.
Default: 10, meaning that the ten most recent announcements display.

AnonymousPrio
Specifies valid priorities for tickets created by guest users. Such users can specify only one of the priorities in the AnonymousPrio list for their tickets. Entries in the list of priorities are separated by spaces. Each entry must be either a number between 1 and 5 or the word “none” (without quotes). The default priority for tickets created by guest users should be specified first, and can be repeated in the list.
The values valid for AnonymousPrio correspond to the symbolic names of the priorities as distributed. You can use the java client to modify these symbolic names; however, this does not affect the specification for AnonymousPrio, which must continue to reference priorities by their default names, where 1 corresponds to the highest priority.
Default: None, meaning that all requests created by a guest user have a priority of none.

Autofill
Specifies that the web interface should auto-fill lookup fields when a user keys data into them and presses Tab to exit the field. When a user does this and the Autofill option is selected, the browser asks the server to confirm that the update is correct. This results either in the full name filling in the field (if the user provided a partial name), or a pop-up search window appearing (if the user’s selection was incorrect or ambiguous).
This property is optional. Autofill is enabled by default so if this property ID is omitted or set to Yes, tabbing out of a lookup field automatically searches the database. If this property is set to No, no auto-fill occurs, and lookup fields are not verified until the record is saved.

CAisd
Specifies the path (including a leading slash) to the alias or virtual directory in your HTTP server that contains the files needed by the CA SDM web server. This property typically has a value of /CAisd in both UNIX and Windows installations. For Apache servers, it should be defined in an Alias statement in a configuration file. For IIS, it should match an Alias field in the Directory Properties Window.

CGI
Specifies the name of the CGI executable program supplied with the web interface (without the .exe suffix).
Default: pdmweb

Note: If you rename this program, you must update this property.

CgiReport

Specifies the name of the CGI executable program for web reports supplied with the web interface (without the .exe suffix).
Default: pdm_cgireport

Note: If you rename this program, you must update this property.

ContactAutoDesc

Specifies whether the contact's name should be inserted into the description of new issues and requests created in the customer and employee interfaces. If this property is omitted or specified as 0, no automatic information is added to the description of new issues and requests. If this property is specified as 1, the contact's name is automatically inserted into the description of issues and requests created in the customer and employee interfaces. This property has no effect on the analyst interface.

ContactAutoDescWithIP
Specifies whether the contact's IP address should be inserted into the description of new issues and requests created in the customer and employee interfaces. If this property is omitted or specified as 0, no IP address information is added to the description of new issues and requests. If this property and the ContactAutoDesc property are both specified as 1, the contact's name and IP address are automatically inserted into the description of issues and requests created in the customer and employee interfaces. This property has no effect on the analyst interface. It is ignored unless ContactAutoDesc is 1.

CstPrio
Valid priorities for issues created with the customer web interface. Users of the customer interface can only specify one of the priorities in the CstPrio list for their issues and cannot update the priority of an issue if an analyst has altered it to a value that is not in the list.
Entries in the list of priorities are separated by spaces. Each entry must be either a number between 1 and 5 or the word "none" (without quotes). The default priority for issues created with the customer interface should be specified first (and can be repeated in the list).
Default: none, 3, 4, 5
The values valid for CstPrio correspond to the symbolic names of the priorities as distributed. You can use the java client to modify these symbolic names; however, this does not affect the specification for CstPrio, which must continue to reference priorities by their default names, where 1 corresponds to the highest priority.

DateFormat
Defines the order of elements in dates.
Default: MM/DD/YYYY hh:mm a(am,pm)

Symbol	Description
M	Print 1 or 2 digits of month
MM	Print 2 digits of month
D	Print 1 or 2 digits of date
DD	Print 2 digits of date
YY	Print 2 digits of year
YYYY	Print 4 digits of year
H	Print 1 or 2 digits of hours on 24 hour clock
HH	Print 2 digits of hours on 24 hour clock
H	Print 1 or 2 digits of hours on 12 hour clock

Symbol	Description
hh	Print 2 digits of hours on 12 hour clock
M	Print 1 or 2 digits of minutes
mm	Print 2 digits of minutes
S	Print 1 or 2 digits of seconds
ss	Print 2 digits of seconds
a(am, pm)	Print am and pm as a string

DateFormatNoTime

Specifies the same definition as DateFormat, but without specifying the time portion.

DebugSource
Enables the standard browser right-click menu on CA SDM forms. When this property is not set, you can right-click a form to display a CA SDM menu. You should use caution when setting this property, because some of the options on the standard browser right-click menu can cause execution errors (this is the reason why it is usually disabled). On Internet Explorer, you can display the standard browser right-click menu although the DebugSource property is not set by pressing the Ctrl key when you right-click.

DebugTrace
Causes the web engine to write trace information to the stdlog file.

Important! This property should *not* be set for typical use. It should only be used when requested by CA Support.

EmpPrio
Valid priorities for requests created with the employee web interface. Users of the employee interface can only specify one of the priorities in the EmpPrio list for their requests and cannot update the priority of a request if an analyst has altered it to a value not in the list.
Entries in the list of priorities are separated by spaces. Each entry must be either a number between 1 and 5 or the word “none” (without quotes). The default priority for requests created with the employee interface should be specified first (and can be repeated in the list).
Default: none, 3, 4, 5
The values valid for EmpPrio correspond to the symbolic names of the priorities as distributed. You can use the java client to modify these symbolic names; however, this does not affect the specification for EmpPrio, which must continue to reference priorities by their default names, where 1 corresponds to the highest priority.

ExclLockSeconds
Specifies the maximum number of seconds that a user is given an exclusive lock on a record after clicking Edit. After this period elapses, the web engine releases the lock, allowing other users to update the record. The web engine attempts to retake the lock if a user asks to save after ExclLockSeconds has expired. This attempt succeeds only if no other user has updated the record

while the lock was available. If the attempt to retake the lock fails, the user must re-enter the updates.
Default: 120 (two minutes)
This argument is optional. If omitted, the default value is assumed.

Note: The ExclLockSeconds setting must be shorter than the Timeout setting. ExclLockSeconds is specified in seconds and Timeout is specified in minutes.

FormCacheMax
Specifies the maximum number of forms to be retained in web engine memory for each user. The web engine always retains the last FormCacheMax forms used by each user. Forms beyond this number are eligible to be timed out. Timed out forms cannot be accessed by the Back or Forward buttons on the main page, and can no longer be submitted on a pop-up form.
Default: 10
Timed out forms save memory in the web engine, but they occasionally require users to manually refresh them. You can set FormCacheMax to - 1 to disable the FormTimeout feature.

FormTimeout
Specifies the minimum number of seconds that a form is retained in the web engine before it is eligible for removal from the cache. Users always have at least the number of seconds specified in this parameter to work on a form before submitting it. In addition, the web engine always retains the most recently used FormCacheMax forms for each user.
You can use the StayCacheList property to prevent specified forms from timing out.
Default: 180 (3 minutes)

FormTitle
Specifies a string to be included in the title bar of a web browser displaying a CA SDM web form. The value of FormTitle supplements the title of the specific form displayed.
Default: CA SDM
For example, if the default value is retained, and Microsoft Internet Explorer is used to display the Announcement Detail form, the title bar displays the following:
Announcement Detail -- CA SDM -- Microsoft Internet Explorer
This property is optional. If omitted, the analyst web interface does not use a constant value in the title. The customer and PDA web interfaces revert to the default value.

HitTrackFile
Specifies the full path to a file that receives a log of all web pages used. One line is written to this file each time a user requests a page. The file can grow indefinitely, so be cautious when specifying this property.

Note: Records containing a time stamp, user ID, database record ID, and HTMPL form name are appended to this file. The format of the records may change. You must periodically maintain this file so that it does not get too large.

This property is optional. If omitted, no hit tracking file is written.

HtmplCacheSize
Specifies the size of the HTMPL cache. When this size is exceeded, the least used form is removed from the cache.
Default: 1000.

ListAllMaximum
Specifies the maximum number of records that can be displayed in a list before a request to display the entire list produces a pop-up warning message advising the user that the request adversely impacts performance and is not allowed.
Default: 2500

ListAllWarn
Specifies the maximum number of records that can be displayed in a list before a request to display the entire list produces a pop-up warning message advising the user that the request may adversely impact performance, and asking for confirmation.
Default: 1000

ListBottomMaximum
Specifies the maximum number of records that can be displayed in a list before a request to scroll to the bottom produces a pop-up warning message advising the user that the request adversely impacts performance and is not allowed.
Default: 2500

ListBottomWarn
Specifies the maximum number of records that can be displayed in a list before a request to scroll to the bottom produces a pop-up warning message advising the user that the request may adversely impact performance, and asking for confirmation.
Default: 1000

ListPageLength
Specifies the maximum number of found records to be shown on a list page after performing a search.
Default: 10

LogoutURL
Specifies the complete URL of a web page to be displayed after a user logs out of CA SDM. This property is optional. If it is not specified, logging out returns the login form.

Lr_Refresh
Specifies the log reader refresh interval in seconds. If this property is non-zero, the Notification Log Reader automatically refreshes itself at the specified interval (with a minimum of thirty seconds). This property is optional. If omitted, the log reader refreshes itself every 5 minutes (a default value of 300 seconds). If this property is specified as zero, the log reader does not automatically refresh at all.

MacroPath
Specifies a list of directory paths that the web engine searches to find files requested by the PDM_MACRO tag. You can specify multiple directories separated by spaces. You can include environment variables in the directory names by prefixing them with a dollar sign (for example, $NX_ROOT). For both Windows and UNIX, separate path components with a forward slash (/), not a backslash (\). This property is required. It is typically set as follows:

```
$NX_ROOT/site/mods/macro $NX_ROOT/bopcfg/www/macro
```

MatchesFound
Specifies the text of the message to display under a field when a user's key for a lookup field is ambiguous and the edit form must be redisplayed with a drop-down select list. This property is optional; if omitted, it defaults to Multiple Matches.

MaxRecordsAutoSuggest

Specifies the number of records that autosuggest displays when search as you type or autosuggest displays suggestions below a lookup.
Default: 25

MaxSelectList
Specifies the maximum number of matches to display in the drop-down select list shown when a user' s key for a lookup field is ambiguous and the edit form must be redisplayed. If more than this many matches are found, the message specified for Too Many Matches is displayed.

MinCharsAutoSuggest
Specifies the minimum number of characters to enter in the lookup fields before search as you type or autosuggest displays suggestions.
Default: 3

MouseoverPreviewDelayTime
Specifies the delay time (in milliseconds) between hovering the mouse pointer over a link and the display of the mouseover preview.
If the mouse moves away from the link before the delay time expires, the preview does not appear.
Default: 1000

NoMatchesFound
Specifies the text of the message to display under a field when a user's key for a lookup field is incorrect and the edit form must be redisplayed. This property is optional; if omitted, it defaults to No Matches Found.

PreLogin Timeout
Specifies the maximum number of minutes the web engine keeps a session active before login. The web engine automatically starts a session when a user requests a login form, in anticipation of the user completing the login. If the user does not login within the time period specified, the web engine destroys the session. If the user subsequently logs in, the web engine creates a session that is transparent to the user.
This property has no end-user impact. Its sole purpose is performance -- balancing web engine memory usage versus the overhead of destroying and recreating a session. This property is optional; if omitted, it defaults to one minute.

RedirectingURL
Specifies the URL the WebDirector should use to send requests to this web engine. This property specifies the full URL of the web engine, including http. This property is required if you are using WebDirector. It is ignored if you are not.

SchedExpMaximum

Specifies the limit of the number of schedule events that can be exported at a time.
Default: 1000

Important! The default is the maximum exports that CA SDM can handle at a time. Increasing this default could cause system instability. If you attempt to export more than the value specified in SchedExpMaximum, a message appears refusing your exporting request.

SelListCacheExclude
Specifies the names of the factories (objects) to be excluded from caching for <PDM_SELECT> lists. To improve performance, the web engine usually caches in its own memory of the contents of small tables used in <PDM_SELECT> (drop-down) lists and hierarchical search lists. You may want to suppress caching for a table if you are using data partition constraints to specify that different users should receive different views of the table. In addition, including tables in the value of this property eliminates the need for the web engine to query their record count at startup, slightly improving startup performance. This property is optional. If specified, it should contain one or more object names separated by spaces.

SelListCacheMax
Defines the maximum number of records in a table that can be cached in the web engine. The web engine keeps the entire contents of tables at or below its cache size in its own memory, improving its performance in building <PDM_SELECT> lists using these tables. Specifying a higher value for this property improves performance at the expense of memory usage.
Default: 10
SelListCacheMax is ignored for tables used in hierarchical search lists, such as category on requests, issues, and change orders. The web engine always stores the entire contents of tables used in hierarchical search lists in its own memory. If you have a large number of values in any of these tables, you may want to specify the SelListCachePreload property.

SelListCachePreload

Specifies one or more tables to be loaded into the web engine's select cache at startup time. Tables not specified in this property are loaded the first time they are used. If SelListCacheMax is large, or if you have a large number of records in a hierarchical search list (such as category), you may want to specify the table in SelListCachePreload. This avoids a response time delay the first time a user accesses a form using the table.
The specification for the SelListCachePreload property is a blank-separated list of object names. Each object name can be followed by an optional list of attribute names in parentheses. The attributes specified in the list are loaded into the web engine. If no attributes are specified, only the common name and rel attr value of the object are loaded. This is sufficient for drop-down selects, but may not be sufficient for hierarchical searches. If you modify the hierarchical search forms (hiersel_xx.htmpl, where xx is an object name), be sure that the SelListCachePreload property specifies every attribute used in the form. If you omit an attribute, the cache is reloaded when the form is used.
The SelListCachePreload property is optional. If it is omitted, nothing is loaded into the select cache until a user requests a form using a drop-down select or a hierarchical search.

```
chgcat(description owning_contract) chgstat crs isscat(description owning_contract)
issstat pcat(description cr_flag in_flag pr_flag owning_contract) pri tskstat urg
pcat_cr(description cr_flag in_flag pr_flag owning_contract) pcat_pr(description
cr_flag in_flag pr_flag owning_contract) pcat_in(description cr_flag in_flag pr_flag
owning_contract)
```

StayCacheList

Specifies the names of forms that are never removed from the forms cache, regardless of the length of time they have been displayed. This property ensures that the fixed frames on a frame display remain for the lifetime of a session. It can be used with caution to cause other forms to be permanently cached. The default is as follows:

```
scoreboard.htmpl top_splash.htmpl buttons.htmp hiersel_admin_tree.htmpl
```

SuppressHtmplCache

Specifies that the web engine should reread all files defining the contents of a page each time the page is requested. Parsing an HTMPL file takes a significant amount of web engine processing time, and usually involves reading several physical files (because most pages use PDM_INCLUDE tags). The web engine normally saves parsed files in its own memory so that future requests for the same page can be satisfied immediately. This markedly improves performance, but can be inconvenient for users in the process of developing new or updated pages, as the web engine must be recycled for changes to take effect.
This property is optional and requires no value. If it is specified, the web engine does not cache parsed files, and changes to HTMPL files take effect immediately. Because of its impact on performance, this property should not be specified in a production environment.

SuppressLoginAndLogoutMsg
Specifies that the web engine should not log a message to the CA SDM log file each time a user logs in or logs out of the web interface.
This property is optional. If it is not specified, the web engine logs a message each time a user logs in or logs out.

SuppressMacroCache
Specifies that the web engine should discard all saved macros each time a new page is requested. The web engine normally saves parsed macros in its own memory so that future requests for the macro can be satisfied immediately. This improves performance, but can be inconvenient for users in the process of developing new or updated macros, as the web engine must be recycled for changes to take effect.
This property is optional. If it is specified, the web engine does not cache parsed macros, and changes to macros take effect immediately. Because of its impact on performance, this property should not be specified in a production environment.

Timeout
Specifies the number of minutes that a user's session can be idle before it is automatically terminated, freeing up all server resources.

Note: The Timeout setting must be longer than the ExclLockSeconds setting. ExclLockSeconds is specified in seconds and Timeout is specified in minutes.

TooManyMatches
Specifies the text of the message to display under a field when a user's key for a lookup field is ambiguous and the number of matches for the key exceeds the value of MaxSelectList. This property is optional; if omitted, it defaults to Too Many Matches.

UpdatedAnnouncementsPopup
The interval that browser checks for a new announcement. When a new announcement is found, it automatically shows the announcement in a popup window. The interval value is in minutes. To reduce the impact to the browser performance, it's recommended to set this variable to the value greater than 5 (minutes).

UseDirector
Specifies when the WebDirector is controlling this web engine. The following table defines possible values:

Value	Description
No	The web engine is independent of the WebDirector. This is the default value.
Yes	The WebDirector must initiate all sessions, including the login form. If a user attempts to make a direct connection to the web engine, the web engine asks the WebDirector for a referral.
AfterLogin	The web engine refers a session to the WebDirector after authenticating a user. A web engine configured with UseDirector AfterLogin is responsible solely for authentication, and is thereby a candidate for the use of secure sockets (SSL) for maximum security.
BeforeLogin	The web engine refers a session to the WebDirector before authenticating a user. A web engine configured with UseDirectory BeforeLogin never displays a login page, and never accepts a login password.

This property is optional. If omitted, the web engine does not use the WebDirector.

UseNestedTabs
Specifies whether to display the nested tab control on detail forms.
Default: Enabled

WebDirectorSlumpName
Specifies the name of the WebDirector servicing this web engine. This property is needed only if you are running more than one WebDirector, or if you have configured your WebDirector to use a slump name other than its default of web:director.
This property is optional if you are using WebDirector. It is ignored if you are not.

WillingnessValue
Specifies the willingness of this web engine to accept sessions, based on a scale of 0 to 10. This property is used only if you are using WebDirector. This value is meaningful only in comparison with the willingness of other web engines associated with the same WebDirector. The WebDirector transfers sessions to web engines in proportion to their willingness values. A web engine with a willingness value of twice that of another web engine's, on average, services twice the number of sessions.
A WillingnessValue of zero means that the web engine does not accept any sessions. This value can be useful when UseDirector is AfterLogin.
This property is optional if you are using WebDirector. It is ignored if you are not. If omitted, the web engine sets its willingness to 5.

WorkFrameTimeout
Specifies the maximum number of seconds the web engine waits for a response to an internal server request before concluding the request has failed. The workframe is used for CA SDM web interface features requiring server data other than normal web pages. This includes such features as autofill, loading category properties, and updating scoreboard counts. Workframe requests to the CA SDM

are unlikely to fail. However, workframe requests to other servers (such as integrated products, such as Knowledge Management) may fail if the targeted server is not running, or if a network problem prevents access to it. The WorkFrameTimeout property specifies a length of time before the request is considered to have failed, and the workframe is available for other requests.

Note: WorkFrameTimeout is not checked unless a workframe is needed and all workframes are in use. Therefore, it is quite likely that a remote server is going to have more time than that specified for WorkFrameTimeout to respond. The value of WorkFrameTimeout is a minimum.

This property is optional. If omitted, the web engine uses a 30 second work frame timeout.

Creating the Business Structure

Contents

A business structure is a logical representation of your enterprise in a CA Service Desk environment. This scenario describes how an administrator can create a business structure for an enterprise to manage and track contacts, groups, and assets that are spread across distributed locations. After you create a business structure, you can generate reports to analyze requests by site, organization, or group.

Example

The fictional company Forward, Inc. uses a request processing system for multiple offices that are spread across geographical locations. The company plans to implement CA Service Desk to analyze the number and types of requests that are generated from its various business segments.

To facilitate effective tracking and decision making, the organization must track the following elements:

- Contacts, contact groups, and locations
- Assets at various locations

Creating a business structure allows the management team at Forward, Inc. to perform the following actions:

- Generate reports to analyze requests by site, organization, and group
- Increase overall efficiency by implementing corrective measures for any gaps in the request process

Create a Site

A site is a geographical region where your organization has one or more locations.

For example, North America can be a site, with locations (offices) in New York, California, and Texas.

Note: If multi-tenancy is enabled, select the appropriate tenant from the drop-down list.

Follow these steps:

1. Select File, New Site from the menu bar on the CA Service Desk Scoreboard.
2. Enter the information as appropriate specific to your site.
3. Click Save.
   The site record is created and saved.

Create Locations

A location is a physical place such as an office address. For example, the addresses for New York, California, and Texas offices can be locations under the site North America.

Creating locations helps you manage contacts and resources in that location. After you create a location, you can assign it to a site.

Follow these steps:

1. Select File, New Location from the menu bar on the Scoreboard.
2. Enter the information specific to your location, then configure the location using the following controls on the tabs:
   - **Address**
     Specifies the physical address of the location.
   - **Auto Assignment**
     Automatically assigns the tickets (requests, change orders, and issues) to members in this location.
     - **Update Request Areas**
       Select the request areas that you want to auto-assign to members of the location.
     - **Update Change Categories**
       Select the change categories that you want to assign to members of the location.
     - **Update Issue Categories**
       Select the issue categories that you want to assign to members of the location.

- **Update Groups**
  Select the groups that you want to update for auto assigning tickets.

Important! After updating the request areas and categories, enable the automatic assignment for each request area and category individually.

3. Click Save.
   The location details are saved.

4. (Optional) Repeat steps 1-3 to add more locations.

Create Organizations

An organization refers to an internal department or division or an external company. You can assign organizations to tickets, Configuration Item (CI) classes, and contacts.

For example, you can define CIs for organizations to specify the hardware, software, and services that the organization uses.

Note: If multi-tenancy is enabled, select the appropriate tenant from the drop-down list.

Follow these steps:

1. Select File, New Organization from the menu bar on the Scoreboard.

2. Enter the information specific to your organization, then specify organization details in the following fields:

   - **Address**
     Displays the address of the location to which you associate the organization. The fields are automatically populated when you assign location to the organization.

   - **Environment**
     Displays the Configuration items (for example, equipment, software, and services) that the organization uses. You can associate one or more configuration items with the organization. Associating the CI items to the organization helps administrators to keep track of the resources used by the organizations in various locations.

3. Click Save.
   The organization details are saved.

4. (Optional) Repeat Steps 1-3 to add more organizations.

Set Up an Organization's Environment

An organization's environment consists of the equipment, software, and services they use.

Follow these steps:

1. Select the Environment tab on the Organization Detail page
2. Click Update Environment.

   The Configuration Item Search page appears.
3. Enter the search criteria to display the configuration items of interest and click Search.

   The Organization Environment Update page displays the configuration items that matched the search criteria.
4. From the list on the left, choose the configuration items you want to add to this organization's environment. To choose multiple items, hold down the CTRL key while clicking the left mouse button.
5. When you have selected all the configuration items you want, click the double right-arrow button.

   The selected configuration items move to the Organization Environment list on the right.
6. Click OK.

   The Organization Detail page displays the selected items listed on the Environment tab.

Create Groups

A group is a collection of contacts that represent a specific area of responsibility. Defining groups lets you assign the responsibility for resolving a ticket when that responsibility is shared among several individuals. For example, a Dallas Human Resources group is responsible for dealing with the personnel issues in the Dallas office of your organization. When an employee in that office has a problem, you can assign the problem to the Dallas Human Resources group for resolution.

Note: The public (shared) option creates the object for all tenants.

Note: If multi-tenancy is enabled, select the appropriate tenant from the drop-down list

Follow these steps:

1. Select File, New Group from the menu bar on the Scoreboard.
2. Enter the information specific to this group and your organization by specifying the group details in the following fields:

- **Notification**
  Defines the contact information and method for notifying the group.

- **Address**
  Assigns the group to a location.

- **Organizational Info**
  Specifies the functional or administrative organization, department, cost center, or vendor information.

- **Environment**
  Specifies the environment (for example, equipment, software, and services).

- **Members**
  Adds or removes contacts.

- **Service Contracts**
  Lists service contracts that have been associated with the group.

- **Auto Assignment**
  Lists auto assignments of tickets that are based on the group membership.

- **Remarks and Special Handling**
  Lists remarks and special handling types, such as VIP or security risk types. You can click Update Contact's Special Handling to search for special handling members.

3. Click Save.
   The group record is saved and the group detail page opens. The following buttons are now available for configuring the group:

   - **Update Environment**
     On the Contact Details, Environment tab, click this button to display the Configuration Item Search window for the group. You can specify search criteria for the assets you want to consider on this page. You can create new configuration item and search assets using the Update window of Contacts respectively.

   - **Update Members**
     On the Members, Service Contracts, Auto Assignment, Members tab, this button displays the contacts. You can add and remove contacts for this group.

4. (Optional) Repeat Steps 1-3 to add more groups as needed.

CA SDM User Authentication

This article contains the following topics:

CA SDM provides a user authentication solution that you can modify as part of the access type. The same authentication is used by all CA SDM interfaces and by other CA products.

Authentication is flexible, allowing you to take advantage of external authentication mechanisms, such as Windows, HTTPD user validation or LDAP authentication. You can also select from a variety of internal authentication options, including operating system password, PIN, guest user access, or no access at all.

How CA SDM Authenticates Users

CA SDM authenticates users based on the user ID defined in their contact record. The product also does the following when a user requests access to the system:

1. If an external user ID is available (from HTTPD or Windows validation), CA SDM looks up the contact by login ID. If the contact is found and has an access type that permits external authentication, the user is allowed into the product.

2. If there was no successful external authentication, CA SDM prompts the user for a user ID and password. The product looks up a contact record for the user ID, obtains the access type, and then authenticates the user as specified by the access type.

Many installations find the predefined access types define authentication that is reasonable for that type of user; however, in some cases you may need to modify the authentication information for a predefined access type or define a new access type to handle a different authentication method for some of your users. You should review the authentication settings for the predefined access types to determine if they meet your needs, or if you need to modify them, or define additional types.

External Authentication

CA SDM permits users to access the system without supplying a user ID if all of the following conditions are met:

- External authentication is set for the user.
- The user's externally authenticated user ID is associated with a contact in your contact table.
- The contact record has an access type whose authentication definition permits external authentication.

External authentication does not permit users to access the system in the following cases:

- A user attempts access through a non-secure server.
- A user attempts access but is assigned to an access type that does not allow external authentication.

None of the predefined access types use external authentication. If you want to use external authentication for users, consider modifying the employee, analyst, and administrator access types to set external authentication. Your individual site requirements and different types of users determine whether to allow external authentication. When external authentication is used, the server configuration controls the access to files and directories. When you define authentication for an access type, you can decide the usage as follows:

- Do not use any external authentication that is already implemented, such as the user login on Windows or validation by the HTTPD server.
- Use the authentication that is implemented and allow or deny access based on it.

Note: If external authentication is not allowed, the user is authenticated based on the validation type that you specify.

Following are some examples of external authentication:

- If a user who has administrator access logs into a Windows computer, the user can perform administrative tasks without re-entering any login information.
- If a user who has HTTPD server validation, the user can access the web interface without re-entering any login information. Because the administrator access type specifies the analyst web user type, the appropriate web interface for the analyst is presented automatically.

Validation Types

Validation types authenticate users only under the following circumstances:

- The user access type does not permit external authentication.
- The user access type permits external authentication, but the user has not been validated externally (for example, the user has attempted access through a nonsecure server).

CA SDM provides you with the following validation options:

- **No Access** -- Users of this type have no access unless external authentication is allowed and is valid.
- **Open** -- Users of this type have access, with no additional authentication required.
  - **OS** -- Users of this type enter their operating system password for access. The operating system used for validation is the one running User Validation Host. This option is the default validation type for the administrator, analyst, and employee access types.
  - **PIN** -- Users of this type gain access by entering the correct value for the PIN field in their contact record as their password. You define the PIN field by entering the field attribute name when you select PIN as the validation type. PIN is the default validation type for the customer access type, which uses the value in the customer ID (contact_num) field as the PIN.

Logged In User Counts and Session Counts

The following KPIs count the number of unique licensed users that are logged in to the system (for example, CA SDM Web UI, SOAP Web Services, REST Web Services, and so on), regardless of how many sessions each user has opened:

Note: For a licensed user, ensure that the Licensed? check box is selected from the Access type page of the contact (navigate to Security and Role Management, Access Type on the Administration tab and search for the contact).

- webConcurrentLicenseCt
- webConcurrentSOAPLicenseCt
- webConcurrentRESTLicenseCt
- webConcurrentTotalLicenseCt

The following KPIs count the numbers of unique unlicensed users that are logged in to the system, regardless of how many sessions each user has opened:

- webConcurrentNonLicenseCt
- webConcurrentSOAPNonLicenseCt
- webConcurrentRESTNonLicenseCt
- webConcurrentTotalNonLicenseCt

The following KPIs count the number of unique sessions that started during the interval:

- webSessionCt
- webSOAPSessionCt
- webRESTSessionCt

For more information about the KPI description, see the KPI detail page (navigate to Service Desk, KPIs on the Administration tab and search for the KPI). For more information about how these KPIs count from different session types, see the How KPIs Count from Different Session Types (see page 1010) topic.

How KPIs Count from Different Session Types

There are different session types that are defined in the system. The following table shows how KPIs count these sessions:

Note: All predefined KPIs are installed as Inactive. For a KPI to begin functioning in your system, it must be set to Active. Navigate to Service Desk, KPIs on the Administration tab and search for the inactive KPI. Open the KPI and click Activate.

Important! Multiple versions of a KPI with the same name cannot be active at the same time.

Session Type	Session Type Description	Counted by KPIs
Web Client	Web browser session	webSessionCt webConcurrentLicenseCt webConcurrentNonLicenseCt webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
Java Client	Java client session	webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
Web Services	SOAP Web services session	webSOAPSessionCt webConcurrentSOAPLicenseCt webConcurrentSOAPNonLicenseCt
Utility	Server utility session	webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
Portal	Portal session	webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
Knowledge Chat	Knowledge Chat session	webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
Mail Server	Mail Server session	webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
Custom Application	Custom Application session	webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
PDA Client	PDA Client session	webSessionCt webConcurrentLicenseCt webConcurrentNonLicenseCt webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt
REST Client	REST Web Services Session	webRESTSessionCt webConcurrentRESTLicenseCt webConcurrentRESTNonLicenseCt webConcurrentTotalLicenseCt webConcurrentTotalNonLicenseCt

Example: KPIs calculating user counts

One licensed (that have the Licensed? check box selected) and two unlicensed end users are logged into the web self-service interface and reviewing some announcements.

At the same time five licensed analysts (that have the Licensed? check box selected) are logged into the analyst interface and working on incidents. One of the analysts also logs in to the SOAP Web Services interface.

- The webConcurrentLicenseCt KPI shows a count of six, meaning that six licenses are currently being used, irrespective of the number of interfaces each user is using.
- The webConcurrentNonLicenseCt KPI shows the count of two, which means that two unlicensed users are logged on to the system, irrespective of the number of interfaces each user is using.

- The webSessionCt KPI shows a count of eight, meaning that eight total users are logged in to the CA SDM Web UI.

- The webSOAPSessionCt KPI shows a count of one, meaning that one user is logged in to the SOAP Web Services interface.

(Applicable for advanced availability configuration only) Example: KPIs calculating user counts from different nodes

A licensed analyst logs in to the analyst interface from the background server and works on incidents. The same analyst logs in to the analyst interface from the application server. The webConcurrentLicenseCt KPI shows a count of one, meaning that one license is currently being used, irrespective of the number of nodes or servers the user has logged in from.

Encrypt Session IDs to Address Vulnerability Issues

CA Service Desk Manager (CA SDM) uses the Session ID for authenticating each request from the user. This Session ID is sent back and forth through the web browser. An attacker can auto-generate the Session ID and can gain unauthorized access to CA SDM, if it matches any of active SIDs in CA SDM. An attacker can sniff the CA SDM web URL using man-in-the-middle attack and can replay the URL to gain unauthorized access to CA SDM. Using encrypted Session ID and cookie for authenticating user requests may have some minimal performance impact on CA SDM.

The following attributes are added in Options Manager to support encrypted Session IDs:

- **use_encrypted_sid_and_cookie (optional)**
  Use the encrypted Session ID and cookie to prevent spoofing and Man-in-the-middle attack. By default, this attribute is disabled. If you want to have enhanced CA SDM security, this attribute can be enabled (Yes).

- **force_browser_to_send_cookie_only_in_ssl_connection** (optional)
  Force the browser to send the Session ID (SID) cookie only if there is an SSL connection. This attribute is applicable only if you have enabled the **use_encrypted_sid_and_cookie** to (Yes). By default, this is turned off. If this flag is enabled, CA SDM can only be accessed through an SSL connection.
  For more information, see Options Manager (see page 1303), Security Options.

Retry Mechanism for CA SDM and CA Process Automation Workflow Options

CA Process Automation Workflows can be attached to CA SDM tickets (for example,Change Orders) through CA SDM Events and Macros. The attached events are triggered by CA SDM at the specified retry interval duration. During retry, if the CA Process Automation is unavailable, the attached event is marked as **Unknown** and the process is not executed. CA SDM retry mechanism automatically re-triggers the attached **Unknown** events when CA Process Automation is available.

CA SDM administrators can enable the retry mechanism by installing additional options in the CA Process Automation Workflow Options Manager. For more information, see Options Manager, CA Process Automation Workflow Options (see page 1303).

- **caextwf_retry_count**: Default value is 3 and can be set in the range [1 – 20].
- **caextwf_retry_interval**: Default minimum value is set as 10 minutes in the range [10-999].

This feature can be disabled by uninstalling these options. Restart CA SDM services after installing or uninstalling these options.

How the CA SDM Retry Mechanism Works

Install the Options Manager options (caextwf_retry_count and caextwf_retry_interval) and restart the CA SDM services. The retry mechanism for a failed event checks if the CA Process Automation services are up and running during the specified time interval in the Options Manager value (default value of 10 minutes). If CA Process Automation Manager services are available, the CA SDM retry mechanism checks for any attached events that are in **Unknown** status. CA SDM triggers such events at the specified time.

The retry mechanism checks for **Unknown** status events for a maximum count value which is equal to Options Manager **caextwf_retry_count** value. This event is not re-triggered once it reaches the maximum retry count value.

For more information, see Options Manager, CA Process Automation Manager Workflow Options (see page 1303).

How to Configure the F5 Load Balancer for CA Service Desk Manager

F5 Load balancers help to enhance the reliability, availability, and scalability of CA Service Desk Manager (CA SDM) servers and improves the overall performance. An F5 load balancer monitors the CA SDM Health Servlet by sending requests to servers and applications that can respond in a timely manner.

To configure an F5 load balancer in your envirnonment, complete the following steps:

- Prerequisites for configuring the F5 Load Balancer (see page 1252)
- Create a Custom Health Monitor (see page 1252)
- Create an F5 Pool for the CA Service Desk Manager Application Server (see page 1253)
- Create an F5 Virtual Server or Node for CA Service Desk Manager (see page 1254)
- Verify the F5 Load Balancer Configuration (see page 1256)

Note: For more information on configuration tasks other than the ones discussed in this article, refer to your F5 Load Balancer documentation.

Prerequisites for configuring the F5 Load Balancer

Before you configure an F5 load balancer for CA SDM, complete and keep handy the following information:

- Identify the CA SDM hosts where you need the load balancing capability.
- Credentials to log in to the F5 interface.
- Before you deploy an F5 load balancer, ensure that you have configured the CA SDM Health Servlet on application servers. For more information on how to deploy the health servlet on a CA SDM Application Server, see Deploy the Health Servlet on the Application Server (see page 898).

Configure the following F5 elements so that these elements can function with the CA SDM Application Servers:

1. Create a Custom Health Monitor (see page 1252)
2. Create an F5 Pool for the CA Service Desk Manager Application Server (see page 1253)
3. Create an F5 Virtual Server or Node for CA Service Desk Manager (see page 1254)
4. Verify the F5 Load Balancer Configuration (see page 1256)

Create a Custom Health Monitor

You can create a custom monitor when the values that you have defined for a pre-configured monitor does not meet your requirements, or when a pre-configured monitor is not available for the type of monitor you are creating. You can give a unique name to your monitor, specify the monitor type, and, if a monitor of that type already exists, import settings and values from the existing monitor. You can change the values of any imported settings.

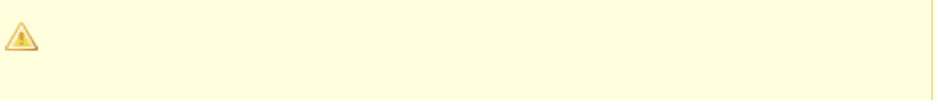
To create a custom health monitor, complete the following steps:

Follow these steps:

1. Navigate to **Local Traffic**, **Monitors**, and Click **Create**. Complete the following field information:
   a. **Name**: Enter the name of the health monitor.
   For example: **SDM_health**

   b. **Type**: Select **HTTP** from the drop-down list.
   You must base each custom monitor on a monitor type. To specify a monitor type, simply choose the one that corresponds to the service you want to check.

   c. **Send String**: Enter **GET /HealthServlet/GetHealth\r\n**.



> **Note:** When you create a new HTTP monitor type, you must include **\r\n** at the end of a non-empty Send String. If you do not include **\r\n** at the end of the Send String, the HTTP monitor fails.

d. **Receive String**: Enter **AA-Server-Status: All OK!**
The above string is displayed when the CA SDM server is healthy. When the server is down, the status displayed is **AA-Server-Status: NOT OK!**

e. **Receive Disable String**: Enter **Quiesce time remaining**.

2. Click **Finished**.
You have successfully created a custom health monitor.
When a user accesses the F5 load balancer URL, CA SDM health check is performed, and the user is routed to a server that is functional and not disabled or temporarily inactive (quiesced).

.

Create an F5 Pool for the CA Service Desk Manager Application Server

Create an F5 pool for the CA SDM server where you want to enable the F5 load balancing capability.

Follow these steps:

1. Select **Main**, **Local Traffic**, and click **Pools.**

> **Note:** The Pool List is empty if you are setting up pools for the first time. The Pool List displays the details for each pool.

2. Click **Create**.

3. Complete the Configuration section on the New Pool page:

a. Select **Basic** from the drop-down list.

b. Enter a name and description for the new pool. .

c. Select an already pre-configured health monitor from the available health monitors list. Select **HTTP** and move it to the active list.

d. If a pre-configured health monitor is not available, create a custom health monitor. For more information on how to create a custom health monitor, see Create a Custom Health Monitor. (see page 1252)

Note: Before you deploy the F5 Load balancer, ensure that you have configured the CA SDM Health Servlet on the application servers to verify the CA SDM application server status. Health Monitors monitor the health of your CA SDM application servers. For more information about CA SDM health servlets, see Deploy the Health Servlet on the CA SDM Application Server (see page 898).

4. Select **Round Robin** from the Load Balancing Method drop-down list. Default option is Round Robin.

5. Select **Disabled** from the Priority Group Activation drop-down list.

6. Add each node or server to the new F5 pool as follows:

    a. Select **Node List** if you are adding a node that is already defined.

    b. If the nodes are not defined, select the **New Node** option to create a node.

    c. Select the CA SDM Application Server IP address (host name) from the **Address** drop-down list that identifies the CA SDM node to add to this F5 pool.
    If the applicant server is no longer valid or no longer in use, select the pool member and click **Disable**.

7. Click **Add**.
The details that you added for this node appear in the New Members list.

8. Click **Finished**.
The new pool is added to the F5 Pool List.

Note: Before quiescing the CA SDM Application Server server for performing a rolling maintenance, ensure that you have deployed the CA SDM application health servlet, or else, remove this server from the F5 Node List. For more information, see Deploy the Health Servlet on the CA SDM Application Server (see page 898).

Create an F5 Virtual Server or Node for CA Service Desk Manager

You can create an F5 Virtual Server for CA SDM application servers to enable the F5 load balancing capability. Complete the following steps to create an F5 Virtual Server:

Follow these steps:

1. Log in to F5. Select **Main**, **Local Traffic**, **Virtual Servers**, and **Virtual Server List**.

2. Click **Create**.

3. Complete the following General Properties on the New Virtual Server page.

a. **Name**: Specifies the name of the virtual server, for example, casdm.

b. **Destination Type**: Specifies Host for a single IP address.
This IP address should be available in the network and must not be assigned to any other device.
For more information, see the F5 Load Balancer documentation.

c. **Destination Address**: Specifies the IP address of the virtual server.

d. **Service Port**: Specifies the associated port for the virtual server.
For example: 80 for HTTP.

e. **State:** Select **Enabled**.
Specifies whether the virtual server is available for load balancing.

4. Complete the Configuration section. Accept all defaults, except for the **HTTP Profile**.

   a. **HTTP Profile**: Select **http**.
   Specifies the HTTP profile for managing HTTP traffic.

   Complete the Resources section:

   a. **iRules**: Specifies the iRules to enable for this virtual server.

   b. **Default Pool**: Specify the CA SDM pool which was created in **step 1** as the default pool.
   The virtual server routes traffic to this pool.

   c. **Default Persistence Profile**: Specifies the persistence profile for this virtual server.
   Select **cookie**.

   d. **Fallback Persistence Profile**: Specifies the persistence profile that this virtual server uses when the default persistence profile cannot be used.
   For example: **source_addr**.

5. Click **Finished**.
   For more information about the F5 Load Balancer persistence profile, see the F5 documentation.

6. Navigate to **Local Traffic**, **Profiles**, **Persistence** to modify the properties of a persistence profile. Select the persistence profile that you want to modify.
   For example, click **source_addr** and change the **Timeout** option to **600** seconds.

   Click **Update**.

   Note: For CA SDM, it is recommended that you set the **Timeout** option to a value of **600**.

7. Click **Finished**.

Verify the F5 Load Balancer Configuration

To verify the F5 load balancer configuration in your environment, complete the following steps:

Follow these steps:

1. Open any web browser, and enter the F5 Virtual Server destination IP address that you created in step 3 (see page 1254) earlier in this article while creating the F5 virtual server. You must be able to view the CA SDM login page.

2. Enter the CA SDM login credentials and click Login.
   Login must be successful.

3. Repeat **step 1** and **2** on all CA SDM application servers and verify that you are routed to these servers by checking the CA SDM logs in the CA SDM install directory.

How to Configure the Mailbox to Handle Inbound Emails

Email lets you communicate with end users, such as employees or customers. The mailbox in CA SDM handles inbound emails from users and provides action according to the email. For example, the user sends an email to CA SDM to create an incident. Mailbox checks the email, creates an incident, and sends a notification back to the user.

CA SDM provides a default mailbox (named Default) that is active and ready for use within your organization. You can modify the default mailbox, create more mailboxes, or both. After creating a mailbox or modifying the Default mailbox, define the mailbox rules. The Mailbox rules let you configure any actions, replies, or both.

Note: The rules that are applicable for one mailbox cannot be associated with another mailbox. To reuse the same rules for a different mailbox, recreate them for the other mailbox. You can also copy the existing mailbox. We recommend that you set the associated mailbox to inactive before configuring a mailbox rule. Else, any messages that are retrieved between your first change and last change are processed with rules that are in effect.

Follow these steps:

1. Log in to the web UI from the following servers, depending on your CA SDM configuration:

   - Conventional: Primary or secondary servers
   - Advanced availability: Application or background servers

2. Choose a Notification Phrase (see page 1257)

3. Define a Mailbox (see page 1261)

Choose a Notification Phrase

The notification phrase is sent to the sender of the email. For example, to confirm that an incident has been created successfully. CA SDM provides predefined notification phrases which are set to inactive by default. You can activate and modify the phrases. You can also create notification phrases to best suit your organization needs.

Choose from the following options:

- Activate a predefined notification phrase (see page 1257).
- Create a notification phrase (see page 1257)

Activate a Predefined Notification Phrase

By default, predefined notification phrases are set to inactive. You activate a notification phrase so that the notifications can use the phrase. Select Notifications, Notification Phrases on the Administration tab and search for the notification phrase. Edit the notification phrase and select Active from the Active drop-down list.

Create a Notification Phrase

You can create notification phrase that contains standardized text and macros. This notification phrase is sent as a response to emails from users.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. Select Notifications, Notification Phrases on the Administration tab.
   The Notification Phrase List page opens.
2. Click Create New.
   The Create New Notification Phrase page opens.
3. Complete the Notification Phrase Fields (see page 1257), as appropriate.
4. Click Save.
   The notification phrase is created.

Notification Phrase Fields

Complete the following fields to edit or create a notification phrase:

- **Symbol**
  Defines a unique identifier for this record.

- **Code**
  Specifies a unique value to use for the notification phrase, in the usp_notification_phrase table. The usp_notification_phrase table lists common phrases that notification message templates can use. For information about the usp_notification_phrase table, see the *Technical Reference Guide*.

- **Phrase**
  Specifies the phrase for the notification. You can specify both plain-text and HTML versions. HTML consolidates most of the whitespace into single spaces, so you must specify line breaks or paragraph breaks with tags.
  For example, the following plain-text phrase is used in the Confidential Notice notification phrase:

```
This e-mail and any files transmitted with it are for the sole use of the intended recipient(s) and contain
information that may be privileged and confidential. Any unauthorized review, use, disclosure or distribution is
prohibited. If you are not the intended recipient of this e-mail, please delete this e-mail and any files transmitted
with it and notify the sender immediately.
```

  The following HTML phrase can be used to ask the user to view the notification list:

```
Click on the following URL to view Notification List:
@{call_req_id.web_url}+HTMPL=cr_lr.htmpl+INSTANCE=@{id}
```

  For more information about phrases, see the Notification Codes and Phrases (see page 1258) topic.

Notification Codes and Phrases

Notification phrases let you add a standardized piece of information or text to a number of different notification messages, without having to enter and maintain the text or formulae separately in each notification template. For example:

Reply to this notification to add additional information to the ticket

Phrases standardize text for use in multiple message templates. For example, you can maintain a common phrase such as a confidential notice in a single record and use it in multiple message templates. Notification phrases are also useful for message replies, such as a Reply Notice, or a web URL link. CA SDM provides phrases and you can create your own phrases. You can set a phrase as active or inactive for use in a message template globally. (Notification phrases are inactive by default.) When a phrase is inactive, the phrase is suppressed in all message templates that use the phrase.

Notification phrases can also be used in the automatic responses to incoming email messages. The processing context for this type of message is different; omit the prefix (change_id., issue_id., call_req_id.) used in certain macros such as ref_num and web_url for phrases that the message uses. As a result, you cannot share notification phrases between notification templates and email automatic responses.

For example, some of the phrases that CA SDM provides are as follows:

Symbol	Code	Phrase
Notify History - Change		

Symbol	Code	Phrase
	notify_history_chg	Click the following URL to view the Notification List: @{change_id.web_url}+HTMPL=chg_lr.htmpl+INSTANCE=@{id}
Notify History - Issue	notify_history_iss	Click the following URL to view the Notification List: @{issue_id.web_url}+HTMPL=iss_lr.htmpl+INSTANCE=@{id}
Notify History - Request/Incident/Problem	notify_history_cr	Click the following URL to view the Notification List: @{call_req_id.web_url}+HTMPL=cr_lr.htmpl+INSTANCE=@{id}

Example: New Phrases

The following phrases are examples of phrases that you can create:

Symbol	Code	Phrase
Notify Confidential	ConfidentialNotice	This email and any files transmitted with it are for the sole use of the intended recipient (s) and contain information that may be privileged and confidential. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient of this email, please delete this email and any files transmitted with it and notify the sender immediately.
Notify Incident Reply	IncidentReply	To add a comment to your Incident, just reply to this email or include the line below (on a line by itself). %incident_id=@{call_req_id.ref_num}
Notify Incident URL	IncidentURL	Click the following URL to view: @{call_req_id.web_url}

Note: Use separate phrases for the plain-text and HTML versions of message templates or email auto-replies. HTML consolidates the whitespaces into single spaces, so line- or paragraph-breaks must be specified with tags. HTML tags included in plain-text versions of messages are displayed rather than processed.

Notification Phrase Syntax

You insert notification phrases in message templates and email reply messages using the following macro syntax:

```
@{notification_phrase[code].phrase}
```

- ***code***
  Specifies the unique Code value, such as ConfidentialNotice, of the Message Phrases (usp_notification_phrase) table.

Note: The usp_notification_phrase table lists common phrases that notification message templates can use.

For example:

```
@{notification_phrase[IncidentURL1].phrase}
@{notification_phrase[RequestReply].phrase}
```

When CA SDM locates the macro, the phrase text from the usp_notification_phrase table replaces the syntax. If no matching code exists (or if it is inactive), an empty string replaces the macro. No errors are written to the standard log (STDLOG), instead a warning message is logged to help you resolve potential problems.

Note: Embedding phrases within other phrases is limited to a maximum depth value that you configure by setting the NX_MAX_EXPAND_DEPTH environment variable (see page 862). This limitation prevents problems which can occur when processing phrases that are accidentally self-referenced (embed themselves) or circular-referenced (when a phrase embeds a phrase into which it is embedded).

Example How Notification Phrases Appear in a Message

This example demonstrates how notification phrases appear in a notification message. The example uses the following codes and phrases:

Code	Phrase
Conf idenc tialNo tice	This e-mail and any files transmitted with it are for the sole use of the intended recipient(s) and contain information that may be privileged and confidential. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient of this e-mail, please delete this e-mail and any files transmitted with it and notify the sender immediately.
IncidentReply	In order to add a comment to your Incident, just reply to this email or include the line below (on a line by itself). %incident_id=@{call_req_id.ref_num}
IncidentURL	Click the following URL to view: @{call_req_id.web_url}

The following message template includes the notification phrases:

```
@{call_req_id.type.sym} @{call_req_id.ref_num} Closed.
Assigned to: @{call_req_id.assignee.combo_name}
Customer: @{call_req_id.customer.combo_name}
Description: @{call_req_id.description}

@{notification_phrase[IncidentURL].phrase}
@{notification_phrase[IncidentReply].phrase}
```

```
@{notification_phrase[ConfidentialNotice].phrase}
```

The phrases appear in a message as follows:

```
Incident 1234 Closed.
Assigned to: Analyst, Joe
Customer: Doe, John
Description: This is a description of my problem

Click on the following URL to view:
http://helpdesk/CAisd/pdmweb.exe?OP=SEARCH+FACTORY=chg+SKIPLIST=1+QBE.EQ.id=400723

In order to add a comment to your Incident, just reply to this email or include the
line below (on a line by itself).
%incident_id=1234

This e-mail and any files transmitted with it are for the sole use of the intended
recipient(s) and contain information that may be privileged and confidential. Any
unauthorized review, use, disclosure or distribution is prohibited. If you are not
the intended recipient of this e-mail, please delete this e-mail and any
files transmitted with it and notify the sender immediately.
```

Define a Mailbox

This topic contains the following information:

CA SDM provides a default mailbox to connect to the mail server. You can configure this default mailbox to change the password, user name, hostname, and so on. You can also create extra mailboxes to suit your organizational needs. Each mailbox can have its own definition, instead of using a single global set of definitions. You can define multiple mailboxes and can use different templates or default values for each mailbox. Multiple definitions allow individual tenants or organization use separate mailboxes with different settings.

Use the Default Mailbox or Create a Mailbox

CA SDM provides an active default mailbox. You can edit the mailbox for incoming mail delivery according to your requirement or create a mailbox that connects to the mail server. Configure the mailbox to set values for host, user, password, and so on.

Follow these steps:

1. Select Email, Mailboxes from the Administration tab.
   The Mailbox List page opens.

2. Click Default from the Name column and click Edit to edit a default mailbox or click Create New to create a mailbox.

3. Complete or update the other fields as appropriate:

   - **Check Interval**
     Specifies the time after which the mail server is polled for new emails.

   - **Active**
     Indicates the mailbox status.

   - **Email Type**
     Specifies the protocol that the mail server uses. CA SDM supports both POP3 and IMAP4. If you select IMAP4, CA SDM polls only the Inbox folder from the mailbox.

   - **Hostname**
     Specifies the hostname of the email server.

   - **Port Override**
     Specifies the port number when the default port number is overridden.

   - **User Name**
     Specifies the user ID on the mail server.

   - **Password**
     Specifies the password on the mail server.

   - **Security Level**
     Specifies the SMTP security level.

   - **Attachment Repository**
     Specifies the repository where the email attachments are stored.

   - **Attach Entire Email**
     Specifies whether to allow entire email as an attachment.

   - **Force Attachment Splitout**
     Specifies whether to split all attachments in the email when an entire email is added as an attachment. The email and its attachments are split into separate files and attached to the tickets. Only applicable when the **Attach Entire Email** option is selected.

- **Allow Anonymous**
  Specifies whether tickets can be created from anonymous mails.

- **Save Unknown Emails**
  Specifies whether to save the emails that the rules defined in the mailbox did not process. These emails are stored in $NX_ROOT/site/mail_unknown.

- **Use Reply-To Address**
  Specifies whether to use the alternate email address for replies.

- **Use TLS**
  Specifies whether to use Transport Layer Security support in emails.

- **CA Certificate Path**
  Specifies the path where the trusted certificate has been deployed.

  Note: For the advanced availability configuration, ensure that you deploy the trusted certificate on the same location for both background and standby servers. CA SDM supports only Base-64 encoded (PEM) format for CA Certificates.

4. Click Create New from the Rules tab to create a mailbox rule.
   The Create New Mailbox Rule page opens.

5. Complete the Mailbox Rule Fields (see page 1263) as appropriate and click **Save**.

6. Select the **Policy** tab to define the mailbox policies to protect your organization against certain types of email abuse. Complete the Mailbox Policy Fields (see page 1273) as appropriate and click **Save**.
   The changes to the default mailbox are saved and applied or a new mailbox is created. The first poll occurs after one second.

Mailbox Rule Fields

Important! We recommend that you set the associated mailbox to Inactive before you configure a mailbox rule. Else, any messages that are retrieved between the first and the last change are processed with rules in effect.

The table (usp_mailbox_rule) maintains the rules that are used to connect to each mail server account (usp_mailbox). CA SDM provides predefined rules which you can use to modify or create mailbox rules.

Complete the following mailbox rule fields, as appropriate:

- **Sequence**
  Specifies the sequence number of the rule. Messages are checked against rules in sequence number order from lowest to highest.

- **Mailbox**
  Specifies the mailbox to which this rule belongs.

- **Active**
  Sets the rule to active or inactive.

- **Filter**
  Specifies what part of the email to search for the filter pattern, for example, Subject contains. For more information, see the Pattern Matching in Mailbox Rules (see page 1267) topic.

- **Filter String**
  Specifies a regular expression string to match with the email content. For example, [\t\r\n]request [\t\r\n]. The placeholder {{object_id}} lets you specify the artifact value for the Text API to use for associating the message with a specific ticket. For more information, see the Filter String Object Identifier Restrictions (see page) and Special Characters in Regular Expressions (see page) topics.

- **Ignore Case**
  Specifies whether to consider letter case when matching patterns.

- **Action**
  Specifies the action to take when the filter criteria matches, for example, Create/Update Object.

- **Action Object**
  Displays the type of ticket object to which message actions apply, for example, Request.

- **Minimum Artifact Type**
  Sets the minimum type of artifact checking that you want to allow:

  - **NONE**
    Specifies no validation of artifacts. This value is the same as not adding the keyword to the input file. Also accepts Text API ticket ID commands.

  - **PROTECTED**
    Validates a ticket against the hash for confirmation. If confirmation fails, the artifact is considered invalid and the email fails filtering where filtering is looking for an artifact ({{object_id}}).

  - **SECURE**
    Validates the ticket number from an encrypted data block. If the value is not a valid encrypted ticket number, the artifact is considered invalid and the email fails filtering where filtering is looking for an artifact ({{object_id}}).

Note: Types that are more secure than what is set are allowed. In other words, if you set the minimum type to **PROTECTED**, then both **PROTECTED** and **SECURE** are allowed, but **NONE** is not. Also, if **PROTECTED** or **SECURE** are selected, Text API ticket ID commands are not accepted. For more information about the artifacts, see the Artifacts Use Considerations (see page) topic.

- **Reply**
  Specifies a notification method to send an automatic response. For example, Email. If you do not set this option, no response is returned. The response indicates success or failure of the actions performed for the message, and is separate from any notifications. If you are using multiple mailboxes, we recommend you to use the notification method to configure email replies (see page 1278).

- **Reply Subject**
  Specifies a subject line for the reply, for example, Service Desk Response.

- **Write to stdlog**
  Write email text to the standard log (stdlog) if the filter matches.

- **Log Entry Prefix**
  Specifies a prefix to add when writing email text to the standard log entries. Use this option to enable matching log entries to rules.

- **Add Subject Line**
  Adds the subject line from the original message to the message body before processing. You can append, prepend, or not add a subject line. The subject line is attached to either the ticket Description or a Log Comment, depending on the actions for the message.

- **Text API Defaults**
  Specifies additional default commands for the Text API when the filter matches. Combines with the contents of the [EMAIL_DEFAULTS] section of the text_api.cfg file. The TextAPI Defaults field includes TextAPI keyword commands that are applied to a ticket when it is created from an email that matches a mailbox rule. The commands are not applied when the message affects an existing ticket.
  To specify TextAPI Defaults commands, place each command on a separate line in the TextAPI Defaults field. Format the commands as follows:

```
OBJECT.FIELD=value
```

  Note: Do not include a leading percentage symbol (%), which is required only for corresponding commands that are embedded in the body of the email.

  For example, format the commands as follows:

```
REQUEST.PRIORITY=3

PROBLEM.CATEGORY=Facilities

INCIDENT.GROUP=Plumbing
```

- **Text API Ignore Incoming**
  Specifies additional Ignore Details for the Text API when the filter matches. Combines with the contents of the [EMAIL_IGNORE_INCOMING] section of the text_api.cfg file.

The TextAPI Ignore Incoming field lists TextAPI keyword commands that are not permitted to be used in the text of the incoming email message. Any commands that are listed in this field are ignored when they are found in an incoming email message.
To specify TextAPI Ignore Incoming commands, do the following steps:

1. Place each command on a separate line in the TextAPI Ignore Incoming field.
2. Format the commands as follows:

```
OBJECT.FIELD
```

> **Note:** Do not include a leading percentage symbol (%), which is required only for the corresponding commands that are embedded in the body of the email.

For example, format the commands as follows:

```
CHANGE.ASSIGNEE

PROBLEM.GROUP

REQUEST.EFFORT
```

3. Define all commands used in either field in the [KEYWORDS] section of the text_api.cfg file. This file is located in the “site” subdirectory of the CA SDM installation directory.

- **Details**
  Specifies information about the rule.

- **Success Text**
  Specifies the plain-text contents of a reply message when the message is processed successfully. For example:

```
Thank you for submitting an update to your request. A support technician will contact you within the next 24 hours.
```

  You can also enter a notification phrase, if already created. For example, you can use a notification phrase for email auto-replies.

```
Thank you for submitting your request.

@{notification_phrase[notification phrase code].phrase}
```

- **Success HTML**
  Specifies HTML contents of a reply message when the message processes successfully. The following options let you edit and preview HTML text:

  - **Edit Success HTML**
    Opens the HTML Editor which you can use to format the HTML.

  - **Quick View**
    Previews the HTML.

- **HTML Source**
  Shows the HTML source.

You can also use a notification phrase, for example,

```
Thank you for submitting your request.</p>

@{notification_phrase[notification phrase code].phrase}</p>
```

- **Failure Text**
  Specifies the plain-text contents of a reply message when the message does not process successfully. You can also enter a notification phrase, if already created. For example, you can use the following text:

```
Thank you for submitting your request.

@{notification_phrase[notification phrase code].phrase}
```

- **Failure HTML**
  Specifies HTML contents of a reply message when the message does not process successfully.

Mailbox Rule Actions

Mailbox rules let you perform any of the following email actions:

Ignore Email -- Does not process the email and does not reply.
This action is useful for system-level messages such as Out of Office or Mail Delivery errors.

Ignore Email and Reply -- Does not process the email, and replies to the sender. Response emails use the reply success messages and the reply failure messages are ignored.

Update Object -- Uses the filter string to determine the object identifier (for example, %Incident: {{object_id}}% in the email), and sends an update request to the Text API. If the object identifier is not found, the Text API does nothing.
This action typically handles email replies where the object identifier is embedded in the email. If no object identifier is present, the failure response message is typically sent.

Create/Update Object -- Uses the filter string to determine the object identifier (for example, % Incident:{{object_id}}% in the email), and sends an update request to the Text API. If the object identifier is found, the Text API updates a ticket. If the object identifier is not found, the Text API creates a ticket.
This action is the standard behavior of the mail daemon (Mail Eater) in which the email does or does not contain Text API keywords.

Pattern Matching in Mailbox Rules

The Mailbox rules use regular expressions for pattern matching. Consider the following whitespace characters that apply to regular expressions in mailbox rules:

- **\t**
  Used for representing a horizontal tab

- **\r**
  Used for representing a carriage return character

- **\n**
  Used for representing a line feed or new line character

The characters that represent line breaks in text can vary with the operating system, mail server, and mail client. For example:

- UNIX uses a \n.
- Microsoft uses \r\n
- Macintosh uses \r
- MacOS X uses \n

CA SDM mail processing elements exchange substitute line break characters to identify text elements like message and attached parameters. Use a line or paragraph break for building filters to match \r or\n. Line breaks between two keywords identify a sequence of one or more \r and \n characters.

Line wrapping can result in unexpected line breaks. Line breaks appear in the middle of the text. A space can change to a carriage return or line feed or both. The carriage return or line feed or both can be inserted after a space. Include spaces in the middle of a filter string through the Regular Expression Block:

[\t\n]+(open-bracket, space, backslash, t, backslash, r, backslash, n close-bracket, plus sign).

Example: Use [\t\r\n] to Match the exact keyword:

The sample example shows how to match the exact keyword "request" and ignore other possible similar keywords:

```
requester
requesting
requested
orequestra
```

To match the exact keyword ''request'', enter the keyword request by one or more white space characters as:

```
[ \t\r\n]request[ \t\r\n]
```

The Mail Eater performs a keyword-based search for ''request and ignores other possible keywords like 'requester', requesting.

Filter String Object Identifier Restrictions

Filter strings determine the object identifier (for example, %Incident:{{object_id}}%) in an email. Text that surrounds an object identifier ({{object_id}}) must be unambiguous in both content and length. The text must clearly define the beginning and end of the ticket ID artifact value between the text.

The following restrictions apply to how the Mail Eater interprets the *start* of the ticket ID artifact value:

1. The {{object_id}} placeholder must not be the first element in the filter string. At least, one character is required. Generally, a distinctive keyword or a sequence of letters, numbers, and symbols must precede the object ID keyword.

2. The character immediately preceding the {{object_id}} placeholder must not be a repeatable or optional character having a plus sign (+), an asterisk (*), or a question mark (?). Whitespace characters (space, tab, carriage return, line feed) must not be part of a ticket ID artifact value.

3. The character immediately preceding the {{object_id}} placeholder must not be a repeatable or optional bracketed-set of characters.

The following restrictions apply to how the Mail Eater interprets the *length* of the ticket ID artifact value:

- The {{object_id}} placeholder must not be the last element in the Filter String. One or more characters must follow the {{object_id}} placeholder.
- The character immediately following the {{object_id}} placeholder must not be a repeatable or optional character with a plus sign (+), an asterisk (*), or a question mark (?). Whitespace characters (space, tab, carriage return, line feed) must not be part of a ticket ID artifact value.
- The first character after the {{object_id}} placeholder must not be a character.
- Avoid the following characters immediately before and after the {{object_id}} placeholder:
  - All upper or lower-case letters
  - Numerals
  - The plus sign (+)
  - The slash (/)
  - The comma (,)
  - The period (.), as it can represent any character in this list except for a line break.

  Any of these characters can exist within the ticket ID artifact value. If a bracketed set (several characters between brackets) precedes or follows the {{object_id}} placeholder, the bracketed set must not contain any of these listed characters.

Special Characters in Regular Expressions

Pattern matching for the filters in mailbox rules follows the rules for ASCII Regular Expressions with C-style special characters.

Important! We recommend that you are familiar with Regex syntax to use special characters in regular expressions.

For example, consider the following special characters for Regex patterns that apply to regular expressions in mailbox rules:

- **\t**
  The mailbox filter string \t specifies a horizontal tab. This string matches the beginning and end of text (and tabs), and is specific to MailEater.

- **\r**
  This string specifies a carriage return (return to the beginning of the current line).
  Note: Do not use \r for searching message subjects or sender addresses.

- **\n**
  This string specifies a newline (combination of line feed and carriage return).

  Note: Do not use \n for searching message subjects or sender addresses.

\t, \r, and \n are the special characters that occur most often in regular expressions for mailbox rules.

Example: \t, \r, and \n Use

```
[ \t]request[ \t]
```

The filter string performs a keyword search for 'request'. The brackets match any one character from the set, including the space, so [\t] matches a space or a tab.

```
[\r\n]+critical[ \t\r\n]
```

The filter string performs a keyword search for 'critical'. This string searches at the start of a line, the start of the message, or the entire line. The brackets match any one character from the set. The + (plus sign) matches one or more of the previous, so [\r\n]+ matches one or more carriage returns and newlines.

Sample Text for Notification Phrases in a Mailbox Rule

This example shows sample text that you can use to include notification phrases in a mailbox rule. Define separate versions of a notification phrase for plain text and for HTML when the phrase contains any line breaks or other formatting.

Use the following text in Success Text, Success HTML, or both fields on the Update Mailbox Rule page, Reply Success tab:

Success Text

```
Thank you for submitting your request.
@{notification_phrase[IncidentURL1].phrase}
```

Success HTML

```
Thank you for submitting your request.</p>
```

```
@{notification_phrase[IncidentURL1H].phrase}</p>
```

Artifacts Use Considerations

An email *artifact* refers to something that arises from the mail process, for example, an email address that is included in a forwarded email. The Text API uses artifacts that contain a ticket ID (such as a reference number) for reply support. When the ticket ID is found, an existing Text API keyword (such as %INCIDENT_ID) is set and added to the input for the Text API. The Mail Eater identifies that a reply is associated with a particular ticket by finding the artifact in the message.

The Mailbox rules let you specify the artifact and the value that the Text API uses. For example, you can define a rule for incidents as Incident:{{object_id}}%. When a rule finds Incident:1234, the Text API uses %INCIDENT_ID=1234 (1234 is the ref_num for the Incident). Because the artifact must be unique in an email and easy to find, you can make the artifact more distinctive such as %Incident: {{object_id}}%. A percentage sign (%), whitespace, or some other character that cannot appear in an artifact value must follow {{object_id}}. Uppercase and lowercase letters, numbers, forward slashes, commas, and plus symbols are potentially part of a value. The secure artifacts are Base64-encoded after encryption. If you do not use the Secure artifacts, the characters that follow the artifact must not be contained in the ticket ID suffix, if any, which has been configured for that type of ticket.

When using the filter string of the mailbox rules to identify the ticket ID Artifact, the keyword {{object_id}} represents the position in the filter string where the ticket ID artifact is expected. This keyword is case-sensitive, even if the mailbox rule is not.

Example: Email Artifact Use

The following example shows an ARTIFACT format for use in a mailbox rule for a change request ticket.

Usage: %REQUEST=@{call_req_id.ref_num}%

Example: %REQUEST=1234%

When you construct the filter string of the mailbox rule, consider the following conditions:

- A clear boundary must exist between the ticket ID artifact and the keywords which precede and follow it. We strongly recommended that you include whitespace text in this boundary text.
- Do not end the portion of the filter string that precedes the {{object_id}} keyword in a repeatable or optional pattern that can match the beginning of the ticket ID Artifact, and do not end a pattern whose length is ambiguous. For example, the filter string must not contain the request (er|ed|ing)?{{object_id}}, because this construction causes an ambiguity whether a trailing er, ed, or ing is the end of the leading text or part of the prefix of an unprotected ticket ID.
- The portion of the filter string that follows the {{object_id}} keyword must not begin in a repeatable or optional pattern that may match the end of the ticket ID artifact, must not begin with a pattern whose length is ambiguous, and must contain at least one element of whitespace. For example:
  - The filter string must not contain {{object_id}}[A-Z]?, because the [A-Z]? may match the last character of the ticket ID artifact.

- The filter string must not end with {{object_id}}Item, because it is possible for Item to appear in the ticket ID artifact, either as the suffix of a ticket ID in a plain-text or protected artifact, or as characters within a secure artifact.

- {{object_id}} Item is acceptable, because the space cannot be part of a ticket ID artifact, and is not part of a protected or plain ticket ID artifact. However, {{object_id}}[\t\r\n]+Item (open-bracket, space, backslash, t, backslash, r, backslash, n, close-bracket, plus sign, +Item) is better, because the [\t\r\n]+ compensates for the mail program inserting a line break after the {{object_id}}.

- When you construct the filter strings for different mailbox rules, avoid using a filter string that completely includes another mailbox rule filter string, or in which the portion before or after a {{object_id}} keyword completely includes that portion of another mailbox rule filter string. Depending on the order in which these filters are checked, a message match intended for one filter can match with another, with a portion of the ticket ID artifact matching the additional text that distinguishes between the two filter strings.

Example: How to Create a Mailbox Rule That Matches Every Inbound Message

You can create a mailbox rule that matches every inbound message that another mailbox rule does not filter.

To create this type of rule, set the filter as Subject Contains and the filter string as a period and an asterisk (".*").

A period matches any character except the line break.

An asterisk matches zero or more occurrences of the symbol immediately before it.

As a result, this combination matches zero or more characters that are not line breaks.

Example: A "Catch-All" Mailbox Rule

This example demonstrates how you can use a ".*" combination to match every inbound message:

```
Filter = "Subject contains"
Filter String = ".*"
```

Example: How to Use the Mailbox Rules TextAPI Defaults and TextAPI Ignore Incoming Settings

The TextAPI Defaults and TextAPI Ignore Incoming fields let you specify default values for incoming mailbox rules, and specify TextAPI commands that should not be accepted in incoming emails. These fields work with the default values that are set in the [EMAIL_DEFAULTS] section and with the forbidden-commands list in the [EMAIL_IGNORE_INCOMING] section of the text_api.cfg file. When a conflict occurs between the definition in a mailbox rule and the definition in the text_api.cfg file, the value set in the mailbox rule applies.

The TextAPI Defaults field includes TextAPI keyword commands that are applied to a ticket when it is created from an email that matches a mailbox rule. The commands are not applied when the message affects an existing ticket.

Follow these steps:

1. Place each command on a separate line in the TextAPI Defaults field.
2. Format the commands as follows:

   ```
   OBJECT.FIELD=value
   ```

   > **Note:** Do not include a leading percentage symbol (%), used only for corresponding comma embedded in the body of the email.

   For example, format the commands as follows:

   ```
   REQUEST.PRIORITY=3
   PROBLEM.CATEGORY=Facilities
   INCIDENT.GROUP=Plumbing
   ```

The TextAPI Ignore Incoming field lists TextAPI keyword commands that are not permitted to be used in the text of the incoming email message. Any commands that are listed in this field are ignored when they are found in an incoming email message.

To specify TextAPI Ignore Incoming commands, follow these steps:

1. Place each command on a separate line in the TextAPI Ignore Incoming field.
2. Format the commands as follows:

   ```
   OBJECT.FIELD
   ```

   > **Note:** Do not include a leading percentage symbol (%), used only for the corresponding commands embedded in the body of the email.

   For example, format the commands as follows:

   ```
   CHANGE.ASSIGNEE
   PROBLEM.GROUP
   REQUEST.EFFORT
   ```

3. Define all commands used in either field in the [KEYWORDS] section of the text_api.cfg file. This file is located in the “site” subdirectory of the CA SDM installation directory.

Mailbox Policy Fields

Email Address/Hour
Specifies the maximum number of emails per email address per hour. You can specify the following values:

- -1 -- No limit (default)

- 0 -- No emails allowed.
- 1 – Maximum number of emails allowed.

Log Violation
Logs the violation to the standard log. You can specify the following values:

- Do not log
- First violation only (default)
- All violations

Note: The First violation only option keeps a list of email addresses associated with messages that violate mailbox policies and uses the list for the log to avoid duplicate log entries. The list is cleared when the Mail Eater daemon is restarted. However, if you change the setting from First violation only to one of the other options and back, the list of email addresses which were logged under this setting is not cleared. If a mailbox logs numerous violations while using this setting, we recommend that you restart the Mail Eater daemon periodically to clear the list, or use the Do not log option.

Inclusion List
Specifies email addresses or domains that are allowed to process emails -- only emails matching the list are allowed. You can specify multiple addresses or domains by delimiting them with a comma, semicolon, space character, or line break. An entry of an asterisk ('*') by itself is the "World Domain," and matches all domains that are not in the Exclusion List.

Exclusion List

Specifies email addresses or domains that are not allowed to process emails. You can specify multiple addresses or domains by delimiting them with a comma, semicolon, space, or line break.

Note: Addresses in the Exclusion List override any values in the Inclusion List. Addresses in the Inclusion List override domains in the Exclusion List, and can provide specific exemptions for specific senders in an otherwise-banned domain. Domains in the Exclusion List override the World Domain in the Inclusion List. The World Domain is not valid in the Exclusion List.

Multiple Mailboxes

CA SDM can process and manage multiple mailboxes. Each mailbox can have its own definition, instead of using a single global set of definitions. You can define multiple mailboxes and use different templates or default values for each mailbox. Multiple definitions let individual tenants use separate mailboxes, or let an individual tenant or organization use different mailboxes, and have different behaviors for each mailbox. You can set up multiple mailboxes by using the Administration interface. Each mailbox uses the following tables:

- usp_mailbox -- Defines the mailbox.
- usp_mailbox_rule -- Specifies a set of rules for each mailbox.
  Because mailbox rules supply Text API defaults, you can establish email interfaces with other software and parameters (such as category, assignee, and so on) that are configured specifically for the interface.

Note: IMAP servers support multiple mailboxes for a single account, but alternate mailboxes are not supported; only the default inbox is supported.

How Multiple Mailboxes Use Rules

The Mail Eater (pdm_maileater_nxd) component on the primary server uses mailbox connections and rules to read and process messages from one or more accounts on one or more mail servers. The Mail Eater processes mailboxes serially (only one mailbox is processed at a time), and processes rules in sequence number order.

Multiple mailboxes use rules as follows:

1. Upon primary server startup, the Mail Eater reads the following tables:
   - **usp_mailbox**
     Represents a connection to a mail server.
   - **usp_mailbox_rules**
     Represents the rules that apply to the connection (usp_mailbox).
   - **Contact_Method**
     Represents the Contact Methods used for automatic replies.
   - **Document_Repository**
     Represents the Document Repositories for storing attachments.

   The Mail Eater automatically detects changes to the objects in any of these tables, including the addition of additional objects. If a change is made to usp_mailbox or usp_mailbox_rule, the polling interval for the affected mailbox is rescheduled to one second after the change is applied.
2. At the interval defined by each mailbox, the Mail Eater retrieves each email in the inbox for the associated account, and processes the email as:
   a. Checks the email address for policy violations. When the Mail Eater finds a violation, processing stops, and the standard log is affected according to the mailbox definition.
   b. Compares the email to each rule (mailbox_rule) that belongs to that mailbox.

c. If a matching rule is found, the Mail Eater submits the message to the Text API for posting, and replies to the user as appropriate based on the specified action for the rule.
For reply emails, the filter string identifies the object and uses the Text API for processing. After processing is complete, the response goes either to the Reply to or the From address.

d. When a matching rule is located, no other rules are checked, and the Mail Eater processes the next email in the inbox.

e. If no matching rule is found, the message is discarded.

3. After the Mail Eater processes all emails for an inbox, the processed and discarded messages are purged from the mail server, and the next processing interval is scheduled.

How to Configure the Email Replies

This article contains the following topics:

The email notifications that you use in mailboxes are specific to the replies that are sent to a contact in response to their emails. For example, you can configure email so that when a contact clicks a reply link in an email notification, the reply email is directed to a mailbox.

Note: This setup differs from the regular email notifications.

Follow these steps:

1. Open the CA SDM Web UI (see page).
2. Verify that you have configured the mailbox for inbound email (see page 1256).
3. Configure the mail server (see page 1277).
4. (Optional) Specify a notification email address in the contact definition.

Note: Select Security and Role Management, Contacts on the Administration tab and select the contact to edit.

5. Modify the email notification method (see page 1278).

Open CA SDM Web UI

Log in to the web UI from the following servers, depending on your CA SDM configuration:

- Conventional: Primary or secondary servers
- Advanced availability: Application or background servers

Configure the Mail Server

Notifications for an event (automatic and manual notify) are sent using a single mail server definition.

Follow these steps:

1. Select Options Manager, Email from the Administration tab.
   The Option List page opens.
2. Click the email option (see page 1277) that you want to install.
   The Options Detail page opens.
3. Click Edit, complete the fields as appropriate, and click Install.
   The mail server is configured to send notifications (outbound mail).
4. Repeat the procedure until all relevant Option List options are configured.

Email Options

The email interface sends email notifications and lets users create tickets from an email.

Option	Description
mail_from_address	Specifies the mail notification From: address. The address is in the format Displayname<user@company.com (http://company.com/)>.
mail_login_password	Specifies the SMTP server login password.
mail_login_userid	Specifies the SMTP server login userid.
mail_max_threads	Specifies the maximum number of concurrent SMTP connections that can attempt to communicate with the server.
mail_reply_to_address	Defines the reply to address for email notifications. This option is useful if emails are sent from one user account, but you want replies sent to another email address. The default value is the same as the from address.
	Defines the domain name of the SMTP server. You can clear the domain name by setting the value to NONE.

Option	Description
mail_smtp_domain_name	
mail_smtp_hosts	Specifies a space-separated list of SMTP server host names for email notifications.
mail_smtp_host_port	Specifies an SMTP port to override the default SMTP port.
mail_smtp_security_level	Specifies the SMTP security level. Valid settings are: 0=no security, 1=basic authentication, 2=NTLM, 3=MD5 and 4=LOGIN. If you set this option to 1, set the mail_login_password and mail_login_userid options. Most SMTP servers do not require authentication.
mail_smtp_use_tls	Specifies the Transport Layer Security (TLS) usage in the email. The valid settings are Yes= Use TLS, No=Do not use TLS.
mail_ca_cert_path	Specifies the path where the trusted certificate has been deployed. **Note**: For the advanced availability configuration, you must deploy the trusted certificate on the same location in all the CA SDM servers. CA SDM supports only Base-64 encoded (PEM) format for CA Certificates.
mail_show_to_cc_list	Shows all the recipients of the email notification. For manual email notification, both “To” and “Cc” list recipients are displayed and for automatic email notification, only “To” list recipients are displayed. By default, this option is installed. **Note:** Pager email notification method does not support the listing of all recipients in To or CC list.

Modify the Email Notification Method

Modify the email notification method to configure the email replies.

Follow these steps:

1. Select Notifications, Notification Methods, Email on the Administration tab and click Edit.
2. On the Email Update Notification Method page, select the Supports SMTP checkbox to enable SMTP.
3. Enter pdm_mail [- F from_email_address] [- T reply_to_email_address] as the Notification Method.

- **from_email_address**
  Specifies the address that is used as the From address of the message. This address overrides the sender address in the outbound mail server configuration.

- **reply_to_email_address**
  Specifies the address to which replies are sent. This address overrides the reply-to address in the outbound mail server configuration.
  When a reply-to address is set in the outbound mail server configuration and no reply-to address is specified in the Notification Method, the reply-to address in the outbound mail server configuration is used with that Notification Method.

Note: If the keyword "$(REPLY_FROM)" is specified as either address, that address is constructed from the username and mail server hostname for the mailbox. This keyword is only valid when a mailbox rule uses the Notification Method; Notification Methods that use it must not be used for any other purpose. For example, user name=dev, server name=mail32.ca.com, $(REPLY_FROM) =dev@mail32.ca.com. Only use this keyword if your mail server is configured to accept the mail server name as equivalent to the email domain name. Use this keyword with caution: If the hostname is not fully domain-extended in the mailbox configuration (for example, mailserver1 instead of mailserver1.customer7.com), it is not extended automatically by the field interpreter.

Note: The from_email_address and reply_to_email_address are the addresses that appear in the From and Reply-To headers of the message when the user reads it. If the addresses are identical, you can specify only the from_address.

4. Click Save.
   The email notification method is modified. When the contact replies to the email notification, the reply is addressed by default to the specified mailbox.

Alternate Sender Address Identification

You can use a -m parameter in the subject of the message so that CA SDM identifies the sender of the message using a different email address from the one that originally sent it. The -m keyword, followed by a space and by the email address that CA SDM recognizes, must be the last elements of the subject line. Consider the following information when you use the -m parameter in the subject:

- Both the actual From address and the alternate address that is specified with -m are verified in the Inclusion and Exclusion lists.

- The email address that is specified as the alternate address must contain only the address, and not the accompanying display name.

- If more than one word follows the -m parameter in the subject line, the alternate address is not recognized.

Mailbox Polling

If an error occurs on the outgoing mail server, email notifications are not sent and queue in the %NX_ROOT%\site\mail_queue directory. When the mail server becomes active again, after an interval it processes and sends email. You can change the interval to recycle the email that was queued when the mail server was busy.

Notification email messages that the outgoing mail server fails to send are resubmitted until you do one of the following:

- Stop the Mail Daemon (pdm_mail_nxd) that handles outbound email notifications.
- Manually delete the messages from the %NX_ROOT%\site\mail_queue directory.

Set the Email Retry Interval Variable

You can define the time interval (in seconds) to retry failed attempts to send outgoing email to the mail server.

Note: CA SDM does not retry sending messages that the outgoing mail server accepts, but cannot be delivered. For these messages, the outgoing mail server retry capabilities and policies, if any, are in effect.

Retries are on a per-message basis. If the mail server is unavailable for a period, each message is retried when its own timer expires, rather than all the messages being sent at once. However, if you restart the outgoing mail daemon, all unsent messages attempt to be sent at that time, and if they all fail to be sent, their retry timers are all reset at the same time.

The setting (NX_EMAIL_RETRY_INTERVAL) in the NX.env file controls the retry interval. You can change the default retry interval setting on one or more servers.

Follow these steps:

1. Log in to the following server, depending on your CA SDM configuration:
   - Conventional: Primary server
   - Advanced availability: Background server.
2. Navigate to the $NX_ROOT directory
3. Use a text editor such as WordPad to open the NX.env file.
4. Modify the value of to the NX_EMAIL_RETRY_INTERVAL interval you want as follows:

   ```
   NX_EMAIL_RETRY_INTERVAL=number_of_seconds
   ```

   - **NX_EMAIL_RETRY_INTERVAL**
     Defines the time interval (in seconds) to retry failed email attempts.

- ***number_of_seconds***
  Specifies the number of seconds for each email retry interval. The default time is 600 seconds (10 minutes). The minimum value that you can use is 20 seconds. If you set a value that is less than the minimum of 20 seconds or more than 2000000 seconds, the default value of 10 minutes is used.

5. Save and close the file.

6. Restart the CA SDM servers (see page 913).
   The change takes effect.

How to Set Up the Data Partition

Data partitions can be assigned to individual contacts, but the preferred method is to assign data partitions based on access type. After associating data partitions with different access types, you can associate a contact to a particular access type, and define its data partition. The access type has a specific option to override the contact data partition.

To associate a data partition to an access type, you set up data partitions that are meaningful to your site and then select one of the data partitions when you define or modify an access type.

Important! Other CA SDM security settings can take precedence over data partition.

The data partition is a subset of CA SDM database that controls a user access to tickets and other data records based on their content.

For example, you can restrict a user view of the database to only those configuration items that are assigned to the user organization. You can also restrict a user to update only assigned tickets and allow read-only access to other configuration items.

A data partition consists of a set of constraints. The data partition constraints identify the table that is being controlled by the data partition and the constraint type. The constraint typesspecify what the user can do, such as create, delete, update, view, and so forth, within the data partition. After you assign a data partition to an access type, which you in turn assign to a user contact record, the constraints and constraint types are what control the user access to the records in the CA SDM database table.

You can also view constraints independent of the data partition using them. For example, you want to view all constraints for a specific table, regardless of the data partition.

Follow these steps:

1. Verify the prerequisites (see page)
2. Create a data partition (see page 1293)
3. Create an access type (see page 1285)

4. Configure Knowledge Management Data Partition Constraints for Role-Based Permissions (see page 1284)

Verify the Prerequisites

Before you set up the data partition, verify the following prerequisites:

- Data Security Structure and Policy (see page 1282)
- Data Partitions Setup (see page 1282)
- Constraint Specifications (see page 1283)

Data Security Structure and Policy

Planning data security involves enforcing restrictions to access the specific portion of the database. These restrictions can be enforced on individual contacts either through roles or access types:

- **Roles**
  Defines the functionality that users in the role are allowed to access. You can assign one or more roles to an individual contact record, or to an access type to define the functional access for all of the access types who are associated with contacts.

- **Access Type**
  Defines how contacts are authenticated when they log in to the web interface. For example, an access type decides whether the contacts can modify web forms or the database schema using Web Screen Painter and which roles are available for the contacts.

As a service desk administrator, you can modify the predefined access types and also create new ones. You can enforce the restriction to the individual users or a group of users through Roles.

Identify the following:

- The objects and the type of restrictions you want to enforce on these objects.
- The Users or Roles on whom the Data Partition are applied. Data Partitions can be applied to contacts directly, but the preferred method is to assign data partitions based on the role and assign this role to all the contacts directly or through the access type.

Data Partitions Setup Specifications

You can define an unlimited number of data partitions. Each data partition consists of a set of constraints and validations on each database table that is restricted by the data partition. For each table in a data partition, you can specify independent authorizations to view, update, create, or delete records using criteria that are specified in a format similar to an SQL WHERE clause. You can base the restriction on any attribute in the record being accessed, combined with any data in the user contact record. This allows considerable flexibility when defining data partitions. For example, using the Vendor field in the Contact table allows data partition restrictions to be placed on vendors that are permitted to access CA SDM directly.

For performance reasons, CA SDM does not allow a data partition constraint to contain a Cartesian join. A Cartesian join results from a constraint containing an “OR” that does fully restrict all joined tables on both sides of the OR. To ensure that your data partition constraint does not produce a Cartesian product join, enter the following command:

- **Windows**

```
bop_cmd -f $NX_ROOT\bopcfg\interp\bop_diag.frg "check_queries()"
```

- **UNIX**

```
bop_cmd -f $NX_ROOT/bopcfg/interp/bop_diag.frg "check_queries()"
```

Important! Any data partitions that are flagged by this program must be updated appropriately.

Constraint Specifications

You specify constraints and validation tests in Majic using the object definition metalanguage.

Constraints that are defined in Majic closely resemble an SQL WHERE clause, with the following exceptions:

- Attribute names in the constraint are object attribute names, not the database attribute name from the schema.
- You can refer to the value of an attribute in the contact record for the logged-in user with a name of the following form, where *att_name* is the Majic name of the desired attribute:

  ```
  @root.att_name
  ```

  For example, specifying @root.location refers to the location ID of the current contact.
  You specify joins with a specification of the following form, where the *foreign-key* is the Majic name of the SREL attribute in the table for which you are writing the data partition constraint, and *attribute-in-referenced-table* is the Majic name of the attribute in the table being joined:

  ```
  foreign-key.attribute-in-referenced-table
  ```

  For example, to refer to the maintenance vendor of the asset that is associated with an incident report, specify the following:

  ```
  resource.vendor_repair
  ```

  This specification is recursive. For example, you could refer to the name of the vendor with the following name:

  ```
  resource.vendor_repair.name
  ```

The following table contains examples of valid constraints to use for the Change_Request table, used to store change order information:

Constraint Type	Code and Description
View	assignee.organization = @root.organization Specifies the user can only view change orders where the assignee's organization is the same as the user's organization.
Pre-Update	requestor = @root.id Specifies the user can only update the change orders where he is the caller or requester.

However, you cannot write a constraint that uses joins on both sides of the expression, as shown in the following example:

```
assignee.org = requestor.org
```

Configure Knowledge Management Data Partition Constraints for Role-Based Permissions

Knowledge Management data partitions are enabled to let you use group and role permissions by default in CA SDM. If you are upgrading from a previous release, the migration tool updates your data partition constraints.

If you used custom data partition constraints to manage knowledge permissions in a previous release, update the constraints manually for the O_INDEXES and SKELETONS tables. You can view the default data partition constraints and apply the changes, as appropriate to your environment.

Follow these steps:

1. Select Security and Role Management, Data Partitions, Data Partition Constraints on the Administration tab.
   The Data Partition Constraints List page opens.

2. Click Show Filter and search use the following search criteria:

   - **Service Desk Analyst** in the Data Partition search.
   - **O_INDEXES** in the Table search.

3. Edit the View constraint type by modifying the Constraint tab to replace "READ_PGROUP in @root.pgroups" as follows:

   ```
   READ_PGROUP in @root.pgroups OR
   READ_PGROUP.[pgroup]contained_roles.role IN @root.id
   ```

4. Save the constraint.

5. Edit the Delete and Pre-Update constraint types by modifying the Constraint tab to replace "WRITE_PGROUP in @root.pgroups"as follows:

```
WRITE_PGROUP in @root.pgroups OR WRITE_PGROUP.[pgroup]contained_roles.role IN
@root.role
```

6. Save the constraints.

7. Repeat the steps to update the View, Delete, and Pre-Update constraints in the SKELETONS table in your data partition.
   The data partition constraints are updated.

Create an Access Type

Access types define how contacts are authenticated when they log in to the web interface, whether the contacts can modify web forms or the database schema using Web Screen Painter, and which roles are available for the contacts.

You can modify the predefined access types and create new ones.

The access types define all aspects of security. Several predefined access types are included, and you can modify them or can define new ones. Each access type for a user controls the following aspects of system behavior:

- How CA SDM performs the web authentication when the user logs in.
- The access level for the user.
- Whether the user can modify web forms or the database schema using Web Screen Painter.
- What are the roles available to the user.

Follow these steps:

1. Select Security and Role Management, Access Types on the Administration tab.
   The Access Type List page opens.
   Default: 15

2. Click Create New and complete the access type fields (see page), as appropriate, on the Create New Access Type page.

3. Use the tabs to complete the following tasks:

   - Configure Web Authentication for an Access Type (see page)
   - Assign Web Screen Painter Permissions to an Access Type (see page)
   - Assign Roles to an Access Type (see page)

4. Click Save.
   The access type is created.

Access Type Fields

The following fields appear on the Create Access Type, Access Type Detail, and Update Access Type pages.

- **Symbol**
  Specifies a unique identifier for the access type.
- **Default?**
  Indicates whether this access type is the default that is associated with contacts.
- **Record Status**
  Specifies whether this access type is Active or Inactive.
- **Description**
  Describes the access type. Use this field to help identify the characteristics of the access type.
- **Receive Internal Notification**
  Determines whether the contacts associated with the access type receive internal notification of activities that are related to tickets.
- **Access Level**
  Determines which access types a user can grant to another user. A user can assign an access type to the contact record of another user only if the access level of the access type they are attempting to assign is ranked the same as or lower than the grant level for their own access type. The levels are ranked as follows:
  - Admin (highest)
  - Analyst
  - Cust/Emp
  - None (lowest)
- **Licensed?**
  Determines whether this contact is a licensed access type. Contacts assigned to unlicensed access types can only view or update their own personal data.

Note: KPIs count the concurrent usages of the users from the system (for example, CA SDM Web UI, SOAP Web Services, REST Web Services, and so on). For example, the webConcurrentLicenseCt KPI counts the maximum number of unique users (with the "Licensed?" option selected) logged in to the CA SDM Web UI during the interval.The following fields appear on the Create Access Type, Access Type Detail, and Update Access Type pages.

Configure Web Authentication for an Access Type

You can configure the web authentication and validation type to specify how roles assigned to this access type are authenticated when users attempt to access the CA products. Complete the following fields in the **Web Authentication** tab.

- **Allow External Authentication**
  Select this check box if you want to allow contacts to be authenticated externally, for example by the HTTPD server or the operating system. If you select this option, users with this access type are validated by the appropriate external method as configured during installation. Checks ensure that no external validation has taken place (for example, that the user has not attempted access through a non-secure server) and that the user is defined as a valid contact in the system using the login ID. Then, it uses the access type to determine the correct interface to use.

- **Validation Type**
  Defines how users are authenticated when an external authorization is either not permitted or fails (for example, if the user is attempting access through a non-secure server). The available options are:

  - **No Access**
    Denies access to CA products unless external authentication is allowed and is valid.

  - **Open**
    Access to the CA products are always allowed, with no additional authentication required.

  - **OS**
    Access to the CA products are allowed through operating system user name and password.

  - **PIN / PIN Number**
    Users of this type can access only if they enter the correct value for the PIN field in their contact record. If you select the PIN option, you can choose which field in the contact record stores the PIN by entering the field attribute name in the PIN Field edit box.

  - **CA EEM**
    Access to the CA products are allowed through CA EEM. This option is available only if CA SDM is integrated with EEM.

Assign Web Screen Painter Permissions to an Access Type

The Web Screen Painter (WSP) utility allows CA SDM users to build and publish web forms and schemas. The Web Screen Painter tab also controls the database access for Web Screen Painter preview sessions. For the details about WSP, see Using the Web Screen Painter (WSP) (see page 1898).

Select the permissions that you want to allow for an access type in the Web Screen Painter tab.

- **Modify Forms**
  Allows the users to do the changes to existing forms without doing the changes available to all users.

- **Modify Schema**
  Allows the users to do the changes to an existing schema without doing the changes available to all users.

- **Publish Forms**
  Allows the users to make their modified forms available to all users.

- **Publish Schema**
  Allows the users to make their modified schema available to all users.

- **Preview Session Can Update Database**
  Allows the users to do the changes to the database during a preview session. By default, database changes are not allowed during a preview session.

Assign Roles to an Access Type

Assign the roles to an access type to limit contacts access to functional areas for assigned roles.

Follow these steps:

1. Select the following roles for this access type:

   - **Reporting Role**
     Defines the reporting access for this type.

   - **REST Web Service API Role**
     Defines the access to the REST web services for this type.

   - **SOAP Web Service API Role**
     Defines the access to the SOAP web services for this type.

   - **Command Line Utility Role**
     Defines the access to the command-line utilities for this type.

2. Click Update Roles.
   The Role Search page opens.

3. Enter any search criteria that you want to limit the list to the roles of interest, and then click Search.
   The Roles Assigned - Update page opens, listing the roles that matched the search criteria.

4. Select the roles that you want to assign. To select multiple items, hold down the CTRL key while clicking the left mouse button.

5. Click the double right-directional arrows, after you have selected all the roles that you want.
   The selected roles move to the Roles Assigned list on the right.

6. Click OK.
   The Access Type Detail page opens, with the assigned roles listed on the Roles tab.

7. Click Save.
   The Access Type Detail page opens, with a confirmation message that your changes have been saved.

8. Select the role that you want to be the default for this access type upon login. Click Set Default Role.
   Your selection for the default role is saved.

- **Symbol**
  Specifies a unique identifier for the access type.

- **Default?**
  Indicates whether this access type is the default that is associated with contacts.

- **Record Status**
  Specifies whether this access type is Active or Inactive.

- **Description**
  Describes the access type. Use this field to help identify the characteristics of the access type.

- **Receive Internal Notification**
  Determines whether the contacts associated with the access type receive internal notification of activities that are related to tickets.

- **Access Level**
  Determines which access types a user can grant to another user. A user can assign an access type to the contact record of another user only if the access level of the access type they are attempting to assign is ranked the same as or lower than the grant level for their own access type. The levels are ranked as follows:

  - Admin (highest)
  - Analyst
  - Cust/Emp
  - None (lowest)

- **Licensed?**
  Determines whether this contact is a licensed access type. Contacts assigned to unlicensed access types can only view or update their own personal data.

  Note: KPIs count the concurrent usages of the users from the system (for example, CA SDM Web UI, SOAP Web Services, REST Web Services, and so on). For example, the webConcurrentLicenseCt KPI counts the maximum number of unique users (with the "Licensed?" option selected) logged in to the CA SDM Web UI during the interval.

Data Partitions

Contents

Data partitions are subsets of the database with restricted access to data records. Restrict access by defining a set of constraints for each data partition. Assign these data partitions to access types. The data partition assignment determines the records that the contact can access.

Create a Data Partition Constraint

Data partition constraints restrict the database record access for users that are assigned to the data partition.

Follow these steps:

1. Select Security and Role Management, Data Partitions, Data Partition Constraints on the Administration tab.
   The Data Partition Constraints List page opens.

2. Click Create New.
   The Create New Data Partition Constraint page opens.

3. Complete the data partition constraint fields (see page), as appropriate.

4. Complete the information in the tabs, as appropriate:

   - **Constraint**
     Specifies the criteria that controls the records in the table and can be viewed, created, updated, or deleted by a user that is assigned to the data partition. For example, you can specify that users can only update issues that are assigned to them. When a user in the data partition requests a record that does not match the condition then the record is read-only.
     Limit: 4000 bytes

   - **SQL Translation**
     Displays the constraint definition in SQL format. The condition that you entered on the Constraint tab is validated, and the underlying SQL WHERE clause is built. This translation is displayed on the SQL Translation tab for the verification.

5. Click Save.
   The constraint is saved and added to the data partition.

Example: Create a Data Partition Constraint for CAB Assignments

You can create a data partition constraint that lets users update only change orders that are assigned to a CAB to which the logged in user belongs.

To create a data partition constraint for CAB change order user assignments, assign the following constraint values for a Change_Request controlled table in a data partition:

- Constraint type: Pre-Update

- Constraint specification: cab.[group]group_list.member IN (@root.id (http://root.id))

The logged in user can only update change orders that are assigned to a CAB to which the user belongs.

Constraint Definition

Specify the condition in Majic format (the metalanguage used to define CA SDM objects).

If the Constraint Type is View, the condition can include joins to other tables and references in the form @root.att_name to Majic attributes in the contact record for the logged-in user. Otherwise, it cannot include joins to other tables, but it can include references in the form @root.att_name to Majic attributes in the contact record for the logged-in user.

If the Constraint Type is Defaults, you may specify one or more assignment statements, separated by semicolons, which specify values to be assigned to empty fields in a new record at the time the record is stored. The syntax of each assignment statement is:

```
att_name=value
```

where att_name is the name of a Majic attribute from the record, and value can be an integer, a string enclosed in quotes, or a reference in the form @root.att_name to a Majic attribute in the contact record for the logged-in user. The way CA SDM uses default values depends on the table they affect.

For tables updated by CA SDM, such as Issues, default values are placed into the record at the time it is displayed, and are shown on the initial display of a new record. A default value can be assigned to a reference field (a Majic SREL) by coding it in the form of a persistent ID (a table name followed by a colon and an integer ID). For example, you might set a default value for category by including the following in the Defaults specification:

```
category='PCAT:12345'
```

where 'PCAT' is the target of the SREL, as shown in the Majic file, and 12345 is the ID number of the desired category. You can list persistent IDs for a table with a command of the form:

```
bop_odump domsrvr pcat "" sym
```

Data Partition Constraints Fields

Complete the following fields to add or modify the data partition constraint fields:

- **Data Partition Name**
  Specifies the name of the data partition for which the constraint being defined.

- **Table Name**
  Specifies the database table that is controlled by the constraint.

- **Constraint Type**
  The type of constraint being defined. There are six constraint types for each table in a data partition.

  - **Create**

  Specifies the criteria that must be met before creating a record. When a user in the data partition attempts to create a record that does not match the create test condition, CA SDM displays the error message that is associated with the constraint and does not save the record.

  - **Defaults**

Specifies one or more assignment statements, separated by semicolons, defining values to be assigned to empty fields in a new record at the time the record is stored. The syntax of each assignment statement is, where *att_name* is the name of a Majic attribute from the record, and *value* can be an integer, a string that is enclosed in quotes, or a reference in the form @root.*att_name* to a Majic attribute in the contact record for the current user:

```
att_name=value
```

For tables updated for tickets, default values are placed into the record at the time it is displayed and are shown on the initial display of a new record. You can assign a default value to a reference field (a Majic SREL) by coding it in the form of a persistent ID. A persistent ID is an object name followed by a colon and an integer ID. For example, you can set a default value for category by including the following in the defaults specification, where PCAT is the target of the SREL (as shown in the Majic file) and 12345 is the ID number of the desired category:

```
category='PCAT:12345'
```

You can list persistent IDs for an object using a command of the form:

```
bop_odump domsrvr pcat "" sym
```

- **Delete**

Specifies the criteria that must be met to delete a record. When a user in the data partition attempts to delete a record that does not match the delete condition, CA SDM displays the error message that is associated with the constraint and does not delete the record.

- **Pre-Update**

Specifies the records in the controlled table that a user can update in the data partition. When a user in the data partition requests a record that does not match the pre-update condition, CA SDM makes the record read-only and displays the error message that is defined with the constraint.

- **Update**

Specifies the criteria that must be met when a record is saved. When a user in the data partition attempts to save a record that does not match the update condition, CA SDM displays the error message that is associated with the constraint and does not save the record.

- **View**

Specifies the records in the controlled table that a user can view in the data partition. This constraint is automatically applied to all lists selected by a user in this data partition, in addition to any selection criteria explicitly specified by the user.
View can include joins to other tables and references in the form @root.*att_name* to Majic attributes in the contact record for the current or logged-in user. The valid examples are:

```
requestor.organization = @root.organization
```

```
requestor.organization.name = 'MIS'
```

```
assignee = @root.id

assignee.organization = @root.organization
```

Note: The Create, Delete, Pre-Update, and Update constraint types now support joins to other tables. They can also include references in the form @root.attribute to attributes in the contact record for the current user.

- **Record Status**
  Indicates whether the constraint is active or inactive.

- **Error Message**
  Specifies the message returned to the user, if the constraint criteria is not met. For example, "You can only update issues assigned to you" or, "You can only create issues for your organization" or, "You can update your contact record but cannot change the data partition."

Create a Data Partition

A data partition is a subset of a CA SDM database. Data partition controls a user access to tickets and other data records based on their content.

Follow these steps:

1. Select Security and Role Management, Data Partitions, Data Partitions List on the Administration tab.
2. Click Create New.
3. Complete the fields as appropriate:
   - **Data Partition**
     A unique identifier for the data partition.
   - **Record Status**
     Record status whether the partition is active or inactive.
4. Click Save.
5. Click New Constraint and attach constraint definitions to the partition.
6. Click Save.
   The data partition is saved with the data partition constraint.

How to Configure Notifications

This article contains the following topics:

With CA Service Desk Manager, you can automatically notify key personnel about ticket activities (researching, escalating) and events (opening a ticket, for example). You can also notify key personnel about Knowledge Report Card (KRC) and Support Automation Assistance Sessions. When a significant activity or event occurs, CA Service Desk Manager creates a notification message that does the following:

- Identifies the ticket activity or the notification event
- References the ticket
- Includes other optional information
- Can identify potential contacts

You can view a notification message for a ticket because of a system action. A system action includes opening, closing, or modifying a ticket through its history information.

Setting up automatic notifications involves the following tasks:

- Defining activity notifications that determine the types of activities that generate notifications.
- Defining object contact notifications that determine the object contacts that can be used to send notifications in an activity notification.
- Identifying the methods used to send messages.

How to Create Object Contact Notifications

Object contact notifications let you notify the recipients based on the current value of a field on the ticket. Instead of identifying a person to notify, as in a notification method, you identify an object. For example, you can identify the To field to ensure that notification goes to the person currently identified in the To field, even if the value has changed since the ticket was defined.

Follow these steps:

1. Select Notifications, Object Contact Notifications on the Administration tab.
   The Object Contact Notification List page opens.

2. Click Create New.
   The Create New Object Contact Notification page opens.

3. Complete the following fields:

   - **Symbol**
     Defines a unique identifier for the object contact notification.

   - **Status**
     Specifies if the object contact notification is active or inactive.

   - **Object Type**
     Displays the name of the object to which the attribute applies.

   - **Object Attribute Name**
     Provides the name of the object contact notification (in the Symbol field) in Majic, which is internal CA code. The attribute name depends on the Object Type selection:

     - If the Object Type is Issue or Workflow Task, the attribute name is assignee, requester, or group; these are the attribute names in the chg objects and they map to fields in the Change_Request tables.

     - If the Object Type is an Issue Activity log, the attribute name must start with the attribute name in the activity log object that links it to a specific instantiation of the chg object. The attribute name could be change_id.group.

   - **Description**
     Describes the object contact notification.

4. Click Save.
   The new object contact notification is displayed in the Object Contact Notification List.

Manual Notification Recipients List

You can set up a default set of Available Recipients that the Manual Notification composition page presents for requests, incidents, and problems. Available Recipients streamline the manual notify process for analysts because you can set up a list of contact objects (for example, Affected End User) or individual contact names for easy use as recipients of manual notifications.

Adding an Object Contact Recipient adds the individual contact names that the Object Contact represents to the Recipients list (consolidating any duplicate entries). The same contact can be referenced multiple times for different Contact Objects such as Assignee and Affected End User. Some entries, such as the Stakeholders List contact object, can add multiple entries to the Recipients list.

Contacts and Contact Objects remain in the Available Recipients list after you add them to the list. This behavior lets you remove recipients without affecting the initial Available Recipients list.

Example: How the Available Recipients List Works

The following examples demonstrate how default recipients streamline the manual activity notification process.

Object Contact Recipients includes the following entries:

- UserA belongs to the "Assignee" and "Affected End User" Contact Objects.

- Stakeholders List includes multiple contact names. For example, UserB and UserC.

You do the following actions:

- Add both Contact Objects that refer UserA to the Recipients list.
  Only one UserA entry is listed in the Recipients list.

- Accidentally remove UserA from the Recipients list.
  You do not have to refer to the ticket to get the UserA name and search to add it back. You can quickly add UserA to the Recipients list because UserA is listed in the Available Recipients list.

- Accidentally remove one contact name, such as UserC, from the Recipients List which came from the Stakeholders List.
  You can add the Stakeholders List from Object Contact Recipients to add the contact name again. Because duplicate entries are consolidated, other Contacts in the Stakeholders List who were not deleted from the Recipients List are not affected.

Previous Assignee Notifications

You can define Previous Assignee or Group values for an activity notification that detects changes to key fields when a ticket is saved. Previous values let you notify a previous assignee when a ticket is transferred, or notify both the current and previous groups when the priority of a ticket is escalated.

The Previous value fields of a ticket are local fields that exist only in memory and not in the database. The fields are populated during the save operation of the ticket only when respective attributes are changed and cleared at the completion of the notification processing. A previous value field is associated with a particular activity type through an activity association.

You can define Previous values that detect changes to the following key fields of a ticket:

Field	Requests, Incidents, Problems	Change Orders	Issues
Status	Yes	Yes	Yes
Active	Yes	Yes	Yes
Assignee	Yes	Yes	Yes
Request Area/Category	Yes	Yes	Yes
Group	Yes	Yes	Yes
Impact	Yes	Yes	Yes
Priority	Yes	Yes	Yes
Urgency	Yes	No	No
Severity	Yes	No	No

There are several contacts that you can specify for each object type (request, incident, problem, change order, or issue), which notify the current and previous contacts when an activity occurs.

- **Assignee** -- Person assigned to handle the ticket.

- **Assignee Previous** -- Person previously assigned to handle the ticket.

- **Group** -- Group assigned to handle the ticket.

- **Group Previous** -- Group previously assigned to handle the ticket.

After the notification rule is saved, the Assignee Previous and Group Previous fields display on the Object Contact Notifications List page.

Example: Configure Current and Previous Values for Key Fields

The following usage example describes how an administrator configures current and previous values for key fields to help ensure that the previous support representative is notified when a request is transferred away from them.

1. **Situation --** A support representative is frustrated because a ticket was transferred away from them and they were never notified.

2. **Task --** The administrator adds the Assignee and Assignee Previous object contacts to the notification rule for the Transfer activity notification. They attach a message template and specify the current and previous assignees to notify on the request form.

3. **Action --** When the request is saved, the Assignee and Assignee Previous fields of the request are populated. When the activity occurs (ticket is transferred), the condition for the rule is evaluated.

4. **Result --** If the condition is met, a notification message that describes the ticket activity is sent to the current assignee and the previous assignee.

Notify Contacts When a Ticket is Transferred Example

You can notify both the current and previous contacts when a CA SDM ticket is transferred.

Example: Notify both the current and previous contacts when a ticket is transferred

1. On the Administration tab, browse to Notifications, Activity Notifications.
   The Activity Notifications List page appears.

2. Select the Transfer activity notification.
   The Transfer Activity Notification Detail page appears.

3. In the Object Type field, select Requests/Incidents/Problems.

4. On the Notification Rules tab, under Symbol, select the Default Transfer Notification Rule.
   The Default Transfer Notification Rule page appears.

5. On the Object Contacts tab, click Update Object Contacts.

6. Click Search.
   The Notification Rule Update Recipients page appears.

7. From the Object Contacts list, select Assignee and Assignee Previous from the list on the left, and click the contact selection button (>>).
   The selected item is added to the list on the right.

Note: Use the CTRL or SHIFT keys plus the left mouse button to select multiple object contacts.

8. Click OK.

9. Save the notification rule.
   The Object Contacts list displays the selected object contact.

10. On the Default Transfer Notification Rule page, click Message Template. Select a template and ensure that the Auto Notification option is enabled.

11. Create a request, specify an Assignee, and click Save.

12. On the Request Detail page, select Activities, and Transfer from the File menu.

13. Specify a new Assignee, and click Save.
    The notification is sent to the current and previous assignees when the transfer activity occurs.

Configuration Item Notifications

A configuration item (CI) notification lets you define an activity notification that is associated with a specific CI that is associated with a specific CA SDM ticket. This feature lets you track information about the users, organizations, and vendors of a CI.

You can specify the CI object contacts on the Notification Rules Update Recipients page, such as CI Maint Org, CI Primary Contact, and so on.

Notify the Primary Contact of a Configuration Item for an Issue Example

You can define an activity notification for a primary contact that are sent for a specific CI for a specific CA SDM ticket.

Example: Notify the primary contact of a configuration item for an issue

1. On the Administration tab, browse to Notifications, Activity Notifications.
   The Activity Notification List page appears.

2. Select the Initial Activity Notification from the list.
   The Initial Activity Notification Detail page appears.

3. Select the object type you want to use.

4. On the Notification Rules tab, select the Default Notification Rule link.
   The Default Notification Rule page appears.

5. Select the Default Message Template link and ensure that the Auto Notification option is enabled.

6. Select the Object Contacts tab, and click Update Object Contacts.
   The Object Contact Notification Search page appears.

7. Click Search. A list of object contacts appears.

8. Select CI's Primary Contact from the list on the left, and click the contact selection button (>>).
   The selected item is added to the list on the right.
   You can use the CTRL or SHIFT keys plus the left mouse button to select multiple object contacts. You can add one object for a request and multiple objects for a change order or issue.
   The object contact is in the list on the right.

9. Click OK.

10. Save the notification rule.
    The Object Contacts list displays the selected object contact.

11. Complete the following tasks:

    - On the Service Desk tab, create or update an existing CI.
    - Add the primary contact listed on the Object Contacts tab. The selected object contact appears on the Configuration Items Detail page.
    - Add the CI to the Issue.

When an activity event occurs, the rule is implemented and the condition is evaluated. If the criteria for the condition is met, a notification message that describes the ticket activity is sent to all contacts of the CI associated with this notification rule.

Notification Log Reader

The Notification Log Reader displays the notifications received for the logged-in user by date, urgency, and status. With the Notification Log Reader, you can do the following:

- Change the sort order and set menu options to have the Notification Log Reader appear automatically when new messages are received.
- Double-click a notification message to request that CA SDM display the detail page for the ticket associated with the notification.
- Monitor notification messages by entering specific selection criteria to query the database for analysis or for selection of notification messages based on data entered in the fields. For example, you can list only those notification messages that have not been cleared by changing the Message Status field to Not Cleared.
- Clear notification messages to keep your list of notifications to a manageable size. Cleared notifications are not displayed when you first access the Notification Log Reader, although you can display them, if needed.

Set Notification Log Reader Options

You can set options for the Notification Log Reader to define how you are notified when new messages are received for an issue.

Follow these steps:

1. On the ServiceDesk tab, browse to View, Log Reader.
   The Notification Log Reader page appears.

2. Use the check box to the left of each notification to set the following options. You can select items to perform operations such as Clear Selected or Delete Selected.

   - **Header**
     Displays the header of the message, which usually contains the number of the ticket and the activity type.

   - **Start Date**
     Displays the date and time the notification was sent to your Log Reader window.

   - **Status**
     Displays the status of the notification.

   - **Urgency**
     Defines the level of urgency for the notification (low, normal, high, or emergency), which indicates the relative importance of different activities. Urgency levels are predefined; however, the system administrator is responsible for setting up other aspects of notification, such as notification methods and activity associations. The system administrator also defines the method of notification used for contacts and groups for each urgency level.

   - **Message Text**
     The full message text for the notification.

   The Log Reader displays any changes.

3. Click Close.
   The Notification Log Reader page closes and the options are set.

Personalized Responses

You can create personalized responses and attach them to requests, issues, and change order records when adding activities to the record. For example, you can append a personalized response on the Status Change or Log Comment windows available from the Activities menu.

Create a Personalized Response

You can create a personalized response to append to requests, issues, and change order records.

Follow these steps:

1. From the Administration tab, navigate to Service Desk, Personal Responses.
   The Personal Response list page displays.

2. Click Create New.
   The Create New Personalized Response page displays.

3. Complete the fields on the page:

- **Response Owner**
  Specifies the contact who owns the response. If this field is left blank, the response is available to all analysts.

- **Response**
  Specifies the text delivered to all those who receive this response. This field can be up to 1000 characters long.
  You can use variables in this field, for example:

```
Ticket ref_num: @{call_req_id.ref_num}

Assignee: @{call_req_id.assignee.combo_name}

Customer: @{call_req_id.customer.combo_name}

Description: @{call_req_id.description}
```

4. Select the type of records for which you want this response available. Click Save.
   A personalized response is created.

Personalized Response Variable Substitution

Variables can be embedded in the text of a Personal Response. These variables allow information to be substituted from the corresponding Request, Change Order, Issue, Problem or Incident. The syntax of the variables is the same as is used elsewhere in the CA SDM product, such as in the Activity Notification Message Templates and the Manual Notify Activity Message Text. The information can only be substituted from the corresponding Request, Change Order, Issue, Problem or Incident. Activity Notification Message Templates and the Manual Notify Activity Message Text allow information from the Activity Log Record to be included as well.

Check boxes for each object type (Requests, Change Orders, Issues, Incidents, and Problems) allow Responses to be filtered during selection. If the object type is not checked, the Response is not available for that object. For example, if only the Request box is checked, the Response is only presented in Activities for a Request.

A single Response can be used for all object types (Requests, Change Orders, Issues, Problems or Incidents). Because each object has different attributes, information that does not apply to the object is not substituted (for example, attempting to substitute the Request Number in a Response for an Issue).

A Response text example and the variable substitutions that occur for each object type follows:

```
This is Request # '@{call_req_id.ref_num}'
This is Change Order #' '@{change_id.chg_ref_num}'
This is Issue # '@{issue_id.ref_num}'
```

For a *Request*, the following substitution occurs:

```
This is Request # 'cr_demo:11'
This is Change Order # "
This is Issue # "
```

For a *Change Order*, the following substitution occurs:

```
This is Request # "
This is Change Order # 'chg_demo:3'
This is Issue # "
```

For an *Issue*, the following substitution occurs:

```
This is Request # "
This is Change Order # "
This is Issue # 'iss_demo:6'
```

By using the "Display this Response for" check boxes, you can create different versions of a Response with the appropriate substitution variables for the corresponding object (Requests, Change Orders, Issues, Problems or Incidents).

The format of the substitution variables for the different objects is as follows.

Object	Variable Format
Request / Incident / Problem	@{call_req_id.attr}
Change Order	@{change_id.attr}
Issue	@{issue_id.attr}

The substitution occurs when the Response is copied to the User Description field. The Response is copied after it is selected from the Personalized Response drop-down list and the drop-down list loses focus.

Internal Logs

You can define whether a particular access type is qualified to view internal logs. If allowed to view internal logs, contacts see a check box labeled Internal on each of the Log Activity windows, which they can select to mark the activity as internal. When activities are marked as internal, only contacts with an access type that is qualified to view internal logs sees the activity or is notified of it.

Administering CA Service Desk Manager

The Administrator role has full access to all product functionality. This role is used typically when implementing the product to help ensure that all users and roles are set up correctly. The Administrator role can also be used for a product environment that has a single person who performs all administration tasks.

Options Manager

Contents

The Options Manager lets you modify the functionality of your system. You can easily install and uninstall specific modified options.

Note: In advanced availability configuration, you can install or uninstall an option only from the background server. You can view the options and the descriptions from the application server.

The Options Manager pages list the applications that can be modified, the options that apply to those applications, and the values that are associated with the options, if any. They also provide descriptions of each option and indicate the status of each option (installed or uninstalled).

You can install these customization options when you install the rest of the product, or you can install any or all the options later. (Some options are automatically installed when you install the application that uses them.) You can also change the values of installed options at any time.

Important! Depending on your role, you may not have access to all the options.

Important! Installing or uninstalling an option requires you to restart the CA SDM servers. For advanced availability configuration, not all options require you to restart all the servers. Ensure that you read the Server Restart List (https://wiki.ca.com/pages/viewpage.action?pageId=103913584#id-.Install/UninstallOptionsManagerOptionsv14.1-ServerRestartList) before restarting any server.

Archive and Purge Options

Option	Description
busy_agent_threshold	Controls the threshold for processing the archive and purge background requests. For efficiency, requests in the background process queue should be processed during low system utilization ("non-busy" times). The Option Value field allows you to specify the number of the busy agents in a percentage. For example, if the Option Value is set to 70, the system starts processing requests in the background process queue when the percentage of busy agents is lower than 70 percent of the total agents in the system. The Option Value field sets the NX_BUSY_AGENT_THRESHOLD variable, which is located in the NX.env file.
default_schedule	The Option Value specifies the default schedule (workshift entry) used by the archive and purge rules. If the Option Value is set to an invalid workshift entry name or empty string, the rule does not execute the rule with the schedule value. The Option Value field sets the NX_DEFAULT_SCHEDULE variable, which is located in the NX.env file.
rule_history_length	The Option Value specifies the maximum number of rule history records saved in the database. The Option Value field is retrieved by archive and purge process at the startup. The default value for this variable is 50, which means 50 of the most recent rule history records are saved. The Option Value field sets the NX_RULE_HISTORY_LENGTH variable, which is located in the NX.env file.

Asset Information Service Options

Option	Description
allow_exceed	An asset/item contains an Inventory Count field. The number of parents an asset/item can have cannot exceed the inventory count. Installing this option allows the number of parents to exceed the inventory count.
allow_unrestricted_asset_upd	If installed, users can fully modify assets/configuration items owned by CA Asset Portfolio Management. If this option is not installed (the default), only a limited number of fields of the asset/item record can be updated.

Audit Log Options

These options control the logging of activities on the data partitions, change orders/issues, and requests. If these options are installed, an audit log entry is created for each field update and insert operation. The operation to be monitored is determined using the following options:

Option	Description
audit_ins	Monitors insertion.
audit_upd	Monitors field updates.

CA CMDB Options

Option	Description
allow_updates_to_inactive_ci	Specifies whether to permit inactive CIs to be updated. Default is NO (new installation) or YES (product upgrade). To uninstall this option, click Edit, Deinstall, Refresh. Then stop and restart the CA SDM server.
allow_updates_to_superseded_ci	Specifies whether to permit superseded CIs to be updated. Default is NO. To uninstall this option, click Edit, Deinstall, Refresh. Then stop and restart the CA SDM server.
ci_filter	Specifies whether to search for CIs in the CI List page. Default is YES. If the option is not installed, the CI search filter has no initial value. To uninstall this option, click Edit, Deinstall, Refresh. Then stop and restart the CA SDM server.
ci_hierarchy_levels	Specifies the number for levels (depth) to search for dependent services for CIs. Valid values are integers 0 (zero) through 9 (nine).
cmdb_model_class_inconsistency	Specifies to prevent, warn, or allow a CI class from being inconsistent with the class that a user specified in the optional CI model. ▪ **Prevent** Stops the CI save from occurring and displays an error message. ▪ **Allow** Allows the class and the class of the model to remain inconsistent. **Note:** Use this option for compatibility with earlier releases of the product, such as CA SDM r12.6. ▪ **Warn** Updates the standard log (stdlog) with a warning and lets the save occur. For example, use this option if you want to transition from Allow to Prevent. **Default:** Prevent

Option	Description
cmdb_versioning_maxrows	Specifies the maximum number of audit log and Change Order history entries that displays in the Versioning tab. **Default:** 400
critical_service_relationship	Specifies a relationship type to identify dependent services for CIs. You can specify multiple relationships separated by a comma. For example, supports, is managed by.

CA Process Automation Workflow Options

Option	Description
caextwf_eem_hostname	Specifies the name of the CA EEM server. For example, *http://<workflow_hostname>* identifies the authentication host. You install caextwf_eem_hostname only if you configured CA Process Automation to use CA EEM as an authentication server. CA SDM uses this value to transform a user name and password into a CA EEM token. Then, the user name and password do not pass in plain text over HTTP. **Note:** If the CA Process Automation installation is not using CA EEM, do not place a value in the caextwf_eem_hostname option, and do not install the caextwf_eem_hostname. Placing a false value or installing caextwf_eem_hostname when it is not necessary causes the integration to fail.
caextwf_endpoint	Specifies the URL that points to the CA Process Automation web services by including the CA Process Automation host name, port, and the mandatory /itpam/soap path. For example, *http://<workflow_hostname>:<workflow_tomcat_port>/itpam/soap* identifies the endpoint. If your implementation uses CA EEM, installing the caextwf_eem_hostname option is required for the integration between CA Process Automation and CA SDM to operate properly.
caextwf_log_categories	Specifies a comma separated list of CA Process Automation process instance log category names to appear on the CA SDM Request, Change Order, and Issue Workflow Tasks tab. For example, *Operator,Response,MyOwnCategory* supplies three log categories. You install caextwf_log_categories based on business decisions from the CA SDM and CA Process Automation process design personnel. This option adjusts the default data that appears on the Workflow Tasks tab for requests, change orders, and issues. When you install the caextwf_log_categories option, all CA Process Automation process instance log messages from the Process category and the categories that you specify appear on the Workflow Tasks tab. When you do not install caextwf_log_categories, only the CA Process Automation process instance log messages from the Process category appear on the Workflow Tasks tab. **Note:** For information about the CA Process Automation predefined log message categories, and defining custom message categories, see the CA Process Automation reference documentation.

Option	Description
caextwf_processdisplay_url	Specifies how to launch a graphical snapshot of a CA Process Automation process instance by supplying the host name and the mandatory /itpam/Web.jsp?page=runtimeeditor&ROID= path. For example, *http://<workflow_hostname>:<workflow_tomcat_port>/itpam/Web.jsp?page=runtimeeditor&ROID=* launches a snapshot of a process instance. On the Workflow Tasks tab of a request, change order or issue, the user selects View Process to see the snapshot. Installing the caextwf_processdisplay_url option is required for the integration between CA Process Automation and CA SDM to operate appropriately.
caextwf_retry_count	Specifies the number of times the CA PAM attached Workflow Events can be re-triggered to retry the Unknown status events. Default retry count value is 3 and range [1-20].
caextwf_retry_interval	Specifies the retry interval duration in minutes to re-trigger each unknown CA PAM Workflow events.Default retry interval duration is 10 and range [10-999].
caextwf_worklist_url	Specifies the process instance path by supplying the host name and the mandatory /itpam?page=tasklist path. For example, *http://<workflow_hostname>:<workflow_tomcat_port>/itpam?page=tasklist* enables CA SDM users to see a list of CA Process Automation process instances that require attention. The list appears in CA Process Automation when the CA SDM user selects a link associated with any listed task in the request, change order, or issue Workflow Tasks tab. Installing the caextwf_worklist_url option is required for the integration between CA Process Automation and CA SDM to operate properly.
caextwf_ws_password	Specifies the administrative password associated with the CA Process Automation user name from the caextwf_ws_user option. CA SDM uses the user name and password to access the CA Process Automation web service functions to perform integration activities such as selecting start request forms, process definition information, and process instance information. Installing the caextwf_ws_password option is required for the integration between CA Process Automation and CA SDM. The password and user name that you specify requires the appropriate access to CA Process Automation. However, it is not necessary for CA SDM to use the user name and password for authentication.
caextwf_ws_user	Specifies the CA Process Automation administrative user name associated with the CA Process Automation user name from the caextwf_ws_password option. CA SDM uses the user name and password to access the CA Process Automation web service functions to perform integration activities. Integration activities include selecting start request forms, selecting process definition information, selecting process instance information, or launching process instances. **Note:** Installing the caextwf_ws_user option is required for the integration between CA Process Automation and CA SDM to operate. The user name and password that you specify requires the appropriate access to CA Process Automation. However, it is not necessary for CA SDM to use the user name and password for authentication.

CA Service Catalog Options

To enable the self-service integration, install the following options:

Option	Description
casc_aty_sync	Specifies the type of activity logs to be synchronized from CA SDM to CA Service Catalog. If this field is left blank, Log Comment activity logs are synchronized. To synchronize other activity log types, (such as, Escalate, Update Status) enter the respective log type codes, separated by comma.
casc_endpoint	Specifies the CA Service Catalog Web Services URL. **Format:** http://<CA_Service_ Catalog_hostname>:<CA_Service_Catalog_portnum>/usm /services
casc_session_timeout	(Optional) Specifies the time in minutes for which the CA Service Catalog web services session will be cached. **Range:** 20 to 60 mins.
casc_user	Specifies the CA Service Catalog administrator username that is responsible for making the web service calls to CA Service Catalog. This user must exist in CA EEM against which CA SDM is configured.
casc_user_password	Specifies the password of the CA Service Catalog user as entered in the casc_user option.
casc_ws_retry	(Optional) Specifies the number of retries to synchronize a CA SDM ticket update (activity logs/ attachments/status) with CA Service Catalog, if there is a failure. Enter -1 to try indefinitely, until the synchronization succeeds. As a system administrator you can define the time interval after which you want the failed ticket update to be retried again. Run the following command to define the time interval:pdm_options_mgr -c -a pdm_option.inst -a option.inst -s NX_CASC_RETRY_INTERVAL -v [time interval in minutes] By default this time interval is set to 15 minutes. If you do not set any value or provide a non-numeric value to this variable, the failed update is retried according to the default time interval (15 mins.). **Range:** -1 to 50
casc_integrated	Enables the self-service integration.

Call Service Desk Options

Option	Description
call_service_desk_default_phone_number	Install this option and specify the value as a phone number for the mobile users to call the Service Desk using this specified number from their mobile.

Option	Description
call_service_desk_mobile_enable	(Installed by default) Enables the mobile users to call the Service Desk number from their mobile. The Service Desk number can be specified using the **call_service_desk_default_phone_number** or **call_service_desk_tenant_phone_number_field** (in case of multi-tenancy) option.
call_service_desk_tenant_phone_number_field	(Applicable if multi-tenancy is enabled) Install this option and set the value as phone_number or alt_phone, as specified in the tenant detail page. This option enables the tenant mobile users to call Service Desk using this specified number from their mobile.

Note: For more information, CA SDM Mobile application users can see the Mobility Wiki (https://wiki.ca.com/display/CASM/.Call+Service+Desk+from+your+Mobile+Device+v14.1) documentation

Change Order Mgr Options

Option	Description
asset_only_one_chg	Restricts Assets from being attached to more than one active change order.
Category_Defaults	Automatically fills certain fields on a change order detail page when the user selects a category. A category can have a default type, assignee, group, and organization/business. When this option is activated, the corresponding fields on the change order detail page are populated with category defaults if they have not been manually filled by the user. If the values are entered by the user, the default rule does not apply.
chg_allow_sla_downgrade	Alters the behavior of the chg_sla option by allowing the system to automatically downgrade a change order's Service Type. The chg_sla option selects the best Service Type from among several change order attributes, but cannot replace the change order's current Service Type with one of lesser rank. If this option is installed, the Service Types for all affected attributes are evaluated whenever one of the attributes changes. The change order's Service Type is set to highest ranked Type found, even if the new Service Type is lesser in rank to the change order's current Service Type. The Service Type with the smallest Rank value is considered the best service. If all the Service Types considered are equal in Rank (including Service Types with empty Rank values), the Service Type created first in the database is selected. The chg_sla option must be installed for this option to function correctly.
Auto Events	Automatically attaches events to newly created change orders. This attachment is specified using the following options: ▪ **chg_auto_events** -- Installs or uninstalls the option itself. ▪ **chg_auto_events_name** -- Specifies the format of a name for the attached events. ▪ **chg_auto_events_count** -- Specifies the number of events attached.

Option	Description
	Event names to be attached are constructed by joining the chg_auto_events_name to a number ranging from 1 to chg_auto_events_count. For example: ▪ chg_auto_events_name is "Auto Event" ▪ chg_auto_events_count is "3" With these settings, installing the chg_auto_events option would cause the following events to be attached to all new change orders: ▪ Auto Event 1 ▪ Auto Event 2 ▪ Auto Event 3 To complete the implementation of this option, you must define an event with these names. For more information, see create an event from How to Configure SLAs (see page 1099) topic.
chg_calendar_start_day_of_week	Specifies the start day of the week in the Change Calender. **Default:** Friday
chg_sla	Installs the rule for defaulting the Service Type field of a change order. The rule is as follows: ▪ The best service among the priority, requester, affected contact, and category is applied to the change order. ▪ The service type with the smallest rank value is considered the best service. If all the service types considered are equal in rank (including service types with empty rank values), the service type created first in the database is selected. ⚠ **Note:** This option is only available if the Classic SLA Processing Option is installed.
conflict_added	Generates Activity Log entries when conflicts are added.
conflict_updated	Generates Activity Log entries when conflicts are updated.
force_closure_code	Modifies the closure code value of children to be identical to the parent. The following values are valid: ▪ **Empty** - (Default) Forces the closure code value of the parent to the children when the child does not have a value for the closure code. It does not overwrite an existing closure code. ▪ **All** - Forces the closure code value of the parent to all children even if they already have a closure code value.
impact_explorer_exclude_hier	Used when building a list of child CIs for a CI in the Impact Explorer tree. If this option is installed and set to Yes, child CIs that are related through the CMDB Relationships tab of a CI Detail page are *not* displayed in the Impact Explorer tree or in the CI Descendants List.

Option	Description
	Note: Child CIs that are related through CA CMDB are displayed.
require_change_assignee	Prohibits change orders with no value in the Assignee field from being saved.
require_change_group	Prohibits change orders with no value in the Group field from being saved.
require_closure_code	Requires a closure code value prior to closing or resolving a change order.

Change-Issue Options

- **edit_completed_tasks**
  When this option is installed with a value of Yes, you are allowed to set both the "Allow Task Update" and the "Task Completed" flags on a Change Order or Issue Task Status detail. However, if you set both the "Allow Task Update" and the "Task Completed" flags, you can only update the Workflow Task Description. The default behavior is to not allow setting of both the "Allow Task Update" and the "Task Completed" flags on a Task Status detail.

Email Options

The email interface sends email notifications and lets users create tickets from an email.

Option	Description
mail_from_address	Specifies the mail notification From: address. The address is in the format Displayname<user@company.com (http://company.com)>.
mail_login_password	Specifies the SMTP server login password.
mail_login_userid	Specifies the SMTP server login userid.
mail_max_threads	Specifies the maximum number of concurrent SMTP connections that can attempt to communicate with the server.
mail_reply_to_address	Defines the reply to address for email notifications. This option is useful if emails are sent from one user account, but you want replies sent to another email address. The default value is the same as the from address.
	Defines the domain name of the SMTP server. You can clear the domain name by setting the value to NONE.

Option	Description
mail_smtp_domain_name	
mail_smtp_hosts	Specifies a space-separated list of SMTP server host names for email notifications.
mail_smtp_host_port	Specifies an SMTP port to override the default SMTP port.
mail_smtp_security_level	Specifies the SMTP security level. Valid settings are: 0=no security, 1=basic authentication, 2=NTLM, 3=MD5 and 4=LOGIN. If you set this option to 1, set the mail_login_password and mail_login_userid options. Most SMTP servers do not require authentication.
mail_smtp_use_tls	Specifies the Transport Layer Security (TLS) usage in the email. The valid settings are Yes= Use TLS, No=Do not use TLS.
mail_ca_cert_path	Specifies the path where the trusted certificate has been deployed. **Note**: For the advanced availability configuration, you must deploy the trusted certificate on the same location in all the CA SDM servers. CA SDM supports only Base-64 encoded (PEM) format for CA Certificates.
mail_show_to_cc_list	Shows all the recipients of the email notification. For manual email notification, both “To” and “Cc” list recipients are displayed and for automatic email notification, only “To” list recipients are displayed. By default, this option is installed. **Note:** Pager email notification method does not support the listing of all recipients in To or CC list.

General Options

Option	Description
add_utf8_byte_order_mark	Causes the default data to include an encoding signature (UTF-8 Byte Order Mark). Editors that support UTF-8 use this signature to display and maintain UTF-8 encoding.
catalog_server	Specifies the CA Service Catalog server location (for example: http[s]://*servername*:8090). If a load balancer is in use, verify that this option specifies the load balancer.
default_superuser_id	Specifies the default superuser ID for CA SDM, such as ServiceDesk.

Option	Description
Status_Policy_Violations	Specifies how strictly the system enforces **Status** policies. This option only applies to automated system processes, such as integrations and macros. The end user is unaffected by this option. Valid option values are: ▪ **Warn** -- Allows the status policy violation to proceed, but a warning message is written to the log. ▪ **Allow** -- Allows the status policy violation to proceed, but *no* warning message is written to the log. ▪ **Reject** -- Rejects the status policy violation and an error message appears.
singleton_notify_list	CA SDM sends the singleton daemon failure notification when it fails to restart a failed singleton daemon. This option controls the list of email recipients that will be notified when a singleton daemon fails to restart on the CA SDM server. Some fields in this page are self-explanatory. Following are the fields that need explanation: **Action Status** Indicates the installation status of the option. ▪ **Option Value** Specifies a list of comma-separated email addresses for sending the singleton daemon failure email. ▪ **Action Status Message** Specifies the message text to be included in the singleton daemon failure email.

Issue Mgr Options

Option	Description
iss_allow_sla_downgrade	Alters the behavior of the Iss SLA Option by allowing the system to automatically downgrade an issue's Service Type. The Iss SLA Option selects the best Service Type from among several issue attributes, but cannot replace the issue's current Service Type with a type of lesser rank. If this option is installed, the Service Types for all affected attributes are evaluated whenever one of the attributes changes. The issue's Service Type is set to the highest ranked type found, even if the new Service Type is lesser in rank than the issue's current Service Type. The Service Type with the smallest Rank value is considered the best service. If all the Service Types considered are equal in Rank (including Service Types with empty Rank values), the Service Type created first in the database is selected. The Iss SLA Option must be installed for this option to function correctly.
iss_assignee_set	Sets the assignee for issues to that of the logged in user, if the user is an analyst. If the option is installed, when an analyst creates a new issue, it is automatically assigned to that analyst.
Issue Auto Events	▪ Automatically attach events to newly created issues. This is specified using three options: ▪ **iss_auto_events** -- Installs or uninstalls the option itself. ▪ **iss_auto_events_count** -- Specifies the number of events attached. ▪ **iss_auto_events_name** -- Specifies the format of a name for the attached events. Event names to be attached are constructed by joining the iss_auto_events_name to a number ranging from 1 to iss_auto_events_count. For example:

Option	Description
	▪ iss_auto_events_name is "Auto Event" ▪ iss_auto_events_count is "3" With these settings, installing the iss_auto_events option would cause the following events to be attached to all new issues: ▪ Auto Event 1 ▪ Auto Event 2 ▪ Auto Event 3 To complete the implementation of this option, you must define events with these names.
Iss_Category_Defaults	Determines what happens when the category field is specified on an issue detail page. A category can have a default assignee, group, and organization/business. When this option is activated, the corresponding fields on the issue detail page are populated with the category defaults, if they have not been manually entered by the user. If these values are filled by the user, the defaulting rule does not apply. Make sure that the default assignee is actually a member of the default group.
iss_sla	Installs the rule for defaulting the Service Type field of an issue. The rule is as follows: The best service among the priority, requester, affected contact, and category is applied to the issue. The service type with the smallest rank value is considered the best service. If all the service types considered are equal in rank (including service types with empty rank values), the service type created first in the database is selected. **Note:** This option is only available if the Classic SLA Processing Option is installed.
require_issue_assignee	Prohibits issues with no value in the Assignee field from being saved.
require_issue_group	Prohibits issues with no value in the Group field from being saved.

Knowledge Options

This option controls the Knowledge functionality:

Option	Description
analyst_preferred_ticket	Sets the link for opening a ticket from a Knowledge Document for the analyst user interface. The analyst has a default setting of Incident, and the available options are Incident, Request, IncidentandRequest, and Issue.
kt_disallow_forums	If this option is set to Yes, the Forum feature is disallowed (inactive), which means you cannot create or update forums or view any menu items.

Option	Description
kt_report_card_issue_status	Allow issue statistics to be calculated and displayed in the Reuse section of the Knowledge Report Card. The validity of the where clause is not checked. **Example:** status='CL'
kt_report_card_request_status	Allow request statistics to be calculated and displayed in the Reuse section of the Knowledge Report Card. The validity of the where clause is not checked. **Example:** status='CL'

KPI Options

These options control the operation of the KPI daemon:

Option	Description
kpi_ticket_data_table	Enables the KPI daemon to collect data whenever CA SDM tickets are opened, closed, or certain fields are modified. Ticket data is written into the usp_kpi_ticket_data database table, and is available for generating web-based reports.
concurrent_lic_refresh_interval	Specifies the concurrent refresh time interval (in seconds) for all the concurrent KPIs (for example, webConcurrentLicenseCt KPI). If this option is installed, all the concurrent KPIs calculate the count only after the specified interval. If you do not install this option, refresh interval time is defaulted to 3600 seconds for all the concurrent KPIs.**Range:** 600 to 7200 seconds.

Note: Enabling this feature may result in degraded CA SDM performance.

LDAP Options

You can set the domain name for LDAP Servers that was configured through Options Manager, by adding the domain name in the NX.env file variable and executing the following commands:

```
pdm_options_mgr -c -a pdm_option.inst -s NX_LDAP_DOMAIN -v <DEFAULT_LDAP_SERV
pdm_options_mgr -c -a pdm_option.inst -s NX_LDAP_DOMAIN -v <DEFAULT_LDAP_SERV
```

Note: Restart the services and login to CA SDM with domain\username credentials.

The following LDAP options are available for installation from Options Manager on the CA SDM Administration tab.

Note: The options identified as required must be installed together to enable integration with an LDAP directory. The options identified as optional are features you can add only if the required options are installed.

Option	Description
default_ldap_tenant (required)	Specifies the default tenant for contacts imported from an LDAP directory into an installation that is configured for a multi-tenancy environment. The option value must set to the UUID for that tenant. You can get the tenant UUID from a database query. For example, "SELECT * FROM ca_tenant". **Important!** This option is only required if multi-tenancy is enabled. Before you run the pdm_buildtenant utility, and if you want to retain the tenant value, you *must* modify NX.env by adding the NX_RETAIN_TENANT_VALUE variable manually, and set it to "yes". If this variable is set to "no", missing, or not set properly, the utility overwrites the tenant information.
ldap_dn	Specifies the LDAP distinguishedName for logging in to the LDAP server. **Example**: CN=Joe, CN=Users, DC=KLAND, DC=AD, DC=com Depending on your site's network configuration, the userid *may* be used instead of a distinguishedName. **Note:** If the LDAP server supports anonymous binds, this value can be empty. For example, if the LDAP directory is the CA EEM identity store, this option is not required because CA EEM allows anonymous access.
ldap_enable	Specifies whether LDAP integration is enabled. The default value is Yes. In addition to this option, you install all other LDAP options indicated as required.
ldap_enable_auto (optional)	Specifies whether automatic creation of contacts from LDAP information is enabled. The default value is Yes. If you install this option, a contact is automatically created from LDAP information whenever a new user logs in.
ldap_enable_groups (optional)	Specifies whether CA SDM assigns a contact's Access Type based on LDAP Group membership. The default value is Yes. To use this feature, you associate CA SDM Access Types with LDAP Groups. **Note:** This option is only applicable for Microsoft Active Directory.
ldap_enable_tls (optional)	Specifies whether Transport Layer Security (TLS) is enabled during LDAP processing. The default option value is Yes.
	Specifies the value of the LDAP objectClass attribute. The default value is *group*.

Option	Description
ldap_group_object_class	This value is always included in the where clause of the automatically generated filters used to search for LDAP groups.
ldap_host	Specifies the LDAP server hostname or IP address. **Note:** If the LDAP directory is the CA EEM identity store, use the hostname of the machine where Ingres is installed.
ldap_port	Specifies the LDAP server port number. **Note:** If the LDAP directory is the CA EEM identity store, use 1684 for the port number.
ldap_pwd	Specifies the password for the ldap_dn for logging in to the LDAP server. **Note:** If the LDAP server supports anonymous binds, this value can be empty. For example, if the LDAP directory is the CA EEM identity store, this option is not required because CA EEM allows for anonymous access.
ldap_search_base (required)	**Note:** If you want to search contacts for a default LDAP server, keep the domain name field in the LDAP Directory Search page as blank or provide the exact LDAP domain name configured in CA SDM to retrieve the contacts in the specified LDAP directory. Specifies the starting point for searches in the LDAP schema tree: ▪ **UNIX** -- You *must* specify a starting container, such as: CN=Users, DC=KLAND, DC=AD, DC=com ▪ **Windows** -- You do not have to specify a container and may start at the top of the schema tree, such as: DC=KLAND, DC=AD, DC=com **Note:** If the LDAP directory is the CA EEM identity store, then use: cn=Users, cn=Entities,cn=iTechPoz This is only applicable when CA EEM is configured to use the MDB rather than an external directory.

Option	Description
ldap_service_type (optional)	Install this option to establish the LDAP service type. If the LDAP type is Active Directory, specify the string “Active Directory”. If the LDAP type is not Active Directory, specify any other string, for example, “eTrust” or “Novell”.
ldap_sync_on_null (optional)	Specifies whether existing contact attribute values are overwritten with null data if the corresponding LDAP user attribute contains a null value. The default value is Yes.
ldap_user_object_class (required)	Sets the value of the LDAP objectClass attribute. The default value is *person*. This value is always included in the where clause of the automatically generated filters used to search for LDAP users. **Note**: If the LDAP directory is the CA EEM identity store, use pozObject. For many non-AD LDAP stores, the correct setting is inetOrgPerson.
num_ldap_agents	Specifies the number of LDAP agents. Install this option only if you have multiple LDAP agents. The default value is 2.

Multi-Tenancy Options

Option	Description
max_tenant_depth	Specifies a limit to the depth of the tenant hierarchy. Default is four (4) levels of tenants.
multi_tenancy	Controls the multi-tenancy features. Multi-tenancy allows organizations or groups to share a single installation. The following values are available: ▪ **off** -- Multi-tenancy is not in use. ▪ **setup** -- Multi-tenancy is not in use, however, administrators can view and edit the tenant-related objects and attributes on the UI. ▪ **on** -- Multi-tenancy is fully operational. You can also add enforcement level options after the "on" setting, as follows: ▪ **warn** -- Untenanted objects can be created or updated, but an error message are written to the log. ▪ **allow** -- Untenanted objects can be created or updated, but a warning message is written to stdlog. **Note:** Setting an enforcement level is useful during migration. It allows SLA and attached event updates to legacy untenanted data.

Notifications Options

Option	Description
add_know_list	Adds the "in-the-know" notify list to all future notifications regarding a change order, issue, or request. When this option is installed, the contacts listed in the notify list are added to all future notifications.
log_all_notify	Logs all notifications, regardless of the method used. Logging a notification creates a notification log object that records the recipient, date/time, method of notification, and the notification text. The administrator uses the **Notification History** list to view and maintain notification log objects. The notification history can also be viewed from an individual ticket. If this option is not installed, the contact receives only the notification specified in the Contact record. No record is kept of the notification attempt.
notification_allow_temp_address	Allows manual notifications to be sent to manually entered SMTP email addresses, rather than to registered contacts only.
web_cgi_url	Allows the recipient of a notification email to click a URL and view the object they were notified about. This option is also used in survey notifications. To define a URL for a user to reach the CA SDM, a reference to the web interface is needed. The reference value is the web interface URL that is used to access the CA SDM web component. The URL has the following syntax. `http://hostname/CAisd/pdmweb.exe` ▪ **hostname** Specifies the location of your web server. (Recommended) For Advanced Availability configuration, it is strongly recommended that this option points to one of the application servers and not the background or standby server. It can also point to a Web Director or a third-party load balancer. ⚠ **Note**: Change the value of this option to point to: ▪ The load balancer if you have more than one application servers. ▪ The application server, if you have only one application server.

Request Mgr Options

Option	Description
Area_Defaults	Determines what happens when the Request Area field is specified on a Request Detail page. A Request Area can have a default assignee and group. When this option is activated, the Request Detail assignee and group are populated with the Request Area defaults.
Assignee_set	Sets the assignee for requests to that of the logged in user, when the user is an analyst. If the option is installed, when an analyst creates a request, it is assigned automatically to that analyst.

Option	Description
autoasg_ci_assign_lowest_agt	Enables the CI-based auto-assignment to assign an analyst from group. The analyst must have active Status as Active and Available as Yes. The tickets assigned to all of the analysts that meet this criteria are counted but the first one encountered with the least number of tickets assigned to them is assigned to the ticket. You have to install this option to use it. After installing, this option restart the CA SDM servers.
autoasg_override	Controls how Auto Assignment handles a Request that is created with an Assignee, Group, or both. Configure your system by setting this option to one of the following values: ▪ Uses the existing Assignee, Group, or both. Auto Assignment processing does not occur if the Assignee, Group, or both was set during the creation of the Request. ▪ Ignores the existing Assignee, Group, or both. Auto Assignment processing occurs and attempts to find an Assignee, Group, or both. The Assignee, Group, or both can be set in various ways: ▪ Manually by the Analyst ▪ Area Defaults and the Assignee set options ▪ Request Templates ▪ Uninstalling this option causes it to operate in its default mode, which is 0.
Auto Events	▪ Automatically attach events to newly created requests. This is specified using three options: ▪ **auto_events --** Installs or uninstalls the option itself. ▪ **auto_events_count --** Specifies the number of events attached. ▪ **auto_events_name --** Specifies the format of a name for the attached events. Event names to be attached are constructed by joining the auto_events_name to a number ranging from 1 to auto_events_count. For example: ▪ auto_events_name is "Auto Event" ▪ auto_events_count is "3" With these settings, installing the auto_events option causes the following events to be attached to all new requests: ▪ Auto Event 1 ▪ Auto Event 2 ▪ Auto Event 3 To complete the implementation of this option, define an event with these names. For more information, see create an event from How to Configure SLAs (see page 1099) topic.
clear_scratch_pad	Clears the Scratch Pad text is after creating a request. The default behavior is to apply the Scratch Pad text to all new requests.
cr_allow_sla_downgrade	Alters the behavior of the CR SLA Option by allowing the system to downgrade a request Service Type automatically. The CR SLA Option selects the best Service Type from among several request attributes, but never replace the request current Service Type with a type of lesser rank. If this option is installed, the Service Types for all affected attributes are evaluated whenever one of the attributes changes. The request Service Type is set to the highest ranked type found, even if the new Service Type is lesser in rank than the request current Service Type.

Option	Description
	The Service Type with the smallest Rank value is considered the best service. If all the Service Types considered are equal in Rank (including Service Types with empty Rank values), the Service Type created first in the database is selected. The CR SLA Option must be installed for this option to function correctly.
cr_sla	Selects the best Service Type from among several request attributes, and never replace the request current Service Type with a type of lesser rank. The Service Type with the smallest Rank value is considered the best service. If all the Service Types considered are equal in Rank (including Service Types with empty Rank values), the Service Type created first in the database is selected.
efficiency_tracking	Specifies Efficiency Tracking, which lets analysts use options to track incidents. This option displays the Show Efficiency Tracking tab on the Incident Detail page.
employee_intf_incident_support	Displays the Incident, Request, or both ticket types for users logged in under the Employee interface type. You can select one of the following Option Values: ▪ Incident only ▪ Request only ▪ Incident and Request **Note:** The employee_intf_incident_support option is installed during CA SDM installation and cannot be uninstalled.
force_resolution_code	Specifies how the Resolution Code field value is handled for requests and incidents when an analyst closes a request or an incident. When this option is installed, select one of the following values: **Empty** -- The resolution code value of the parent is forced to the children only when the child does not have a value for the resolution code field. The option does not overwrite an existing resolution code value. This is the default value. **All** -- The resolution code value of the parent is forced to all children even if they already have a value for the resolution code field. The option overwrites the current value with the value of the parent. ▪ If this option is not installed, the resolution code values of all children remain unchanged. ▪ If the option is installed, the resolution code value of the parent is propagated to its children.
force_resolution_method	Specifies how the Resolution Method field value is handled for requests and incidents when an analyst closes a request or an incident. When this option is installed, select one of the following values: **Empty** -- The resolution method value of the parent is forced to the children only when the child does not have a value for the resolution method field. The option does not overwrite an existing resolution method value. This is the default value.

Option	Description
	All -- The resolution method value of the parent is forced to all children even if they already have a value for the resolution method field. The option overwrites the current value with the value of the parent. ▪ If this option is not installed, the resolution method values of all children remain unchanged. ▪ If the option is installed, the resolution method value of the parent is propagated to its children.
guest_intf_incident_support	Displays the Incident, Request, or both ticket types for users logged in under the Guest interface type. You can select one of the following Option Values: ▪ Incident only ▪ Request only ▪ Incident and Request ⚠ **Note:** The guest_intf_incident_support option is installed during CA SDM installation and cannot be uninstalled.
monitor_joins	Specifies whether to monitor joined tables for updates to dynamic lists. Updates to another table can affect the contents of a list. This effect often occurs when you use data partition view constraints containing a join. For example, a view constraint on change orders/issues where: `assignee.organization = @root.organization` results in a join from the Change_Request table to the Contact table in all change order, issue, or both lists. Keeping a change order or issue list containing this constraint up-to-date requires monitoring updates to the Contact table, and refreshing the list whenever a contact changes its organization/business. The result can be that a large number of lists updating simultaneously after an update to a joined table, with a possible performance degradation while the update is occurring. The monitor joins option allows the list updating (and the monitoring of the joined table) to be suppressed at sites where the up-to-date accuracy of such lists is less important than the performance degradation.
Netres_pty	Escalates a request based on the associated asset. If you specify an asset with a Priority greater than the Priority on the request, the request Priority is set to match the asset. An escalation activity is not created. This option does not override a Priority that you manually specified on the Request Detail page during the same editing session.
require_incident_assignee	Prohibits incidents with no value in the Assignee field from being saved.
	Prohibits incidents with no value in the Group field from being saved.

Option	Description
require_incident_group	
require_problem_assignee	Prohibits problems with no value in the Assignee field from being saved.
require_problem_group	Prohibits problems with no value in the Group field from being saved.
require_request_assignee	Prohibits requests with no value in the Assignee field from being saved.
require_request_group	Prohibits requests with no value in the Group field from being saved.
urgency_on_employee	Specifies whether to show the Urgency field on Self Service incidents or requests. When the urgency_on_employee option is not installed, the Priority field appears on Self Service incidents or requests. When urgency_on employee option is installed, the Urgency field appears instead of the Priority field. The range of Urgency values are based on *web.cfg* settings.
use_incident_priority	Specifies whether to calculate the Incident Priority field on the Incident Detail page. When the administrator uses Web Screen Painter to add the Incident Priority field, the Incident Priority field appears on the Incident Detail page. When the use_incident_priority option is not installed, the Incident Priority value calculated is zero. When the use_incident_priority option is installed the Incident Priority calculates as the sum of the Urgency and Impact values.

Request-Change Options

Option	Description
edit_inactive	Prevents editing change orders, issues, or requests unless their status is Active. Default behavior is to allow editing of inactive tickets.
set_sla_evt_open_date	Uses the open date/time value of a change order, issue, or request as the start date /time of attached events. The attached events are triggered as soon as the ticket is saved.

Request-Change-Issue Options

Option	Description
	Allows or prevents the Activity Log fields from being edited. The only exception to this option's setting is the Internal field. This is always editable.

Option	Description
activity_log_security	**Note:** The activity_log_security option is installed during installation and cannot be uninstalled.
Any_Contact	Some CA SDM objects restrict field values for Contacts based on Contact Type. This type of restriction is typically found on fields labeled, "Assignee" and only allow Contacts with a Contact Type Analyst. This option removes the contact type restrictions across the entire CA SDM application, allowing any type of contact to be used as an assignee.
classic_sla_processing	Enables the "classic" model of service types and SLA's. This model uses the Rank value for Service Types to determine the correct Type for a ticket. Only one Service Type can be applied to a ticket. **Note:** The Chg SLA Option, CR SLA Option, and Iss SLA Option are available if the Classic SLA Processing Option is installed.
delete_null_properties	Determines what happens to the properties when the Change Category, Issue Category, Request Area, Incident Area or Problem Area change and you install the keep_tasks option. A saved ticket with a specified category can have a number of properties and tasks. If this option is not installed, the following occurs: ▪ All existing properties are preserved. ▪ Any new properties, if any, from the new category are added. If this option is installed, the following occurs: ▪ All existing properties that contain non-empty values are preserved. ▪ All existing properties that contain empty values are deleted. ▪ New properties from the new category, if any, that do not have the same label value as any of the existing kept properties are added. When new properties are added to a ticket with existing properties, the system automatically adjusts (increases) the sequence numbers of the new properties to ensure they do not conflict with existing properties. The new properties always have greater sequence numbers than the existing ones.
filter_template_search	Filter the initial template search with end user's Organization.
force_rootcause	Specifies how the Root Cause field is handled for requests, change orders, and issues. ▪ If this option is not installed, the root cause field values of all children are left unchanged. ▪ If the option is installed, the root cause value of the parent are propagated to its children. When this option is installed, choose one of the following values: ▪ **Empty** -- The root cause value of the parent are forced onto the children only when the child does not have a value for the root cause field. It does not overwrite an existing root cause value. This is the default.

Option	Description
	▪ **All** -- The root cause value of the parent is forced onto all children even if they already have a value for the root cause field. It overwrites the current value with the value of the parent.
init_list_search	Performs a search when opening the Request, Change Order, and Issue List pages to display the logged-in user's list of tickets. If this option is not installed, these list pages are blank on opening until the user performs a search.
keep_tasks	Specifies what happens if you move a ticket to a different category or area: ▪ If keep_tasks is *not* installed, all existing properties on the ticket are removed. Any properties or tasks associated with the new category or area are added. Tasks with a status of Wait are removed. Tasks with any other status are retained. ▪ If keep_tasks *is* installed, all existing properties and tasks on the ticket are retained. Any properties or tasks associated with the new category or area are added. **Note**: When new properties or tasks are added to a ticket with existing properties or tasks, the sequence numbers are automatically adjusted to prevent conflict. New properties and tasks are always assigned greater sequence numbers than the existing ones.
leave_children_open	Keeps child incidents, requests, problems, changes, or issues, open when the parent is closed.
lex_lang	Allows you to select the language to be used for spell checking. Default is US-English. This option sets the NX_LEX_LANG variable located in the NX.env configuration file.
sla_workshift_override	Use this option to default the workshift for Service Type Events. ▪ When this option is not installed, events for a Service Type always uses the workshift specified each event's template. ▪ Installing this option defaults the workshift for Service Type Events to the workshift specified on the Service Type. The default occurs only when the event does not specify its own workshift. If an event template specifies a workshift, it is always used. **Tip:** Set the event's workshift to the supplied '24 hour' workshift if you want the event to always start, regardless of any Service Type workshift.

Search Engine Options

The following options control Knowledge Management search performance:

Option	Description
ebr_max_qps	Specifies the maximum number of queries per second (QPS) that is logged in the .stdlog file. The default is 2 QPS. QPS below this number is logged in trace mode.

Option	Description
ebr_qps_timeout	Specifies the time interval (the number of seconds) by which QPS are measured. Default is 300 seconds.

The following options control search engine integration:

Option	Description
ebr_search_engine_baseport	Specifies the port selected when the search engine was installed. Default is 13000.
ebr_search_engine_host	Specifies the host name or IP address where the search engine is installed.
ebr_version	Defines the search engine you want Knowledge Management to use for searches. The KM Search Engine specifies the engine that is installed and configured with CA SDM. **Note:** The document is not indexed when the Search Engine and all the text fields contain noise words.

Security Options

Option	Description
bopauth_host	(Applicable only for advanced availability configuration) Specifies the server name where bopauth_nxd is running. bopauth_nxd authenticates users accessing CA SDM through different interfaces. Select default if bopauth_nxd has to run in background server. This option cannot be uninstalled.
ldap_virtdb_host	(Applicable only for advanced availability configuration) Specifies the server name where ldap_virtdb is running. Select default if ldap_virtdb has to run in background server. This option cannot be uninstalled.
eiam_hostname	Specifies the hostname of the server where EEM is running. Required for EEM user name and password or artifact authentication.
force_browser_to_send_cookie_only_in_ssl_connection	(optional) Force the browser to send the Session ID (SID) cookie only if there is an SSL connection. This attribute is applicable only if you have enabled the **use_encrypted_sid_and_cookie** to (Yes). By default, this is turned off. If this flag is enabled, CA SDM can only be accessed through an SSL connection.
force_unique_userid	Prevents using duplicate active system login names. **Important!** We recommend that you keep the force_unique_userid option enabled at all times. If this option is uninstalled, and there are multiple contact records with the same login id, you may experience problems with data partitions, multi-tenancy, security, and other functionality.
	Specifies the Guest user login ID. Default is Anonymous. Must be a valid user ID.

Option	Description
guest_user_name	
ignore_security_case	If installed, the user ID is not case sensitive.

Portal_Safe_List	Stores a list of machine names and port numbers where Portal is installed. The machine name and the port are entered as follows
	
	`machine-name:8080`
	
	For multiple Portal installations, separate the machine name/port number with a comma. For example:
	
	`machine-name1:8080,machine-name2:8081,machine-name3:8080`

url_etrust_password_reset	The URL for the eTrust Admin web interface. This enables the password reset link on the web interface. For example: `http[s]://hostname/EAOWebi/EAOLogin`
use_eiam_artifact	Allows EEM artifact to be used when users log in to CA SDM / Knowledge Management using URL.
use_eiam_authentication	Allows use of EEM authentication when users log in to CA SDM / Knowledge Management and the access type authentication is set to OS.
use_encrypted_sid_and_cookie	(optional) Use encrypted Session ID (SID) and cookie to prevent SID spoofing and Man-in-the-middle attack. By default, this attribute is disabled. If you want to have enhanced CA SDM security, this attribute can be enabled (Yes). Enabling this attribute can have some performance impact on the CA SDM Application.

Support Automation Options

Option	Description
sa_domsrvr	Specifies that the Support Automation main server communicates with the specified Support Automation domsrvr. If this variable is not installed, the Support Automation main server communicates with the default primary CA SDM Domsrvr named "domsrvr".
sa_primary_domsrvr	Specifies whether to start the Support Automation primary domsrvr. This variable is used to determine if a dedicated object server is already configured. If this option is not installed, the domsrvr:sa runs on one of the secondary CA SDM servers and you are required to startup for domsrvr:sa.
supportautomation_url	Specifies the URL of the Support Automation web application, which CA SDM uses to communicate with the Support Automation main server. The host name and port number should correspond with the values set during configuration. We recommend that you configure the supportautomation_url with a host name because you may encounter problems when you configure the supportautomation_url with an IP address, if you use an IP address which has an existing host name mapping, the HTTP request processing resolves to this host name.

Option	Description
	Note: The administrator installs this option after you configure the Support Automation main server on a primary or secondary CA SDM server to enable Support Automation usage in CA SDM. Do not install this option if Support Automation is not configured.

Time-to-Violation Options

These options control the process that monitors the service level agreements on all open tickets and tasks, and records the time the Service Type enters violation:

Option	Description
ttv_enabled	Runs the Time to Violation daemon, which monitors the SLAs for all open tickets and tasks. This process does not set the SLA violation, but records the date the ticket or task is violated in its current state. This projection is updated when the ticket or task is updated. This option must be installed in order for the other Time to Violation options to function correctly. **Important!** This option requires that the classic_sla_processing option *not* be installed.
ttv_evaluation_delay	Sets the delay between a request to the time-to-violation (TTV) daemon and when it actually evaluates a ticket. Whenever a ticket is updated, a request is sent to the TTV daemon to update the time-to-violation projections. Because tickets are often updated several times in quick succession, a delay in evaluation helps prevent needless evaluations and improves performance. **Important!** This option is dependent on the ttv_enabled option, which must also be installed. **Note:** This value may never be set below 60 seconds.
ttv_highlight	Highlights a ticket in a list if the ticket has a Time to Violation value set to start by a certain time. The default highlight color is a pale yellow. The ticket number is highlighted only if one of its Time to Violation values is less than the date /time specified by the Timespan, "TTV_THRESHOLD". By default, this Timespan is set to show tickets with Time to Violation values less than midnight of the current day, for example, "today". You may modify this Timespan to any value. This option only affects ticket list forms on the web interface client. It applies to lists of Requests, Issues, Change Orders, Incidents, Problems and Tasks. It's an option because the Time to Violation value is stored in a database table separate from the ticket, and requires an extra database fetch *for each row displayed*. Given this extra DBMS activity, installing this option may increase the load on your database so that performance may be affected.

Option	Description
	Important! This option is dependent on the ttv_enabled option, which must also be installed.

Ver Ctl Options

The ver_ctl option controls the actions that are taken by the Version Control Manager when a version discrepancy is detected. The Version Control Manager detects discrepancies by comparing version files across all CA SDM servers (client and servers). Depending upon the CA SDM configuration, the following client and servers are used:

- Conventional:
  - Client: Secondary server
  - Server: Primary server
- Advanced availability:
  - Client: Application and Standby servers
  - Server: Background server

Only components that are listed in the version files are controlled. When you restart the servers and if a discrepancy is detected, the client connects to the server to send a list of its controlled components. The server compares the list to its own master list. The affected components on the client are upgraded or terminated, depending on the ver_ctl option.

ver_ctl
Installing this option activates the Version Control Manager. Valid option values are:

- **Fail** -- A version discrepancy terminates the secondary server's connection to the primary server. The secondary server is prevented from connecting to the primary server until it is manually updated.
- **Notify** -- Default value. On Windows, a version discrepancy results in a message window asking if you want the secondary server to continue or quit. On UNIX, a version discrepancy is logged, but the secondary server always completes initialization.
- **Upgrade** -- When a version discrepancy is detected, an upgrade of the affected components is attempted on the secondary server. If the upgrade is successful, the secondary server connection continues; otherwise, the secondary server connection terminates.
- **Disable** -- Version discrepancies are ignored. All secondary servers are allowed to connect to the primary server.

Web Options

These options control the CA SDM web interface operation:

Option	Description
auto_suggest_status	Displays matching records for the text entered in lookup fields within the Analyst interface. **Note**: For this option to work correctly, the Using Screen Reader user preference must be disabled. To specify user preferences, select View, Preferences on the menu bar. **Default:** On
copy_inactive	Copies the inactive attributes of an object (such as the previous assignee) from the original record to the new record. **Note:** By default, this option is uninstalled so that links to inactive objects are not copied. If you install this option, or if you migrated from CA SDM r12.5, links to inactive objects are copied.
charset	Defines the default HTTP character set for the web interface. You cannot uninstall this option. The value of this option is set in the charset parameter of the HTTP content-type header and it matches the character encoding of the operating environment when CA SDM is configured. Under normal circumstances, this option does not need updating after initial configuration. **Important:** Restarting the CA SDM server is *not* required.
export_max_fetch_rows	Determines the maximum number of rows that users can export for a list. **Default:** 5000
max_files_to_upload_simultaneously	Defines the maximum number of files that you can simultaneously upload during the same operation. **Valid Range:** Greater than or equal to 0. Zero means unlimited. **Default:** 10
max_records_auto_suggest	Specifies the number of suggestions to display in matching results. For example, increase the number of suggestions if analysts in your environment request 50 suggestions. **Default:** 25
min_chars_auto_suggest	Specifies the minimum number of characters that a user enters in a lookup field before the field starts displaying matching results. For example, increase the number of characters if your environment contains many users that share the first three characters in their user names. T **Default:** 3

Option	Description
mouseover_preview_delay_time	Specifies the delay time, in milliseconds, between hovering the mouse cursor over an object link and the display of the mouseover preview. The preview is not generated if the mouse is moved away from the link before the delay time expires. Enter a value from 100 to 5000 in the Option Value field. **Default:** 1000
pdmweb_cache_disable	All regular files from bopcfg/www are cached. If this option is installed, the PDMWEB servlet does not cache the files, which means all files are retrieved from the directory each time one is needed.
pdmweb_cache_site mods	The PDMWEB Servlet, by default, does not cache files from the $NX_ROOT/site/mods folder. If this option is installed, files are cached from the sitemods folder.
prompt_for_knowledge	Enables a dialog that prompts users to search the knowledge base before creating issues from the customer web interface and requests from the employee web interface.
scoreboard_entry_limit	Limit for adding new scoreboard nodes and folders. When the system reaches the limit, existing folders and nodes continue to display information. However, the user must delete unused folders or nodes before creating new ones.
suppress_web_hier_search	Suppresses the hierarchical search used on the web for request, incident, and problem areas, category, and root cause. This option is useful for tables that are not organized hierarchically, or when one or more of the hierarchical levels contains a great many records. When hierarchical search is suppressed for a table, search requests on the table are processed as lookups. The value of this option is list of object names of the tables for which hierarchical search is suppressed. If more than one table name is specified, values are separated by spaces. Valid values are: ▪ **chgcat** - Change order category ▪ **isscat** - Issue category ▪ **pcat_cr** - Request area ▪ **pcat_in** - Incident area ▪ **pcat_pr** - Problem area ▪ **rc** - Request root cause **Important!** To avoid errors when using autocomplete, we recommend that you use this option instead of modifying the dtlHier macro to dtlLookup in the HTMPL file.
use_nested_tabs	Displays nested tabs within the current form. The analyst can expand each tab to view key details. If you want to revert to the notebook styles used in CA SDM r12.5, you can disable the nested tabs control. For example, analysts in your environment prefer to click a tab that shows only the content of that tab.

Option	Description
web_auto_update	Requests the automatic update of scoreboard counts for analyst web users. When this option is installed, each web analyst session requests updated scoreboard counts at the interval specified in the option. The value of this option is the number of seconds between updates, with a minimum value of 60 seconds (one minute). Web scoreboard updating occurs in the background. The analyst end user can see periodic activity on the main page. In addition, updated count values are highlighted on the scoreboard. The highlighting remains until the user either clicks on the scoreboard link to display the associated list, or presses the Update Counts button. Activating this option affects the overall load of the system as follows: ▪ Each web user can send additional requests to the server at the frequency specified in the option. ▪ The web engine receives messages from the object engine each time a database update causes the count associated with a query to change. When the web auto update option is not installed, the web engine requests counts from the object engine only when a web user explicitly requests an update.
web_wildcard_search	Installing this option enables a wildcard search for all text fields when using Search Filters. To perform a wildcard search, you add the "%" symbol after a text string. For example, entering the string "option%" retrieves all records that begin with the word "option". Installing this option eliminates the need for the "%" symbol and conducts wildcard searches by default. **Note:** Installing this option enables functionality equivalent to using the "%" symbol only at the *end* of the search string, not at the beginning. For example, with this option installed, searching the Options Manager option list for the string "ldap" finds all options with names beginning with "ldap" but does not find the "default_ldap_tenant" option.
wsp_domsrvr	Specifies the name of an object engine dedicated to the Web Screen Painter (WSP). The WSP webengine, designated by the companion option wsp_webengine, is the only client process allowed to connect to the object engine identified by wsp_domsrvr. You must install both the wsp_domsrvr option and wsp_webengine option in order to enable the WSP schema modification test feature. The value of this option must be a string beginning with the characters "domsrvr:". It is recommended that you use domsrvr:wsp as the name of the WSP object engine. Installing this option automatically runs the WSP object engine on the primary server.
wsp_webengine	Specifies the slump name of the webengine used by Web Screen Painter users. All WSP users connect to this webengine, and use it for preview sessions. All files saved by WSP users are stored in the site/mods directory on the server running this webengine, which must be the CA SDM primary server. Because WSP saves information on the server running its webengine, all WSP users must connect to the same webengine. If the wsp_wengine option is not installed, WSP users connect to the default webengine: web:local, sharing it with other users. The value of this option must be a string beginning with the characters: "web:". We recommend you use web:wsp as the name of the WSP webengine.

Web Report Options

These options control the CA Business Intelligence reporting integration with the BusinessObjects server:

Option	Description
bo_server_auth	Specify which type of authentication you want to use for reporting. You can specify the following types of authentication: ▪ **secEnterprise**. (Default) Specify Enterprise Authentication as your authentication type if you prefer to create distinct accounts and groups in BusinessObjects for use with CA Business Intelligence, or if a user hierarchy has not been set up on an LDAP server or a Windows AD server. ⚠ **Note**: If you choose the secEnterprise option, you need to add your CA SDM report users to the BusinessObjects Central Management Console (CMC). The CMC allows you to control users' access to Business Intelligence Launch Pad and other BusinessObjects applications. In the CMC, you must enter the same user names and passwords configured in CA SDM. ▪ **secLDAP**. Specify LDAP Authentication as your authentication type if you have already set up an LDAP directory server and want to use your LDAP user accounts and groups in BusinessObjects for use with CA Business Intelligence. ▪ When you map LDAP accounts to BusinessObjects, users can access CA Business Intelligence with their LDAP user name and password. This eliminates the need to recreate individual user and group accounts within BusinessObjects. ▪ **secWinAD**. Specify Windows AD Authentication as your authentication type if you are working in a Windows 2000 environment and want to use your existing AD user accounts and groups in BusinessObjects for use with CA Business Intelligence. ▪ **secExternal**. Specify External Authentication as your authentication type if you integrate the BusinessObjects authentication solution with a third-party authentication solution (for example, using JCIFS with Tomcat). This authentication type requires setting up Trusted Authentication in BuisnessObjects to allow users to log on without providing their passwords. ⚠ **Note:** During the Trusted Authentication configuration, you must set the user name retrieval method to REMOTE_USER in the BusinessObjects web.xml file. ⚠ **Note:** For information about alternative security options, see the *CA Business Intelligence (see page 3180)*.

Option	Description
bo_server_cms	Specify the name of the Central Management Server (CMS) that is responsible for maintaining a database of information about your BusinessObjects that you use with CA Business Intelligence. For the bo_hostname, use the hostname of the machine where CA Business Intelligence is installed. The default bo_cms_port is 6400.
bo_server_location	Specify bo_hostname by using the hostname of the machine where CA Business Intelligence is installed. CA SDM uses this URL to put together report URLs for requesting reports from the BusinessObjects server. The CMS location is specified by hostname and port. **Important!** The default bo_application_server_port is 8080 (for example, this can be the Tomcat port). If you install CA SDM and CA Business Intelligence on the same server, you must specify a different port. Use the port specified when starting Business Intelligence Launch Pad. For example, http://hostname:8180/businessobjects/enterprise115/desktoplaunch/businessintelligencelaunchpad/logon/logon.do displays that 8180 is the value to use for bo_tomcat_port.

Web Service Options

Option	Description
rest_webservice_access_duration	Specifies the number of hours that the REST Web Service Access Key remains active before expiration. The Access Key timeout is not based on inactivity time, but it is based on duration time since the Access Key creation. After the Access Key meets the specified duration, the Access Key ends regardless of whether it is being used. Optionally, the REST client can also provide the Access Key duration time for the specific Access Key during the Access Key request. To provide the duration value, set it directly on the expiration_date attribute of the rest_access resource, as part of the POST request payload. **Valid Range:** 1-8760 hours **Defaut:** 168
rest_webservice_disable_basic_auth	Disables Basic Authentication in REST Web Services. **Default:** No
rest_webservice_list_max_length	Specifies the maximum number of rows that a REST Web Service query returns. **Default:** 500
rest_webservice_list_page_length	Specifies the default number of rows that a REST Web Service query returns per page. **Valid Range:** 1-500 **Default:** 25

Option	Description
rest_webservice_resources_to_expose	Specifies the list of Majic factories (resources) that CA SDM exposes through REST Web Services. This option overrides the default behavior. By default, CA SDM exposes all factories through REST Web Services. If you do not enter values in this option, the default behavior exposes any Majic factory that does not have the REST_OPERATIONS property set to NONE. By default, no Majic fatory has this property set to NONE. Use the REST_OPERATIONS property to set the specific HTTP CRUD (CREATE, READ, UPDATE, DELETE) methods for CA SDM to expose on a given Majic factory. **Default:** rest_access **Example:** rest_access, cnt, grp, cr, crs, pri, alg, urg, imp, pcat, org
hmac_algorithm	Specifies the algorithm that you use to compute the signature for Custom/Secret Key Auhentication in REST Web Services. **Default:** HmacSHA1
string_to_sign_fields	Specifies the fields that you use to compute the signature for Custom/Secret Key Authentication in REST Web Services, in addition to the default REQUEST_METHOD, REQUEST_URI, and QUERY_STRING fields. **Default:** blank
webservice_domsvr	Specifies the name of the object engine that SOAP web services use. If not installed, SOAP web services use "domsvr". The value of the option must be a string beginning with the characters "domsvr:"
webservice_session_timeout	Sets the timeout value (in minutes) for SOAP Web Service sessions. When the time between successive web method calls is greater than the value specified, the session ID is marked expired. The session is then no longer valid. To prevent sessions from expiring due to activity, set the value for this option to 0. Other methods, such as logoff routines, can still invalid sessions.

xMatters

xMatters is used for mass notifications and Alerts. When a CA SDM ticket (incident, request, or problem) is created or updated, the integration mechanism sends the notification along with ticket information to the xMatters agent. The notification works only with CA SDM CR objects (incident, request, or problem). The CA SDM notification feature sends notifications to users based on the rules set for notification. CA SDM sends the Notify Log Reader information automatically along with ticket information to the configured xMatters agent.

CA SDM administrators can enable or disable integration with xMatters through the Options Manager options. You must install these options as these options are not installed out of the box. Restart CA SDM services after installing or uninstalling these options. On successful installation of xMatters options, a new daemon the pdm_xmatters_sync is started and can be monitored through the task manager process list. This daemon is a singleton process and runs on the primary or background server.

The pdm_xmatters_sync daemon gathers notification records with status **Pending** or **Error** based on the **xmatters_retry_count** option value. It also maintains a list of newly created notification records. After the existing record list is run, the pdm_xmatters_sync runs the newly created record list. This is an ongoing process. In case of failure, when the xMatters agent is not available, the records wait for the time specified in the Options Manager **xmatters_retry_interval** option and re-triggers the pdm_xmatters_sync daemon till all records attain a status of either **Success** or **Abort**.

The pdm_xmatters_sync daemon runs the records in the same order in which they are created. Records having **xMatters-Pending** or **xMatters-Error** status are processed first and then, the newly created records are processed.

Based upon the set notification rules, the notification history page will have information along with the status.

Rule	Information
xMatters – Error	Return error code status to CA SDM. Indicates that this notification message was sent to xMatters agent but was not received by xMatters agent. This can happen due to xMatters agent not running or other issues with the agent. Notifications having this status will retry based on the Options Manager *xmatters_retry_count* and *xmatters_retry_interval*.
xMatters – Abort	Return error code status to CA SDM. Indicates that CA SDM triggered the number of iterations mentioned in the Options Manager *xmatters_retry_count* and *xmatters_retry_interval* options, but the xMatters agent did not receive this message.
xMatters – Success	This status indicates that xMatters agent received this notification message successfully and returned the success status code. These records can be shown from xMatters system web interface.

Install the following xMatter Options Manager Options. These options control the CA SDM and xMatters integration provides a reliable and stable mechanism to integrate notifications.

Option	Description
xmatters_cr_attr	The valid CR majic attribute name. Specify the request attributes for xMatters notification. This can include custom attributes.
xmatters_retry_count	The default and minimum value is set as 3 in the range [1-20]. This value indicates the number of times the retry option can be triggered for failed transactions or notifications.
xmatters_retry_interval	The default and minimum value is set as 15 minutes in the range of [15-999]. This value indicates the time gap between each retry and specifies the retry interval duration in minutes for each failed xMatters notification.
xmatters_URL	Valid xMatters server agent and port number. Specifies the xMatters integration URL link. **Example URL:** http://<xmattersagentname>:<port>/http /caservicedesk15_caservicedesk15

For more information, see Create a Notification Method (see page 834) and Create Contacts Manually. (see page 1213) To complete the implementation of this option, you must define an event with these names. For more information, see create an event from How to Configure SLAs (see page 1099) topic.

Install/Uninstall Options Manager Options

Contents

You can install Options when installing CA SDM or can install them later. Some Options are automatically installed when you install the application that uses them.

Install an Option

You install an option from CA SDM. If you are using advanced availability configuration, you can install an option only from the background server. From the application or standby server, you can view the option details after it is installed.

Follow these steps:

1. Log in to the following server, depending upon your CA SDM configuration:
   - Conventional: Primary or secondary server
   - Advanced Availability: Background server
2. On the Administration Tab, browse to Options Manager.
   The Option Search page opens.
3. Search for the option you want to install.
   The Option Detail window opens.
4. Click Edit.
   The Update Option window opens.
5. Click Install.
   The Option Detail window displays a refresh message.
6. Click Refresh.
   The Option Detail window displays the Action Status of the option as "Installed."
7. Click Close Window.
8. Depending on your CA SDM configuration,

Important! Changes in some options do not require you to restart all the servers. Ensure that you read the Server Restart List (see page 1341) before restarting any server.

- Restart the CA SDM servers in conventional configuration (see page).
- Restart the CA SDM servers in advanced availability configuration (see page 866).

The Option List displays the updated status of the option when you restart the servers.

You can also install options from the command line using the following script:

```
$NX_ROOT/bin/pdm_options_mgr -c -b -a pdm_option.inst
```

Uninstall an Option

You can edit an option to uninstall it. If you are using advanced availability configuration, you can edit an option only from the background server. From the application or standby server, you can view the option details.

Follow these steps:

1. Log in to the following server, depending upon your CA SDM configuration:
   - Conventional: Primary or secondary server
   - Advanced Availability: Background server
2. On the Administration Tab, browse to Options Manager.
   The Option Search page opens.
3. Search for the option you want to uninstall.
   The Option Detail window opens.
4. Click Edit.
   The Update Option window opens.
5. Click Deinstall.
   The Option Detail window displays a refresh message.
6. Click Refresh.
   The Option Detail window displays the Action Status of the option as "Not Installed."
7. Click Close Window.
8. Depending on your CA SDM configuration,

   Important! Changes in some options do not require you to restart all the servers. Ensure that you read the Server Restart List (see page 1341) before restarting any server.

   - Restart the CA SDM servers in conventional configuration (see page).
   - Restart the CA SDM servers in advanced availability configuration (see page 866).

The Option List displays the updated status of the option when you restart the servers.

You can also uninstall options from the command line using the following script:

```
$NX_ROOT/bin/pdm_options_mgr -c -b -a pdm_option.deinst
```

Restart the CA SDM Servers in Conventional Configuration

For the conventional configuration, you restart the servers in the following order:

Note: To restart a server click Start, Settings, Control Panel, Administrative Tools, Services. Right-click the CA SDM Server and select Start.

1. Restart the secondary server.
2. Restart the primary server.

Restart the CA SDM Servers in Advanced Availability Configuration

For the advanced availability configuration, we recommend that you restart the CA SDM servers in the following order:

Note: To restart a server click Start, Settings, Control Panel, Administrative Tools, Services. Right-click the CA SDM Server and select Start.

1. Restart all Standby Servers.
2. Promote the Standby Server as the New Background Server (see page 867).
3. Start the Old Background Server.
   When you start the background server, it becomes a standby server.
4. Choose the Less Active Application Server (see page 868).
5. Restart the Less Active Application Server.
6. Stop the Other Application Server (see page 868).
7. Start the Application Server.
8. Perform the steps 6 and 7 for the other application servers.

Promote the Standby Server as the New Background Server

Before you stop the background server, promote the standby server (that you have upgraded) as the new background server. If Support Automation is installed with CA SDM, notify the active Support Automation users about the background server shutdown.

Follow these steps:

1. Execute the following command on the background server to notify all active users using Support Automation to save their work:

   ```
   sa_server_notifier [-h] | [-q seconds] | [-c]
   ```

   - **-h**
     Displays the help page.

   - **-q seconds**
     This option notifies a local server (background) to quiesce in a specified time interval. This interval is the number of seconds before the server goes offline. This option cannot be used for a standby server or application server.

   - **-c**
     This option cancels a previously sent quiesce request.

   A pop-up message is displayed to all the active users using Support Automation. This message notifies the users about the server shutdown and the time that is left for the shutdown. The users must save their work and logout within that scheduled time.

2. Execute the following command on the standby server that you wish to promote as the new background server:

   ```
   pdm_server_control  -b
   ```

   - **-b**
     Notifies a local standby server to become the background server. The standby server must already be running. If the server is not running, it is started but no failover is performed; to start a failover, run the command again.

   The background server shuts down automatically and the standby server is promoted as the new background server. This change does not affect the end-user sessions. The in-progress updates (if any) are stored and delayed, until the new background server comes online.

Choose the Less Active Application Server

You choose an application server with the least user activity. Run the following command on each application server to choose the one with no or minimal active sessions.

```
pdm_webstat
```

Note: This command does not capture the SOAP or REST Web Service sessions.

Stop the Other Application Server

You inform all the active users on an application server to move to the less active application server before you stop it. Ensure that you have restarted the less active application server before moving all the users to it.

Follow these steps:

1. (Recommended) Inform all active Support Automation analysts on the application server which you want to stop, to create a ticket in CA SDM with their session information. This process ensures that the session information is not lost. For example, the Support Automation analyst is in a session with a customer to resolve a hardware issue. In such a case, the Support Automation analyst can create an issue in CA SDM with the session information before the application server shuts down.

2. Send a notification (for example, an email notification) to all the active users on the application server to move to the less active application server that you just restarted. This notification can include the details of the updated application server.

3. Execute the following command on the application server:

   ```
   pdm_server_control [-h] -q interval -s server_name
   ```

   - **-h**
     Displays the help page.

   - **-q interval -s server_name**
     Notifies a local or remote application server to quiesce in a specified time interval. This interval is the number of seconds before the server goes offline. When using this option without a server_name, the local server is notified to quiesce. This option cannot be used for a background or a standby server.

   A pop-up message is displayed to all the active users on the application server to notify them about the server shutdown and the time left for the shutdown. The users must save their work and logout within that time. The application server stops after the specified time. The users log on to the other application server to resume their work. The Support Automation analyst can refer to the ticket and resume their work.
   The application server is stopped successfully.

Server Restart List

Depending upon the CA SDM configuration, restart the following servers:

- Conventional: Primary server

- Advanced Availability: Application, Background, and standby servers. The following options do not require you to restart all the servers:

Options Type	Options	Action

Change Order	Category_Defaults, chg_auto_events, chg_sla	Restart all servers *quickly* to maintain functionality consistency. Change in these options contains Majic and/ or Spel changes
Email	mail_from_address, mail_login_password , mail_login_userid, mail_max_threads, mail_reply_to_address, mail_smtp_domain_name, mail_smtp_hosts, mail_smtp_host_port, mail_smtp_security_level	Restart all standby servers and then the current background server.
Issue Mgr	iss_auto_events, Iss_Category_Defaults, iss_sla	Restart all servers *quickly* to maintain functionality consistency. Change in these options contains Majic and/ or Spel changes.
LDAP	ldap_dn, ldap_enable_tls, ldap_group_object_class, ldap_host, ldap_port, ldap_pwd, ldap_search_base, ldap_service_type, ldap_user_object_class, num_ldap_agents	Restart all standby servers and then the current background server.
Request Mgr	Area_Defaults, auto_events, cr_sla, Netres_pty	Restart all servers *quickly* to maintain functionality consistency. Change in these options contains Majic and/ or Spel changes.
Request-Change-Issue	Any_Contact	Restart all servers *quickly* to maintain functionality consistency. Change in these options contains Majic and/ or Spel changes.
Search Engine	ebr_cr_where_clause, ebr_index_queue_timeout, ebr_iss_where_clause, ebr_max_qps, ebr_qps_timeout, ebr_search_engine_	Restart all standby servers and then the current background server.

	baseport, ebr_search_engine_host, ebr_version	
Security	force_unique_userid	Restart all servers *quickly* to maintain functionality consistency. Change in these options contains Majic and/ or Spel changes.
Support Automation	sa_domsrvr, sa_primary_domsrvr	Restart all standby servers and then the current background server.
Time-to-Violation	ttv_evaluation_delay	Restart all standby servers and then the current background server.
Web	export_max_fetch_rows	No action required. Changes to this option takes effect when the user exports the list.
Web	web_wildcard_search	Restart all standby servers and then the current background server.
Web Service	hmac_algorithm, rest_webservice_access_duration, rest_webservice_disable_basic_auth, rest_webservice_list_max_length, rest_webservice_list_page_length, rest_webservice_resources_to_expose, string_to_sign_fields	Restart all application servers where RESTful Web Services are configured.

Multi-Tenancy

This section contains the following articles:

Multi-tenancy enables multiple independent tenants (and their users) to share a single implementation of CA SDM. All Tenant users interact with each other in defined ways as per assigned roles and tenant hierarchies. Typically, each tenant views the CA SDM implementation as per the assigned access right. Tenants cannot update or view data that are related to other tenant unless specified.

Multi-tenancy allows tenants to share hardware and application support resources and reduce cost.

Service Provider

This article contains the following topic:

The service provider is the primary tenant (owner) in a CA SDM multi-tenancy installation. The first tenant added to a CA SDM installation is always the service provider tenant. The service provider tenant cannot have a parent tenant.

CA SDM associates the privileged user (typically ServiceDesk on Windows, or srvcdesk on Linux/UNIX) with the service provider tenant.

Only the service provider tenant can perform any of the following CA SDM tasks:

- Set the CA SDM options
- Set the Knowledge Management options
- Set the Support Automation options
- Create the tables or columns
- Create, edit, or delete the tenants
- Allow the tenants to have subtenants
- Update the public data

Note: An administrator can grant tenant users access to data other than their own. The Non-Service Provider tenant analysts have access to only their tenant and sub-tenants. For example, a role definition can set separate read and write access to certain tenant groups for users within that role.

Important: When a tenant is created and set as the service provider, the service provider check box and record status fields are read-only.

Service Provider Administration

The service provider can permit tenants to administer their own settings. The Tenant administrators have access to a subset of administration tasks that is the same for all tenants. The default Tenant Administrator role defines the administration functions that are available to tenant administrators. To designate a user as a tenant administrator, select the Tenant Administrator for that user role.

How Multi-Tenancy Works

This article contains the following topics:

After enabling CA SDM multi-tenancy, you can grant contacts access to all tenants (public), a single tenant, or a tenant group (user-defined or product-maintained). A contacts role controls access and specifies the read-write access independently. As the tenant access is role-dependent and a contact can modify roles during a session, contact tenant access is also subject to change.

Most of the CA SDM objects when multi-tenancy is installed include a tenant attribute to specify owner of the object. Objects fall into three groups, depending on their tenant attribute and how it is used:

Untenanted

Defines objects without a tenant attribute. All data in these objects is public.

Examples: Priority and urgency.

Tenant Required

Defines objects with a tenant attribute that cannot be null (enforced by CA SDM, not the DBMS). All data in these objects is associated with individual tenants; there is no public data.

Examples: Ticket tables (Request, Issue, and Change Order).

Tenant Optional

Defines objects with a tenant attribute that can be null. Some of the data in these objects is public, and some is associated with specific tenants. Each tenant's view of the object is a merged view of the public data and their tenant-specific data.

Examples: Category and location.

When a user queries the database, CA SDM restricts the results to objects belonging to tenants. The user is authorized to access these tenants. This restriction applies in addition to any data partition restrictions that are in effect.

If a user creates an object with update access to multiple tenants, the user must specify the tenant explicitly.

Note: Few SREL references (such as the assignee of an incident) are permitted to reference objects that belong to tenants in their containing object's tenant hierarchy. Such references are designated as SERVICE_PROVIDER_ELIGIBLE in the CA SDM object schema (the Majic). The SERVICE_PROVIDER_ELIGIBLE flag makes a difference only if the service provider tenant is not in the tenant hierarchy; if the service provider tenant is in the hierarchy, tenant validation rules permit service provider references.

Note: If CA SDM limits a user from updating tenant data, an error message can announce a data partition limitation. If you receive this error message, either data partition or multi-tenancy restrictions are in effect.

The Multi-Tenancy Option

You activate multi-tenancy by installing one of the following multi-tenancy options:

- **Off** -- Multi-tenancy is not in use. Multi-tenancy features are not available, and objects do not have a tenant attribute. This option is the default setting at a new CA SDM installation.
- **Setup** -- Multi-tenancy features are in effect for administrators, so that tenant-related objects and attributes are visible and editable. However, CA SDM does not enforce tenancy restrictions, and non-administrator users see no changes. This setting allows an administrator to prepare for multi-tenancy by performing such tasks as defining tenants or assigning objects to tenants without impacting normal use of CA SDM.
- **On** -- Multi-tenancy is fully operational. All users see the UI changes appropriate to them, and CA SDM enforces tenancy restrictions.

Tenant Information

You create and update tenants when you install multi-tenancy (in either setup or full enforcement mode). Information that is maintained for a tenant is similar to the data maintained for Organization, except for the following two attributes:

- **Logo**
  Provides a URL to an image file with the logo of the tenant. The logo is shown both on the Tenant Detail page itself, and as a substitute for the CA logo on web forms that are displayed by a tenant user or showing an object that is associated with the tenant.
- **Service Provider**
  Indicates whether the tenant is the service provider. The service provider tenant is always the first tenant added. When the administrator adds the first tenant:
  - The first tenant becomes the service provider. This designation cannot be changed.
  - The privileged user (usually ServiceDesk) and all system contacts (such as System_AHD_Generated) are set to belong to the new service provider tenant.

Note: The system user "Administrator" is added in Windows only and is not assigned a tenant. The privileged user must assign a tenant to Administrator manually.

Tenant Access

The role of a CA SDM user governs both access authorization and the user interface. The set of roles available to users depends on their access type. Multi-tenancy lets you control the tenant or tenant group that a user can access within the role.

The Role Detail page provides Tenant Access and Tenant Write Access drop-down lists on its Authorization tab. Tenant Access is view-only, and Tenant Write Access also allows create and update.

You can assign the following associations to roles:

- **Same As Tenant Access (Tenant Write Access Only)**
  Sets Tenant Write Access to be the same as the Tenant Access setting. Default for Tenant Write Access and only valid for Tenant Write Access.

- **All Tenants**
  Removes tenant restrictions. CA SDM allows a user in a role with this access to view any object in the database (read access) or create and update (write access) any tenanted object in the database. When users with All Tenant access create an object, CA SDM requires that they select the tenant of the new object.

- **Single Tenant**
  Sets a role's tenant access to a named tenant. When this option is selected, a second field appears on the web UI that allows selection of a specific tenant. CA SDM restricts a user in a role with this access to view (read access) or create and update (write access) only those objects that are associated with the named tenant. This selection is valid for either Tenant Access or Tenant Write Access.

- **Tenant Group**
  Sets a role's tenant access to a user-defined or system-maintained tenant group. When the Tenant Group option is selected, a second field appears on the web UI that allows selection of a specific tenant group. CA SDM restricts a user with the role to view (read access) or create and update (write access) only those objects that are associated with one of the tenants in the group. When a user with tenant group access creates an object, CA SDM requires that they select the tenant for the new object. This selection is valid for either Tenant Access or Tenant Write Access.

- **Contact's Tenant**
  Sets a role's tenant access to the tenant of the contact using it. CA SDM restricts a user in a role with this access to view (read access) or create and update (write access) only those objects that are associated with their own tenant. This selection is valid for either Tenant Access or Tenant Write Access.

- **Contact's Tenant Group (Analyst Only)**
  Sets an analyst's role access to the tenant group that the analyst works with, as specified on the analyst's contact record. If the user with the role is not an analyst, this selection has the same effect as Contact's Tenant. It is valid for either Tenant Access or Tenant Write Access.

- **Contact's Subtenant Group**
  Sets a role's tenant access to the Subtenant group of the contact using it. CA SDM restricts a user in a role with this access to view (read access) or create and update (write access) only those objects that are associated with their own Subtenant group. This selection is valid for either Tenant Access or Tenant Write Access.

- **Contact's Supertenant Group**
  Sets a role's tenant access to the Supertenant group of the contact using it. CA SDM restricts a user in a role with this access to view (read access) or create and update (write access) only those objects that are associated with their own Supertenant group. This selection is valid for either Tenant Access or Tenant Write Access.

- **Contact's Related Tenant Group**
  Sets a role's tenant access to the Related Tenants Group of the contact using it. CA SDM restricts a user in a role with this access to view (read access) or create and update (write access) only those objects that are associated with their own Related Tenants Group. This selection is valid for either Tenant Access or Tenant Write Access.

All users can view public data, regardless of their current role's access rights. The Update Public check box controls whether a service provider user in the role has the authorization to create or update public data. The Tenant users (users belonging to a tenant other than the service provider) cannot update public data, regardless of their role.

Edit Tenant Access for a Role

The role of a CA SDM user governs both access authorization and the user interface. The set of roles available to users depends on their access type. Multi-tenancy lets you control the tenant or tenant group that a user can access within the role.

The Role Detail page provides Tenant Access and Tenant Write Access drop-down lists on its Authorization tab. Tenant Access is view-only, and Tenant Write Access also allows create and update.

You can assign or edit tenant access for a role.

Follow these steps

1. Navigate to Security and Role Management, Role Management, Role List.

2. Click a role and click Edit.

3. Select options for Tenant Access and Tenant Write Access.
   Note: Exercise caution if you select different options for these settings.

4. Click Save.
   The updated tenant access options are saved for the role.

Tenant Terms of Usage

An end user is presented with a terms of usage statement while logging in the CA SDM application. The terms of usage statement is regarding proper usage, terms and conditions of using the product by the end user. The user must agree to the terms before logging to CA SDM. Entries are written to the standard log and in the user event log after the attempted session login.

You can perform the following terms of usage actions:

- Create, update, and delete a terms of usage statement.
- Associate a terms of usage statement with a tenant.

  Note: You must enable multi-tenancy and configure one or more tenants before associating a terms of usage statement with a tenant.

- Force the end user to accept the statement every time they log in.
- Let the end user ignore the initial statement by presenting a blank terms of usage statement.

For more information about creating terms of usage statement, see Setting Up Terms of Usage (see page 1000).

How to Configure Terms of Usage

The terms of usage statement presents the end user with an initial page statement when they log in to CA SDM. The statement reminds the user about the proper use of the product. The user must agree to the terms before they can continue to log in to CA SDM. If the end user selects Accept, CA SDM proceeds with the login and displays the main form. If the user selects Reject, CA SDM returns to the login. Entries are written to the standard log and in the user event log after the attempted session login.

Typically, you configure the contact tenant terms of usage statement. If the contact tenant is configured with an inactive terms of usage statement, the terms of usage is not configured, or if <empty> is selected in the Terms of Usage drop-down list, CA SDM displays the terms of usage statement for the tenants parent, grandparent, and so on. If no terms of usage statement is found at any level, CA SDM proceeds with the login. If you configure a tenant with a blank terms of usage statement, CA SDM proceeds with the login and displays the main form.

You can configure terms of usage as follows:

1. Enable multi-tenancy (see page 974).
2. Configure one or more tenants (see page 974).
3. Define a terms of usage statement (see page 1001).
4. Update a tenant to use the specific terms of usage statement (see page 1001).

User Interface Impact

This article contains the following topics:

Installing the multi-tenancy feature changes the user interface, depending on the authorization and tenant access that is associated with the user role. The changes affect both tenant users and service provider users.

Tenant Users

If the role of a user is restricted to a single tenant and the user is not an administrator, substitute a custom tenant logo for the default CA Technologies logo on all pages. Substitution depends on whether a logo is defined on the Tenant Detail page for the tenant.

For non-administrator tenant users, the user interface menu items or buttons allowing update or edit are suppressed for public objects. The tenant users are not authorized to update the public object.

Tenant Administrators

List pages for these objects automatically include a Public column specifying whether the list row is public data. In addition, the first element in the search filter is a Public Data drop-down list containing the following selections:

- Include (default)
- Exclude
- Only

A tenant administrator with access to multiple tenants sees a Tenant column on list pages for any tenanted object. This column takes the place of the Public column in lists of tenant optional tables.

Users with View access to a Tenant Group

A user role allows view access to multiple tenants.

- **Untenanted objects**
  Untenanted objects contain only public data. The service provider user is allowed to create or update an untenanted object only if their role has Update Public authorization. If not, the UI suppresses menu items or buttons allowing update or edit, such as the Edit button itself, or the Create New button on a list page. Tenant users cannot update public objects, and these users never see an Edit or Create New button on a list page for an untenanted object.

- **Tenant-required objects**
  Tenant-required objects contain only data associated with a particular tenant. List forms for these objects automatically include a Tenant column after the last link column. In addition, the search filter contains a tenant selector allowing the user to restrict a list to a single tenant.

- **Tenant-optional objects**
  Tenant-optional objects contain both public and tenant-specific data. List forms for these objects automatically include a Tenant column (a blank tenant indicates a public object). In addition, the search filter contains both a tenant selector and a Public Data drop-down list (the same one seen by tenant administrators).

Note: If tenant required tables incorrectly contains untenanted data in a multi-tenancy system, a public data drop-down list appears in tenant required tables. The following message: “AHD05358 is displayed. There were untenanted active xxx objects at Service Desk startup.”

Users with Update Access to Multiple Tenants

If a user role allows access to multiple tenants, or a service provider user role has Update Public authorization (typical for an analyst that works for a service provider), detail pages change as follows:

- **Untenanted objects**
  Untenanted objects contain only public data. There are no changes to their detail pages for a service provider user with Update Public authorization. If the user is in a role without Update Public authorization, or does not belong to the service provider, read-only pages for untenanted objects are with no Edit button.

- **Existing Tenant-required objects**
  Tenant-required objects contain only data that are associated with a particular tenant. Detail pages for existing tenant-required object show the object tenant as part of the standard page header.

- **Tenant-optional objects**
  Tenant-optional objects contain both public and tenant-specific data. The detail page for these objects depends on whether the user belongs to the service provider and is in a role with Update Public authorization:

  - If a service provider user role has Update Public authorization, the detail page is the same as that for tenant-required objects.

  - If the user role does not have Update Public authorization, or the user does not belong to the service provider, detail pages for public objects do not have an Edit button. Other detail pages are the same as those for tenant-required objects.

Support Automation Impact

The impact of multi-tenancy on your support environment depends on tenant and role restrictions that are placed on end users and analysts. The Service Provider manages read/write permissions for both public and tenant-specific data. For example, an analyst can handle assistance sessions from the public queue and a tenant-specific queue, but the analyst can only use Live Assistance tools that are enabled for each tenant.

For end users with Support Automation access, do not configure the end user to have write access to a tenant that is not a sub-tenant of the owning tenant of the end user, unless the foreign key (FK) group is altered to include the owning tenant. If the end user selects a login tenant, or is invited

through a ticket in a tenant that does not meet this criterion, they receive an error when they try to access the Support Automation end-user client. This restriction does not apply if the owning tenant of the end user is the service provider tenant.

For analysts with Support Automation access, do not configure the analyst to have write access to a tenant that is not a sub-tenant of the owning tenant of the analyst, unless the foreign key (FK) group is altered to include the owning tenant. If the analyst attempts to handle an end user, or invite an end user from a ticket, in a tenant that does not meet this criteria, the analyst sees an error.

Analysts and end users without read access to their tenant cannot launch the Support Automation client. For analysts, a warning message appears in CA SDM in this case, such as from the main Support Automation tab.

You can use the following roles to manage Support Automation users:

- **Support Automation Analyst**
  SA Analyst provides end-user support using Live Assistance. The Service Provider determines the appropriate tenant access and can enable Live Assistance tools and can read/write access to automated tasks.

  Important! If a non-Service Provider analyst has write access to a parent, sibling, or unrelated tenant, function access must be updated for that tenant. Analysts without read access to their tenant cannot launch the Support Automation analyst client, and a warning message appears in CA SDM, such as from the main Support Automation tab or a ticket.

- **Support Automation Administrator**
  Configures the Support Automation environment for analysts and end users. The Service Provider determines your tenant access and lets you view a tenant drop-down list on List and Detail forms. These forms let you select specific tenants or public data when searching, creating, and modifying Support Automation data in a multi-tenancy environment.
  Note: Objects such as queues, privacy levels, and chat presets are tenant optional.

Knowledge Management Impact

This article contains the following topics:

The impact of multi-tenancy on your knowledge environment depends on the tenant restrictions that are placed on users:

- **Tenant Users**
  Substitutes the logo of the tenant for the default, if the role is restricted to a single tenant.

- **Tenant Administrators**
  This option enables administrators to view both public and tenant-specific data. List pages for these objects automatically include a Public column specifying whether or not the list row is public.
  When searching for knowledge, the filter contains a Public Data drop-down list with selections of Include (default), Exclude, and Only.

Note: Objects such as approval process templates, categories, documents, files and forums are tenant optional.

Knowledge Categories and Documents

Knowledge Documents and Knowledge Categories are both tenant optional. Consider the following information for tenant optional and public objects:

- Public Knowledge Documents can only be added under public Knowledge Categories.
- Public Knowledge Categories can only be added under public categories.
- Tenant categories can be added under public categories and under tenant categories.
- Only tenant documents can be added under tenant categories.
- Public and tenanted documents can be added under public categories.

Note: The Cut/Copy/Paste category functionality is allowed only if the source and destination have the same tenant, or if the destination is public.

Repositories are defined as tenant optional, so the administrator can create different repositories for different tenants.

Embedded images are allowed only when the document and image are set to the same tenant. Attachment Folders, Attachments and Attachments to document links are also defined as tenant optional.

FAQ Rating

When viewing the FAQ rating for tenant users, consider the following information about public documents:

- Public documents are viewed by a larger audience than tenant users.
  The FAQ rating of public documents is higher than a tenant-specific document.

- Each tenant has different needs, so usage patterns are different between tenants.

The Top Solutions on the CA SDM home page displays the top five public documents, as well as a tenant's top five documents.

You can configure the Top Solutions by navigating to Knowledge, Solution Survey, FAQ Settings on the Administration tab.

Knowledge Report Card

The Knowledge Report Card allows analysts and administrators to view various metrics such as document creation, publication, hits, and votes. This report is for a predetermined time period, per analyst, category, and organization.

When using the Knowledge Report Card to provide information for a role having single tenant access, the data is limited by the tenant criteria.

Create a Remote Reference

You can configure remote references to execute external programs from the CA SDM application. CA SDM lets you create a remote reference to an external program.

Follow these steps

1. Select Service Desk, Application Data, Remote References on the Administration tab.
   The Remote References List page appears.

2. Click Create New.
   The Create New Remote Reference page appears.

3. Fill in the remote reference fields (see page) as appropriate.

4. Click Save.
   The remote reference definition is saved and the Remote Reference Detail page appears.

Remote Reference Fields

You can use the fields on the Remote Reference pages to define, search, and edit Remote Reference definitions.

Note: All search fields that allow text entry support use of the % wildcard character.

The following fields require explanation:

- **Function Access**
  Specifies the functional area where the remote reference belongs. For example, if the reference pertains to administrative functions, select Admin. If the reference pertains to notifications, select Notify.

- **Architecture Type**
  Specifies the appropriate operating environment for the remote reference (Windows or UNIX).

- **NT Server, UNIX Server, or UNIX Client Exec Command**
  Specifies the character string that executes the remote reference on a Windows server or a UNIX operating environment.

You can click the More icon to display the Additional Search Arguments field. This field is intended only for expert users who understand SQL and Majic. You can enter a SQL WHERE clause in this field to specify an additional search argument.

Audit Log List

The Audit Log List displays information regarding changes to the issue, change order, requests, and data partition tables. The audit log captures the user ID and an associated day/date/time stamp. The log also records the before and after values of the operation performed (update or insert). You can search the Audit Log List, and can use the results for report generation.

The Audit Log is automatically installed. Enable it by installing the Audit Log options with the Options Manager:

- audit_ins
- audit_upd (see Audit Log Options)

Define Form Groups

Form groups define the sets of pages in the web interface that are available to a role. Each role can have one form group. Users can display only the web pages that are included in the form group that is assigned to their role.

You can create a form group to specify which forms are visible to the members of a group.

Follow these steps

1. From the Administration tab, navigate to Service Desk, Form Groups.
   The Form Group List page appears.

2. Click Create New.
   The Create New Form Group page appears.

3. Fill in the following fields:

- **Symbol** -- A unique identifier for the form group.
- **Record Status** -- Indicates whether the form group is active or inactive.
- **Description** -- Provides a detailed description of the form group. Identifies the forms that are contained in the group or the roles that would use this form group.

SOAP Web Services Policy

This section contains the following articles:

Create a SOAP Web Services Error Type

CA SDM SOAP Web Services provide a defined set of default error types, which are created for*every* policy. The default types that are designated as *internal* error types, can be deactivated but cannot be deleted. Use the Web Services Access Policy Detail page to see the default error types when a policy is created.

CA SDM provides the following default error types:

The following information describes each internal error type:

- **ACCESS_ERROR**
  Indicates that the system failed to connect to or find a resource, such as a file or website.
- **EXCEPTION_FATAL**
  Indicates that the application is shutting down unexpectedly.
- **EXCEPTION_RUNTIME**
  Indicates that the application code encountered an exception.
- **LOGIN_ERROR**
  Indicates that the operator failed to gain access to the application.

You can create SOAP Web Services error types.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps

1. Select SOAP Web Services Policy, SOAP Error Types on the Administration tab.
   The SOAP Web Services Error Type List page appears.

2. Click Create New.
   The SOAP Create New Web Services Error Type page appears.

3. Fill in the SOAP Web Services Error Type fields (see page) as appropriate.

4. Select the Duplicate Handling tab to define the actions to take if the system detects an identical ticket that exists in the system. Select one of the following options:

   - Create the ticket and ignore duplicates. This option is the default action.
   - Do not create a ticket; add an activity log to the existing duplicate.
   - Do not create a ticket; add an entry to the CA SDM standard log.
   - Create a ticket and attach it as a child to the duplicate.

   A ticket is considered a duplicate when all following statements are true:

   - At least one ticket of the same type (request, issue, change order) and is ACTIVE.
   - The existing ticket was created using the web service.
   - The existing ticket was created with the same Policy and Error Type as the potential new ticket.
   - The create date of the existing ticket is within a specified threshold (for example, it was opened less than two days ago). This threshold is specified in the Maximum time interval for searching for duplicates field. Use the format of: HH:MM:SS.

5. Select the Return Data tab to specify data that indicates an action to take or a message displayed to the user.

6. Click Save.
   The SOAP Web Services error type is created.
   The error type definition is saved and the SOAP Web Services Error Type Detail page appears.

SOAP Web Services Error Type Fields

The following fields require explanation:

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

- **Code**
  Specifies the unique code that identifies the error type to the system. This field is required.

- **Owning Policy**
  Specifies the web services access policy that owns this error type.

- **Default**
  Indicates that this type is the default error type for the policy. Only one active default error type is allowed. If this option is selected while creating an error type, the default setting of the current default error type is removed.

- **Internal**
  Indicates whether this type is a default error type.

- **Ticket Template Type**
  Specifies the type of ticket that is created when this error is reported.

- **Ticket Template Name**
  Identifies the template to use to create a ticket when this error is reported.

> **Note:** The owning policy contact is the end user of the ticket.

Create a SOAP Web Services Policy

To minimize web services ticket flooding, and to maintain the stability of the server, CA SDM SOAP Web Services uses an Access Control and Management system. Handles excessive service activities by trusted user applications resulting from programming errors or exceptions. This system also works as a barrier and controls access to CA SDM SOAP Web Services from malicious attackers.

> **Note**: CA SDM provides a default access policy that has a code of DEFAULT. The default access policy contains no access restrictions and is only applied to sessions authenticated through username and password.

You can create SOAP web services policies to control access from SOAP web services applications.

> **Note:** If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps

1. Select Administration tab, SOAP Web Services Policy, SOAP Policies.
2. Click Create New.
3. Fill in the fields as appropriate.
4. Select the Access Control tab to define the number of operations permitted per hour for each web services category.

5. Enter a number in each operation counter field to represent the number of operations that are permitted per hour.

   Note: The default value of -1 in any operation counter indicates that no restrictions apply to the corresponding operation. A value of 0 (zero) indicates that the corresponding operation is not allowed.

6. Select the Error Types tab to review the error types in effect for the web services policy.

7. To add an error type, click Add an Error Type.

8. Click Save.
   The policy definition is saved and the SOAP Web Services Policy Detail page appears.

SOAP Web Services Policy Fields

The following fields require explanation:

- **Code**
  Specifies the unique code that identifies the access policy to the system. This field is required.

- **Proxy Contact**
  Specifies the contact to use for all web service operations and security. You can enter a contact name directly into this field, or click the search icon to select the contact name.

- **Default**
  Indicates that this policy is the default policy. Only one active default policy is allowed. If you select this option when creating an access policy, the default setting of the current default policy is removed.

- **Has Key**
  Indicates whether a public key as been associated with this policy. This field is updated when a public key is associated with a policy using the pdm_pki utility and cannot be changed.

- **Allow Impersonate**
  Allows the policyholder to invoke the impersonate() web services method and create a web services session. Additional access authentication is not performed when creating the session. However, only when the grant_level of the new user access type is less than or equal to the access_level of the proxy user access type, can this method be successfully called.

  If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

Manage Service Type and Service Type Events

This article contains the following topics:

Service types identify the levels of support service provided to or contracted by your service desk customers.

Create a Service Type

You can also use service types to categorize customers.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps

1. Select Service Desk, Service Types on the Administration tab.
   The Service Type List page appears.
2. Click Create New.
   The Create New Service Type page appears.
3. Fill in the service type fields (see page 1360) as appropriate.
4. (Optional) Use service type tabs (see page) to add events to the service type.
5. Click Save.
   The service type definition is saved and the Service Type Detail page appears.

Service Type Fields

The following fields require explanation:

- **Symbol**
  A unique identifier for this service type. Use the symbol to identify the service type. For example, to set up a service type that requires a response within an eight hour time period, assign the symbol 08_hr_resolution.
- **Ranking**
  Service types can be associated with various objects, such as contacts, organizations, categories, and priority codes. If different service types are associated with a ticket, the one that is used depends on the value in this field. The one with the lowest number has the highest priority. For

example, if an issue is opened and the Affected End-User contact has a 12-hour resolution service type, which is ranked as 2, while the priority code has a four-hour resolution service type and is ranked as 1. The service type for the issue is four hour resolution.
Enter a value of one or greater; values of 0 or negative numbers are not allowed.

- **Workshift**
  Specifies the dates, days, and hours when the service type is in effect. Usually coincides with your service desk is operating time period (for example, 24 Hours, Regular, or Non-Business Hours).
  The following rules apply to a workshift:

  - If you apply a workshift to a service type, stop and restart the service for the workshift to take effect immediately.
  - If a workshift for a service type has been specified, but one has not been specified for an event, the service type workshift is in effect.
  - If a workshift for an event has been specified, but one has not been specified for a service type, the service type workshift is ignored.
  - If a workshift for event and for service type have been specified, the service type workshift is ignored.

- **Timezone**
  The time zone for the service type. You can enter the time zone directly in this field, or click the search icon to select the time zone from a list.
  This time zone is used for triggering events in the system if the Use End-User Time Zone option is not selected.

- **Use End User's Timezone**
  Select this option if you want to use the timezone that is defined for the affected end user on a ticket for triggering events in the system.

- **Violation Cost**
  The cost that is incurred if the service type time limit is violated.

If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

Service Type Tabs

The following tabs are available on the Create Service Type, the Service Type Detail, and the Update Service Type pages:

Requests

- **Requests**
  Allows you to add service type events to request tickets. The event object type must be Request.

- **Request Tasks**
  Allows you to add service type events to Request, Incident, and Problem workflow tasks. The event object type must be Request/ Incident/ Problem Workflow Task.

- **Request Targets**
  Allows you to link a Service Type to a Service Target Template for managing Request, Incident, and Problem tickets.

Change Orders

- **Change Orders**
  Allows you to add service type events to change order tickets.

- **Change Order Tasks**
  Allows you to add service type events to change order workflow tasks. The event object type must be Issue Workflow Task (not Workflow Task).

- **Change Order Targets**
  Allows you to link a Service Type to a Service Target Template for managing Change Orders.

Issues

- **Issues**
  Allows you to add service type events to issue tickets.

- **Issue Tasks**
  Allows you to add service type events to issue workflow tasks. The event object type must be Issue Workflow Task (not Workflow Task).

- **Issue Targets**
  Allows you to link a Service Type to a Service Target Template for managing Issues.

Attach a Service Type Event

Service types determine the level of support that is given for a ticket. You can associate service type events with tickets. An event that is associated with a service type is attached to records defined with that service type.

Follow these steps:

1. On the Service Desk tab, select Incidents, Problems, Requests, Change Orders, or Issues.

2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.

3. Select the desired ticket from the list that appears.

4. Choose the Service Type tab, and click Attach Service Type Event.
   The Attach Service Type Event page appears.

5. Click Service Type Event.
   The Event Search page appears.

6. Complete one or more of the search fields, and click Search.
   The Event List displays the events that match your search criteria.

7. Select the desired event.
   The Attach Service Type Event page appears.

8. Click OK.
   The Delay Time field appears. The delay time indicates the interval of time after which the event occurs.

9. Specify the delay time as hh:mm:ss (hours, minutes, seconds).
   For example, if the event is attached to the incident at 2:20, and the Delay Time is 01:00:00 (one hour), the event occurs at 3:20.

10. Click OK.
    The ticket detail page appears with the event listed on the Service Type tab.

Create Service Type Event

You can create service type events for requests, change orders, change order tasks, issues, and issue tasks.

Follow these steps

1. From the Service Type Detail page, select the appropriate tab (Requests, Change Orders, Change Order Tasks, Issues, or Issue Tasks).
   The Event List for the ticket type appears.

2. Click Add Service Type Event.
   The Create New Service Type Event page appears.

3. Fill in the fields on this page, including:

   - **Event**
     The name of the event to which this service type event is attached. An event is a procedure that is automatically followed after a certain amount of time has elapsed. Events consist of checking for conditions and performing actions that are based on the results of those conditions. Attach events to tickets to make it easier to monitor and take measures to close these tickets.
     For example, an event may send a message if a priority 1 issue is not resolved in an hour. The event begins when an hour has elapsed. First, the system checks for the condition, which is "open issues with the priority of 1." If the condition is true, the system performs an action, which is sending the message.

   - **Delay Time**
     The interval of time after which the event occurs. Specify the delay time as hh:mm:ss (http://hhmmss/), For example, if an event is attached to an issue at 2:20, and the Delay Time is 01:00:00 (one hour), the event occurs at 3:20.

4. Click Save.
   The tab definition is saved and the Tab Detail page appears.

Delay or Resume a Service Type Event

You can delay and resume service type events.

Follow these steps:

1. Select the desired ticket from the list page on the Service Desk tab.
   The ticket detail page appears.

2. Select the Service Type tab.
   A list of any service type events that have been added to the ticket appears.

3. Click Delay or Resume.
   The Reason page appears.

4. Enter the reason, and click OK.
   The ticket detail page displays the Status of the event.

Create a Service Target Template

A service target is the estimated time frame for completing and resolving a ticket. To minimize Service Level Agreement (SLA) violations, create service target templates for analyzing each stage of ticket resolution. *A* service target template *is* a set of service targets with conditions for managing and prioritizing tickets. Each template identifies a condition, deadline, and relative cost for failing to complete the service target on time.

You can apply service target templates to requests, incidents, problems, change orders, and issues. When you link the service target template to a service type for a ticket, the service target automatically attaches only to new tickets.

On new tickets with service targets, analysts can use the Remaining Time and Violation Cost fields to prioritize ticket resolution. During ticket creation, a service type assigns one or more service targets to track each stage of the ticket resolution. Each time the ticket opens or changes, the active service target evaluates the condition. If the condition is met, the ticket and activity log show the actual completion time.

Note: If you are also using priority calculation, fields such as Priority automatically update and can affect the way service targets attach to tickets. After you configure a service target template, test your service targets on the intended ticket type.

You can create a service target template to measure service targets for requests, incidents, problems, issues, or change orders. After you create the template, you can link it to a service type.

Note: If multi-tenancy is installed, specify the tenant in the Tenant field.

Follow these steps:

1. Select **Service Desk**, **Service Target Templates** on the **Administration** tab.
2. Click **Create New**.
3. Select a ticket type from the **Object Type** field, and click **Continue**.
4. Complete the following fields as appropriate:
   - **Name**
     Defines a descriptive identifier for the service target.
   - **Object Type**
     Identifies the ticket type for this service target.
   - **Target Duration**
     Specifies the maximum amount of time for service target completion in the hh:mm:ss (http://hhmmss) format.
   - **Workshift**
     Specifies the workshift which contains a range of working hours that are used in time calculations for a service target, for example, M-F 08:00-17:00.
   - **Cost**
     Defines information such as the estimated cost associated with missing the service target.
   - **Record Status**
     Indicates whether this target is active or inactive.
   - **Condition**
     Specifies the name of the condition macro or site-defined condition. Evaluates the ticket data and determines whether the service target is met.
   - **Required Outcome**
     Specifies a True or False value that indicates whether the service target is complete.
   - **Allow Set Actual**
     Specifies whether to allow users to set the date and time for a service target.
   - **Allow Reset Actual**
     Specifies whether to allow users to reset the date and time for a service target.
5. Click **Save**.
   The service target template is created.

Create Log Interval Configuration

Interval Logging allows you to collect resource usage data from the CA SDM servers. The collected interval log is used to analyze and troubleshoot any performance or memory-related issues in the CA SDM servers. You can also share the collected data with CA Support Online to help identify and resolve CA SDM server problems.

Note: For Windows, install and add the pslist.exe tool to the windows OS %PATH% environment variable on each of the CA SDM servers.

To collect the usage data on the CA SDM servers, add the servers to the Interval Log Configuration list. Select the type of data you want to collect from each server, and change the logging options for the servers.

For example, if you select only the CPU usage option for a particular server, the utility collects the server CPU usage data.

Follow these steps:

1. Select **System**, **Interval Logging** from the **Administration** tab.
2. Click **Create New** to add an interval logging configuration.
3. Complete the fields as appropriate for the configuration.
   - **Server Name**
     Specifies the server for which you want to collect the log data. Use the Search icon to view the list of servers you can add for the interval logging.
   - **Recurrence Interval**
     Specifies the time interval during which the log data is collected for the server in hh:mm:ss (http://hhmmss/) format. For example, if the recurrence interval is set to 3 minutes, the log data is collected for every 3 minutes.
     - **Default: 3 minutes**
     - **Minimum: 2 minutes**
   - **Enabled**
     Indicates whether logging is enabled or disabled for the server. If enabled, log data is generated for the server.
   - **Record Status**
     Indicates whether the interval logging configuration is active or inactive.
   - **Scheduled Start Date**
     Specifies the start date and time for collecting the log data. If you do not enter a start date, interval logging starts immediately till the configuration is active, enabled, or scheduled end date.
   - **Scheduled End Date**
     Specifies the end date and time for collecting the log data. If you do not enter an end date, interval logging continues to run till the configuration is active and enabled.
4. Select the appropriate interval log you want to collect from the server. For example, select CPU Usage if you want to collect the log for CPU usage data.

- **CPU Usage**
  Collect the CPU usage statistics for the server by executing the pslist - x on Windows, or "ps" on Unix.

- **Memory Usage**
  Collects the memory usage data for the server by executing the pslist - m on Windows, or "ps" on Unix.

- **Network Status**
  Collects the information of all active connections and network statistics by executing the netstat /b or /a.

- **Task List**
  Collects the application and services information for all the tasks running on the server.

- **Web Session Counts**
  Collects the CA SDM sessions and user statistics for the web engine processes by executing the pdm_webstat command.

- **Server Status**
  Collect the information about all CA SDM daemons or processes on the server by executing the pdm_status command.

- **DB Report**
  Collects the information of database record types by executing the db_report command.

- **Virtual DB Info**
  Collects the information that is related to queued database requests by executing the pdm_vdbinfo command.

- **List Server Connections**
  Collects the information on active connections for the server by executing the pdm_listconn command.

- **List Slump Processes**
  Collects the information about slump connections and processes by executing the slstat command.

Note: Depending on the selected server type, the interval logging options are enabled or disabled for the server.

5. Click **Save**.
   The server is configured for interval logging.

6. (Optional) Repeat Steps 1-5 to create more interval log configurations.

How to Manage Contact Groups

This article contains the following topics:

A group is a collection of contacts that represent a specific area of responsibility within your service desk. Groups let you assign responsibility for resolving a ticket.

For example, you can have a Dallas Human Resources group responsible for dealing with personnel issues in the Dallas office. You can assign employee issues and request redressal from the Dallas Human Resources group.

You can associate request areas, locations, and a work shift with a group. You can also determine how contacts within a group can accept the automatic assignment of a request.

Create a Group

A group is a collection of contacts that represent a specific area of responsibility.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. Select Security and Role Management, Groups on the Administration tab.
2. Click Create New.
3. Complete the fields as appropriate for the group.
4. (Optional) Use the controls available on the tabs at the bottom of this page to configure the group.
5. Click Save.
   The group record is saved and the Group Detail page appears. The following buttons are now available for configuring the group:

-

- **Update Environment** -- The Configuration Item/Asset Search window for the group to specify search criteria for assets. Click Search and on the Environment Update window add and remove assets for this group.

- **Update Members** -- The Contact Search window to specify search criteria for the contacts for a group. Click Search and on th eContacts Update window to add and remove contacts for this group.

Set Up Group Notification Parameters

You can define the contact information and the method you want to use to notify a group.

Follow these steps:

1. On the Group Detail page, select the Notification tab.

2. Enter the appropriate contact information, such as Telephone Number, Fax Number, Email Address, etc.

3. Select the notification method you want to use for each message urgency level for this group (low, normal, high, and emergency).
   For example, you may want to notify this group using the Email method for normal level activities, but you may want to use the Pager_Email notification method for emergency level activities.

4. Select the workshift that is valid for each notification urgency level.
   For example, you may assign a Regular workshift (five-day week, eight-hours a day) to the normal level notification, but a 24 hour workshift to the emergency level notification.

5. Click Save to save the notification parameters.

Assign a Group to a Location

Locations precisely identify a specific physical place, such as the address of a particular company, or an office address. You can assign contacts, groups, and configuration items to a specific location.

Follow these steps:

1. On the Group Detail page, select the Address tab.

2. Enter the location where you want to assign the group, or click the search icon to select the location.
   The address information for the location is automatically filled in on the Address tab.

3. Click Save to assign the group to the selected location.

Assign a Group to an Organization

Organizations describe internal departments and divisions or external companies that can be assigned to tickets, CI classes, groups, and contacts.

Follow these steps:

1. On the Group Detail page, select the Organizational Info tab.
2. Enter the field values as follows:
   - **Functional Organization** -- The organization for which the group works.
   - **Department** -- The department where the group works.
   - **Administrative Organization** -- The organization to which the group reports for accounting purposes.
   - **Cost Center** -- The code to which this group's expenses are charged.
   - **Vendor** -- The name of the vendor associated with this group.
   - **Supervisor** -- The name of the person to which this group reports.

   Note: You can enter the values directly in the fields or click the search icon to search for the desired field value.
3. Click Save to save the organizational information to the group detail record.

Set Up a Group Environment

A group's environment consists of the equipment, software, and services they use.

Follow these steps:

1. On the Group Detail page, select the Environment tab.
2. Click Update Environment.
3. Enter the search criteria to display the desired configuration items and click Search. For more information, see Search Configuration Items.
4. From the list on the left, choose the configuration items you want to add to this group's environment. To choose multiple items, hold down the CTRL key while clicking the left mouse button.
5. When you have selected all the configuration items you want, click the double right-arrow button.
   The selected configuration items move to the Group Environment list on the right.
6. Click OK.
   The Group Detail page displays with the selected items listed on the Environment tab.

Group Remarks

You can enter notes regarding a group on the Remarks tab. These notes can be anything related to the group's role, or any other pertinent information that needs to be saved to the group detail record.

Follow these steps:

1. On the Group Detail page, select the Remarks tab.
2. Type the remarks in the Contact Notes field.
3. Click Save to save the remarks to the group detail record.

Assign Members to a Group

A group is a collection of contacts that represent a specific area of responsibility. Adding members (contacts) to your group lets you assign responsibility for resolving a ticket to several individuals who share this responsibility.

Follow these steps:

1. On the Group Detail page, select the Members tab.
2. Click Update Members.
3. Enter the search criteria to display the desired contacts and click Search. For more information, see Search Contacts.
4. From the list on the left, choose the contacts you want to assign to this group. To choose multiple items, hold down the CTRL key while clicking the left mouse button.
5. When you have selected all the contacts you want, click double right-arrow button.
   The selected contacts move to the Members list on the right.
6. Click OK.
   The Group Detail page displays, with the selected contacts listed on the Members tab.

Group Auto Assignments

The Auto Assignment tab lets you establish a relationship between change category, issues categories, and locations. You can automatically assign tickets (requests, change orders, and issues) using the request areas or category to eligible group members.

Important! The system administrator must enable automatic assignment for each request area and category individually. Listing them on the Group Auto Assignment tab does not enable this function.

Follow these steps:

1. On the Group Detail page, click Edit and select the Auto Assignment tab.
2. Click one of the following buttons:
   - Update Request Areas to select request areas for auto assignment.
   - Update Change Categories to select change categories for auto assignment.
   - Update Issue Categories to select issue categories for auto assignment.
   - Update Locations to select locations for auto assignment.

   The Search page for the selected item displays.
3. Enter the search criteria to display the items you want, and click Search.
   The Update page displays, listing the items that matched the search criteria.
4. From the list on the left, choose the desired items. To choose multiple items, hold down the CTRL key while clicking the left mouse button.
5. When you have selected all the items you want, click double right-arrow button.
   The selected items move to the Assigned list on the right.
6. Click OK.
   The Group Detail page displays, with the selected items listed on the Auto Assignment tab.

CA SDM Environment Promotion

CA Service Desk Manager Environment Promotion lets you promote configuration, customization, and object data changes between the source and target systems with minimal manual intervention. As an administrator, you can promote any configuration, customization, or object data changes between the development, test, pre-production, and production systems. For example, you can promote modified forms, added tables, columns, spel, majic files, object data to the production system. Based on the type of change (Configuration/Customization or Object Data), the environment promotion is initiated either through Command Line Interface or CA SDM User Interface.

How CA SDM Environment Promotion Works

CA SDM Environment Promotion works in the following two-phased manner:

1. Promotion of the configuration and customization of files.
   For more information, see SDMP Configuration and Customization . (see page 1374)
2. Promotion of the object data.
   For more information, see Database Promotion . (see page 1383)

All modifications made to the files, .htmpl, .mods, .spl, .maj, and so on, are directly stored in the *NX_ROOT/site/mods* folder. These files are copied from the *NX_ROOT/site/mods* folder and creates an export package. Any modification made to add tables and columns using the Web Screen Painter are stored in the database. These modifications are captured in the form of .dat files as part of the export package.

Prerequisites

Verify the following prerequisites before performing any environment promotion processes:

- To promote changes from the source to target system, ensure that the CA SDM 14.1.02 patch is applied on the CA SDM 14.1 or CA SDM 14.1.01 version.
- Close all the SDM-related files.
- Ensure that the CA SDM services are running before you perform Export or Import.
- When the environments are tenanted, both source and target systems must have the same tenants. The environment promotion does not create any tenants.
- To execute the export or import process, the user must have the operating system administrator privileges to create files and folders.
- The user must have access to Web Screen Painter to successfully execute the import process.
- The user must have read and write access to the *$NX_ROOT* *site* folder.
- Do not change the name of the exported zip file. If the exported zip file name is changed, the import process fails.
- For configuration and customization, the export or import process must be executed on the same type of servers, database, and operating systems.
  For example:
  - If an export is performed on a primary server, import of the package is allowed only on the primary server.
  - If an export is performed on a background server, import of the package is allowed only on the background server.
  - If an export is performed on a secondary server or application server, the import of the package is allowed only on the secondary server or application server.
    For more information about additional scenarios, see Approaches in Typical Environment Promotion Scenarios (see page 1374)
- Administrators are required to copy the .htmpl files to the secondary servers or application servers manually or modify the version control file to propagate the .htmpl files on the secondary servers or application servers.
- Ensure that the Apache Tomcat service is running before you perform database export.

- On Non-windows system, ensure that you enable X-Windows or an equivalent session to launch the browser for Web Screen Painter login.

- On Non-windows system, set the CA SDM bin path and CA SDM LIB path environment variables before executing the export or import process.

  For example:

```
For AIX:
export PATH=/opt/CA/ServiceDeskManager/bin:$PATH
export LIBPATH=/opt/CA/ServiceDeskManager/lib:$LIBPATH

For Solaris and Linux:
export PATH=/opt/CA/ServiceDeskManager/bin:$PATH
export LD_LIBRARY_PATH=/opt/CA/ServiceDeskManager/lib:$LD_LIBRARY_PATH
```

Tip: Performing environment promotion affects the CA SDM application performance and also restarts the services. We recommend that you perform the CA SDM Environment Promotion operations during off peak hours.

Approaches in Typical Environment Promotion Scenarios

Scenario 1: To perform environment promotion when the number of servers vary in the test and production systems.

On the source system, there is one primary server and one secondary server. Whereas, on the target system, there is one primary server and multiple secondary servers.

The environment promotion is successful when the configuration on all the servers is the same.

CA SDM Configuration and Customization

To promote your configuration and customization changes from the source to the target systems, perform the following tasks:

1. Verify the promotion prerequisites (see page 1372)
2. Export the configuration and customization (see page 1375)
3. Import the configuration and customization (see page 1376)

You can use the following SDMP command to execute the export, dryrun, or import processes:

```
sdmp -a <export/dryrun/import> -p <package name> -version
```

-a denotes actions such as export, dryrun, or import.

-p denotes the package name. This parameter is mandatory for dryrun and import processes.

-version displays the version details of CA SDM, Java, OS, Tomcat, and Database type.

-h denotes Help.

The history file *SDMP_HISTORY.HIS* located at *NX_ROOT*, captures the details of the operations performed when promoting configuration and configuration changes.

This section contains the following topics:

- Export (see page 1375)
- Import (see page 1376)
- How to Customize the SDMP CSV File (see page 1378)
- How CA SDM Environment Promotion Utility Works in Advanced Availability and Conventional Mode (see page 1380)

Export

CA SDM Environment Promotion lets you export the configuration and customization changes from the source system. These configuration and customization changes are captured on the source system, which you can import on the target system using the CA SDM Environment Promotion import process. The export process can be run on the primary, secondary, background, and application servers.

Warning: Do not initiate multiple export processes on your system.

Before initiating the export process, perform the following tasks:

- Set the **export_import_path, disk_space, timeout** property values in the SDMP Config properties file. For more information, see SDMP Config Properties File. (see page 1382)
- On Non-Windows, define the following environment variables:
  - Solaris and Linux: define the PATH and LD_LIBRARY_PATH environment variables.
  - AIX: define the PATH and LIBPATH environment variables.
    For example:

```
For Solaris and Linux:
export PATH=/opt/CA/ServiceDeskManager/bin:$PATH
export LD_LIBRARY_PATH=/opt/CA/ServiceDeskManager/lib:$LD_LIBRARY_PATH

For AIX:
export PATH=/opt/CA/ServiceDeskManager/bin:$PATH
export LIBPATH=/opt/CA/ServiceDeskManager/lib:$LIBPATH
```

Export Configuration and Customization Changes

To export the configuration and customization changes, execute the following export command:

```
Windows: sdmp -a export
Non-windows: sdmp.sh -a export
```

After initiating the ***sdmp -a export*** command, the export process validates the CA SDM release version and captures information about Java version, Tomcat Version, host name, OS name and version, CA SDM locale, database type, and server type. Files are copied as per the entries made in the *sdmp_files.csv* file. For more information, see How to make changes to SDMP Files . (see page 1378)

Warning: After export, do not rename the exported package name.

After successful completion of the export process, package and summary report files are generated. To view these files, navigate to *<export_import_path>/Promotion/Export* as specified in the SDMP Config Properties file. If the *export_import_path* property is empty, navigate to *NX_ROOT/Promotion /Export* to view the exported package and summary report. For more information, see SDMP Config Properties File. (see page 1382)

- Package

  `sdmp_export_yymmdd_hhmmss.zip`

  For example: **sdmp_export_151008_122725.zip**

- Summary Report

  `sdmp_export_summary_yymmdd_hhmmss`

  For example: **sdmp_export_summary_151008_122725.txt**

Note: You can skip the customization and promote only the configuration changes by setting *skip.validation.wsp* as *true*. For more information, see SDMP Config Properties File. (see page 1382)

If you encounter any errors or failures during the export process, verify the *sdmp.log* file in the *NX_Root/log* folder.

Import

For the import process, CA SDM 14.1 or CA SDM 14.1.01 versions must have similar installation configuration on both the source and target systems.

Before you initiate the import process, verify the following:

- Verify Prerequisites (see page 1372)
- Manually copy the exported package from the source system to the target system and place this package under the *NX_ROOT/Promotion/Import* folder. However, if you have set *export_import_path* in the SDMP config properties file, create *the Promotion/Import* folder under *export_import_path* and place the exported package.

Warning! Do not rename the exported zip file.

- Ensure that you have set the timeout value in the SDMP config properties file as per your environment. For more information, see SDMP Config Properties File . (see page 1382)
- On Non-windows system, set PATH and LD_LIBRARAY_PATH environment variables.
  For example:

```
For AIX:
export PATH=/opt/CA/ServiceDeskManager/bin:$PATH
export LIBPATH=/opt/CA/ServiceDeskManager/lib:$LIBPATH
For Solaris and Linux:
export PATH=/opt/CA/ServiceDeskManager/bin:$PATH
export LD_LIBRARY_PATH=/opt/CA/ServiceDeskManager/lib:$LD_LIBRARY_PATH
```

- (Optional) Set the **export_import_path**, **disk_space**, **timeout** property values in the SDMP Config properties file. For more information, see SDMP Config Properties File (see page 1382).
- The user must have access to Web Screen Painter to successfully execute the import process.

How to Execute the Import Process

The CA SDM Environment Promotion performs *pdm_configure* as a part of the import process.

Warning: Do not initiate multiple import processes to avoid the target system resulting in an inconsistent state.

Tip: We recommend that you execute the dryrun process before executing the import process.

Follow these steps:

1. Execute the dryrun command:

   ```
   Windows: sdmp -a dryrun -p <exported package>
   Non-windows: sdmp.sh -a dryrun -p <exported package>
   ```

   The dryrun process reports failures, if any.

   For example: **sdmp -a dryrun -p sdmp_import_151008_122725**

   The process generates a dryrun summary report that is located in the *<export_import_path> /Promotion/Dryrun* folder. The summary report contains the number of files that needs to be imported, number of records to be loaded, and failure messages related to read and write access and validation failures (Text fixes, CA SDM version, locale, Java version, server type, and database Type.)

Note: When you encounter a patch level mismatch error, you can choose to fix or ignore the error, and proceed with the import.

2. Create a backup of *NX_ROOT* folder before you proceed with the import.

Note: If the import fails, restore the application files from the location where you saved the backup.

3. Execute the Import command and follow the on-screen instructions.

```
Windows: sdmp -a import -p <exported package>Non-windows: sdmp.sh -a import -p
<exported package>
```

For example: **sdmp -a import -p sdmp_import_151008_122725.zip**
The import process performs the following tasks on the target system:

- Validates that the CA SDM version, text fixes, locale, Java version, Tomcat version, server type, and database type of the target and source systems are similar.
- Generates a summary report, which contains the number of files and records imported, in the *<export_import_path>/Promotion/Import* folder.

4. After completing the import process, verify that the changes are reflected on the target system.

Note: To verify errors or failures encountered during the import process, check the *sdmp.log* file in the *NX_Root/log* folder.

5. If any failures are encountered during import, rerun the import process using the same package.

   The import process restarts from the point of failure.

How to Customize the SDMP CSV File

The import process uses the *SDMP_FILES.CSV* file as the input file, which manages the files for promotion. This article explains how to customize the *SDMP_FILES.CSV* file.

Important: The .exe and .dll files must not be considered for promotion.

Navigate to *NX_ROOT/site/cfg* directory, edit the *SDMP_FILES.CSV* file, and create entries in a sequential order as listed below:

- **path**: Specifies the relative path from NX_ROOT.
- **file**: Specifies the file name or wildcard characters (for example: ***.***,*.xml, eiam*.config).
- **extension**: Specifies the file extension.
- **group**: Specifies the logical group of files for exporting:
  - Onetime - Files that are rarely modified and require administrator intervention to compare the differences and merge manually on the target system. These files are not replaced on the target system.
  - Copy - Copies a specific file.
  - Environment - Files specific to the environment.
  - Recursive - Applicable for folders and sub folders recursively.
  - Reports - Files related to reports.
- **parser:** Controls file processing.
  - Copy: Copies a specific file.
  - Onetime: Files grouped as onetime require administrator intervention to compare the differences and merge manually on the target system. These files are not replaced on the target system. These files are available at *export_import_path/Promotion/Import/<import package>/<exported package>*. Check the respective folder. For more information, see SDMP Config Properties File (see page 1382) .
    If the *export_import_path* property value is empty, navigate to the *NX_ROOT/Promotion /Export* folder to view the exported package and summary report.
  - Recursive: Performs a recursive copy of files and folders.
- **OS**: Specifies the operating system.
  - Both: Applicable for Windows and Non-Windows.
  - Win: Applicable for Windows.
  - Non-Win: Applicable for Non-Windows.

For example:

Path	File	Extension	Group	Parser	OS
/site/mods/interp/	*.*		Recursive	recursive	Both
/pdmconf/	NX.env.tpl	tpl	Copy	copy	Win

Path	File	Extension	Group	Parser	OS
/pdmconf/	NX.env.tpl	tpl	Copy	copy	Non-Win
/fig/cfg/	*.fmt	fmt	Reports	copy	Both
/pdmconf/	eiam*.config	properties	onetime	onetime	Both

How CA SDM Environment Promotion Utility Works in Advanced Availability and Conventional Mode

Before initiating the export process, complete the following tasks:

- Verify Prerequisites (see page 1372).
- Set the **export_import_path, disk_space** and **timeout** property values in the SDMP Config properties file. For more information, see SDMP Config Properties File. (see page 1382)
- For Configuration and customization promotion, the export or import process must be executed on the same type of servers.
  For example:
  - If an export is performed on a primary server, import of the package is allowed only on the primary server.
  - If an export is performed on a background server, import of the package is allowed only on the background server.
  - If an export is performed on a secondary server or application server, the import of the package is allowed only on the secondary server or application server.

Note: CA SDM Environment Promotion is not supported on CA SDM Standby servers.

Environment Promotion For Advanced Availability (Background Server)

CA SDM administrators must copy the .htmpl files to the application servers manually or modify the version control file to sync the .htmpl files on the application servers.

Follow these steps:

1. Export the package.
   For more information about how to export the package, see Export. (see page 1375)
2. Log in to the CA SDM target system.
3. Copy the exported zip (*sdmp_export_<timestamp>.zip*) to the *export_import_path/Promotion /Import* folder.
   If the *export_import_path* is empty, copy the exported zip to *NX_ROOT/Promotion/Import* folder.
4. Run the dryrun command.

```
Windows: sdmp -a dryrun -p <exported_zip>
Non-windows: sdmp.sh -a dryrun -p <exported_zip>
```

5. After successful dryrun, run the import command and follow the on-screen instructions.

   ```
   Windows: sdmp -a import -p <exported_zip>
   Non-windows: sdmp.sh -a import -p <exported_zip>
   ```

   The administrator performs the failover manually when the instructions for performing failover are displayed on the Command Line interface.

6. Log in to the Standby server and run the failover command:

   ```
   pdm_server_control -b
   ```

7. After failover is complete, use the new standby server (old background server). Press **Y** to continue the import process.

8. After successful import, perform failover again on the new standby server to make it as the background server. Run the following command:

   ```
   pdm_server_control -b
   ```

Note: If you want to export or import from one application server to another, see Export (see page 1375) and Import. (see page 1376)

Environment Promotion for Conventional Setup

CA SDM Environment Promotion does not support propagation of files (.htmpl) from the primary server to the secondary server. Either copy the files manually or use version control to propagate the files (.htmpl) to the secondary servers.

Follow these steps:

1. Export the package.
   For more information about how to export the package, see Export. (see page 1375)

2. Log in to the CA SDM target system.

3. Copy the exported zip (*sdmp_export_<timestamp>.zip*) to the *export_import_path/Promotion /Import* folder.
   If the *export_import_path* is empty, copy the exported zip to *NX_ROOT/Promotion/Import* folder.

4. Run the dryrun command.

   ```
   Windows: sdmp -a dryrun -p <exported_zip>
   Non-windows: sdmp.sh -a dryrun -p <exported_zip>
   ```

5. After successful dryrun, run the import command.

   ```
   Windows: sdmp -a import -p <exported_zip>
   Non-windows: sdmp.sh -a import -p <exported_zip>
   ```

Note: To export or import from one secondary server to another, see Export (see page 1375) and Import. (see page 1376)

SDMP Config Properties File

Edit the *sdmp_config.properties* file to control the behavior of the export or import process. By default, the file is installed at *NX_ROOT/site/cfg/sdmp_config.properties*.

The SDMP configuration file contains the following properties:

export_import_path

This property defines the environment promotion root folder. Set to local path, mapped drive path, or authenticated network shared path, only in the supported formats.

For example: *C:\\data\\work* or *C:/data/work*

\\\\sharedpath\\work or //sharedpath/work

If you do not specify a value, the *NX_ROOT* path is used.

disk_space:

This property is applicable for configuration and customization promotion. Ensure that you have enough disk space available on the system to execute the export or import process.

Default: 10 MB

Specify the value in MB.

timeout

CA SDM Environment Promotion uses the CA SDM pdm command utilities. If any command line utility does not respond in the specified time out period, the utility exits.

Default: 600 seconds

Specify the value in seconds.

db_data_disk_space

This property is applicable for object data promotion. Ensure that you have enough disk space available on the system to execute the export or import process.

Default: 10 MB

Specify the value in MB.

skip.validation.tomcat

Indicates if the validation or comparison of source and target Tomcat versions is skipped. If the value is set to True, validation is skipped.

Default: False

skip.validation.java

Indicates if the validation or comparison of source and target Java versions is skipped. If the value is set to True, validation is skipped.

Default: False

skip.validation.wsp

Indicates if the customization changes (WSP) on the source system is skipped. If the value is set to True, customization is skipped.

Default: False

Object Data Promotion

Perform the Export process from Command Line interface or navigate to **Administration**, **System**, **Data Export** page on the CA SDM User Interface to promote customized data from the source to the target system.

- Verify the prerequisites before initiating object data promotion (see page 1372)
- Export Object Data from the CA SDM User Interface (see page 1383)
- Export Object Data from the Command Line Interface (see page 1385)

You can manage the export and the import processes by configuring the property files.

- Import Object Data (see page 1386)
- Property Files for Object Data Promotion (see page 1388)

Note: If CA SDM is tenanted, data from a source tenanted system is promoted to a target tenanted system. CA SDM Environment Promotion does not support creation of tenants.

Export Object Data from the CA SDM User Interface

This article explains the export process when you promote object data from the CA SDM user interface.

Before initiating the export process, perform the following tasks:

- Verify the Prerequisites (see page 1372).

- Set the **export_import_path** and **db_disk_space** values in the SDMP configuration properties file. For more information, see SDMP Config Properties File . (see page 1382)
- When promoting the *risk_level* and *prptpl* objects, update the following property files located in the *NX_ROOT**pdmconf*\ folder, on the source and target systems:
  - Edit the *dbpromote.uniqkey* file and update the following properties:
    - risk_level.uniquekey=enum
    - prptpl.uniquekey=object_type, object_attrname, object_attrval, sequence
  - Edit the *DBImport.properties* file and update the following property:
    - resolve.prptpl.attributes=object_attrval

Follow these steps:

1. Log in to CA SDM user interface with privileged user access.
2. Navigate to **Administration**, **System**, **Data Export**.
3. Specify the **Start Date**, **End Date**, **Last Modified by**, **Active** fields based on your requirement.
   - **S tart Date**: Specifies the earliest modified date of the object data.
   - **End Date**: Specifies the last modified date of the object data
4. Click **Search** to view the list of objects that match the filters.
5. Select the objects that you need to promote from the **Object List** page.
6. Click **Data Export** and enter appropriate description.

   Note: Special characters such as ; : { } / * \ (# + % & ' " are not allowed in the description.

7. (Optional) Click **Data Export/Import History** in the left navigation pane to verify that no other job is in progress before you submit your job.
8. Click **Submit** on the description pop-up.
9. Click **Data Export/Import History** to verify the status and location of the data export package. One of the following status messages may be displayed as per the status of the data export package:

- **In Progress**: Indicates that the data export process is running.
- **Complete**: Indicates that the data export process for the selected objects is complete.

- **Abort:** Indicates that the in progress operation was cancelled using the **Abort** button.

You can view the exported package in the <*export_import_path*>*/Promotion/Export/DB* location on the CA SDM server.
If any errors or failures are encountered during the export process, check the *stdlog* file and the *dbpromote.log* file in the *NX_Root/log* folder.

Export Object Data from the Command Line

Apart from the CA SDM user interface, you can also export the object data from the command line.

Before initiating the export process, perform the following tasks:

- Verify the Prerequisites (see page 1372).
- Set the **export_import_path** and **db_disk_space** values in the SDMP configuration properties file. For more information, see SDMP Config Properties File . (see page 1382)
- When promoting the *risk_level* and *prptpl* objects, update the following property files located in the *NX_ROOT**pdmconf*\ folder, on the source and target systems:
  - Edit the *dbpromote.uniqkey* file and update the following properties:
    - risk_level.uniquekey=enum
    - prptpl.uniquekey=object_type, object_attrname, object_attrval, sequence
  - Edit the *DBImport.properties* file and update the following property:
    - resolve.prptpl.attributes=object_attrval

Execute any of the following commands to promote the object data changes from the source system to the target system:

```
db_promote export -d <description> -w <whereclause> -i <inputfile>
db_promote export -d <description> -w <whereclause> -f <factoryname>
```

The command line options are described as follows:

-d

(Optional) Specifies the description about the package that is exported.

-w

(Optional) Specifies the *Where* clause to filter objects for export.

Important! We recommended that you use the *Where* clause to optimize the search results.

-f

Specifies the factory name of the object.

-i

Specifies the input text file, which lists the object factory names in each row.

-h

(Optional) Denotes help for a command.

```
For Example:db_promote export -d "Export categories" -w "last_mod_dt > {unix
timestamp}" -i "C:/objectlist.txt"
db_promote export -d "Export categories" -w "last_mod_dt > {unix timestamp}" -f
"pcat"
```

After successful completion, the export process generates a zip file in the *<export_import_path> /Promotion/Export/DB* folder. If the *export_import_path* property is empty, navigate to the *NX_ROOT /Promotion/Export/DB* folder to view the exported package and summary report. The report file contains the number of objects that are exported. The exported package and the corresponding report file are shown in the following format:

```
sdmp_db_data_export_yymmdd_hhmmss.zip
```

```
sdmp_db_data_export_report_yymmdd_hhmmss.txt
```

For Example:

```
sdmp_db_data_export_151009_140940.zip
```

```
sdmp_db_data_export_report_151009_140940.txt
```

Import Object Data

You can import a data object using the Command Line interface.

Follow these steps:

1. Log in to the CA SDM target system as an administrator.
2. Create a back up of the existing database.

   Note: If the import fails, restore the database from the backup location.

3. Manually copy the exported zip file, *sdmp_db_data_export_yymmdd_hhmmss.zip,* from the source system to target system.

4. Execute the following command to validate the object schema (number of xml files, table names, and column names) in the target system and follow the on-screen instructions.

   ```
   db_promote import -v -p <path_to_the_zip_file>
   ```

   For example: *db_promote import -v -p c:/temp/sdmp_db_data_export_151008_102754.zip*

5. The command line options are described as follows:

   -p

   Specifies the import package name.

   -u

   (Optional) Performs the import using the specified user name.

   -h

   (Optional) Denotes the help for a command.

   -v

   (Optional) Validates the schema.

6. Execute the following command to import the object data:

   ```
   db_promote import -p Path_to_the_zip_file
   db_promote import -p Path_to_the_zip_file -u <sdm contact userid>
   ```

   For example: *db_promote import -p c:/temp/sdmp_db_data_export_151008_102754.zip*

7. Verify the import status by accessing Administration, System, Data Export/Import History in the CA SDM User Interface and refer the following report files generated at the *NX_ROOT/log* location:

   - **dbimport.dryrun.report.<timestamp>**: The DryRun report validates all the object schema. Schema related issues, if any, are listed here.
   - **dbpromote.log**: This file contains logs for the export/import operation.
   - **Failure_Report_<package ID>_<timestamp>**: This file contains object data failures that were encountered during import.
   - **Imported_Object_Report_<package ID>_<timestamp>**: This file contains the successfully imported object data related information.
   - **<export_import_path>/Promotion/Import/DB/Import_report_<package name>_<timestamp>**: This file contains the consolidated import summary.

Note: The **DBImport.properties** file is available *in the NX_ROOT/pdmconf/* location, which contains all configurable variables for object data import utility (db_promote). Configure this file to customize as per your environment requirements. This property file includes the following:

- **temp.work.area**
  Specifies where import will extract the exported package. If it is empty or undefined, it will use the system temp folder provided by jvm.
  For example, temp.work.area=c:\\mywork\\temp

- **domsrvr.default=domsrvr**
  Specifies the default dom server used for the data i mport process. Update the value if there are multiple dom servers.
  For example: domsrvr.default=domsrvr:02

Behavior of Abort in Import

We recommend that you do not abort the import process. The following scenarios explain the impact of Abort during the Import process.

Scenario 1: When the user closes the Command Line interface or presses the Ctrl+C key during the import process.

The status gets updated as *Aborted* in the database. In this scenario, the data import is partial, which may cause the CA SDM application to be in an inconsistent state.

Scenario 2: When the user clicks the **Abort** button on the **Administration**, **System**, **Data Export /Import History** page during the import process.

The status gets updated as *Aborted* in the database. The process keeps running on the server until the process is complete.

Important! Using the Abort button from the UI updates **only** the status as Aborted in the database and allows you to execute another process. Typically, you need to abort an import process from the user interface when it terminates abruptly.

Property Files for Object Data Promotion

This sections lists the properties files that you can manage to control the behavior of object data promotion tasks:

- Database Promote Unique Key File (see page 1389)
- Export Configuration File (see page 1389)
- Promotable Objects File (see page 1389)

Database Promote Unique Key File

The **dbpromote.uniqkey** property file that contains the secondary key in the form of key value pair for each factory is available in the *NX_ROOT/pdmconf/* location. By default, *common_name* is assumed to be the secondary key. If the *common_name* of any factory has duplicate entries, specify the attribute that works as a secondary key or combination of attributes to form a unique key in order to identify the record. This file can be customized based on requirements. Ensure that the same file exists on the source system and target system after customization.

Specify the unique key in the following format:

```
<factory name1>.uniqKey=<attribute1>
<factory name2>.uniqKey=<attribute1>,<attribute2>,<attribute3>
```

Export Configuration File

The *export.cfg* configuration file is available in the *NX_ROOT/pdmconf/* folder. You can define the following values for the object data export process:

- **MAXDEPTH:** Sets the maximum depth level for export. As this is a recursive export, it limits the export till the MAXDEPTH level, and the dependent data after the MAXDEPTH level is not exported.
  For example: If the value set to 4, data is exported till 0-3 levels.
  Default: 10

- **EXCLUDE**: Contains a list of excluded objects (factory) specified in each row. Data for the excluded objects is not exported. However, when an excluded object is referred to as a dependent object, its value is exported. Importing the objects on the target system does not load the data for the excluded objects. If the excluded object exists on the target system a link is established between the objects.

Promotable Objects File

This article lists the out-of-the-box objects that CA SDM supports for object data promotion.

S. No.	Object Name	User Interface Label	User Interface Navigation Path
1	arcpur_rule	Archive and Purge Rules	Administration tab, Archive and Purge
2	grc	CI Classes	Administration tab, CA CMDB
3	nrf	CI Families	Administration tab, CA CMDB
4	mfrmod	CI Models	Administration tab, CA CMDB
5	ci_rel_type	CI Relationship Types	Administration tab, CA CMDB
6	rss	CI Service Status	Administration tab, CA CMDB
7	ci_managed_attribute	Manage Attributes	Administration tab, CA CMDB ,Configuration Control
8			Administration tab, CA CMDB ,Configuration Control

S. No.	Object Name	User Interface Label	User Interface Navigation Path
	ci_managed_chgstat	Manage Change Status	
9	mailbox_rule	Mailbox Rules	Administration tab, Email
10	mailbox	Mailboxes	Administration tab, Email
11	KT_ACT_CONTENT	Action Content	Administration tab, Knowledge
12	CI_WF_TEMPLATES	Approval Process Templates	Administration tab, Knowledge,Approval Process Manager
13	CI_STATUSES	Document Status	Administration tab, Knowledge,Approval Process Manager
14	QUERY_POLICY	Automated Policy	Administration tab, Knowledge, Automated Policies
15	KT_FLG_TYPE	Comment Types	Administration tab, Knowledge, Documents
16	CI_DOC_TEMPLATES	Document Templates	Administration tab, Knowledge, Documents
17	KEIT_TEMPLATES	Export/Import Templates	Administration tab, Knowledge, Documents, Export/Import
18	search_source	Search Sources	Administration tab, Knowledge, Federated Search
19	EBR_NOISE_WORDS	Noise Words	Administration tab, Knowledge, Search, KT Search Engine
20	EBR_ACRONYMS	Special Terms	Administration tab, Knowledge, Search, KT Search Engine
21	EBR_SYNONYMS	Synonyms	Administration tab, Knowledge, Search, KT Search Engine
22	act_type_assoc	Activity Association	Administration tab, Notifications
23	ntfm	Message Templates	Administration tab, Notifications
24	cmth	Notification Methods	Administration tab, Notifications
25	notification_phrase	Notification Phrases	Administration tab, Notifications
26	acctyp	Access Types	Administration tab, Security and Role Management
27	dcon	Data Partition Constraints	Administration tab, Security and Role Management, Data Partitions
28	dmn	Data Partitions	Administration tab, Security and Role Management, Data Partitions
29	func_access	Functional Access	Administration tab, Security and Role Management
30	menu_bar	Menu Bar	Administration tab, Security and Role Management, Role Management
31	menu_tree_res	Menu Tree Resource	Administration tab, Security and Role Management, Role Management
32	menu_tree_name	Menu Trees	Administration tab, Security and Role Management, Role Management

S. No.	Object Name	User Interface Label	User Interface Navigation Path
33	role	Role List	Administration tab, Security and Role Management, Role Management
34	tab	Tabs	Administration tab, Security and Role Management, Role Management
35	web_form	Web Forms	Administration tab, Security and Role Management, Role Management
36	ca_tou	Terms of Usage	Administration tab, Security and Role Management
37	attr_alias	Attribute Aliases	Administration tab, Service Desk, Application Data, Codes
38	auto_close	Auto Close Settings	Administration tab, Service Desk, Application Data, Codes
39	ctp	Contact Types	Administration tab, Service Desk, Application Data, Codes
40	cost_cntr	Cost Centers	Administration tab, Service Desk, Application Data, Codes
41	country	Countries	Administration tab, Service Desk, Application Data, Codes
42	dept	Departments	Administration tab, Service Desk, Application Data, Codes
43	perscnt	End User Roles	Administration tab, Service Desk, Application Data, Codes
44	ical_event_template	iCalendar Event Templates	Administration tab, Service Desk, Application Data, Codes
45	imp	Impacts	Administration tab, Service Desk, Application Data, Codes
46	loc	Locations	Administration tab, Service Desk, Application Data, Codes
47	outage_type	Outage Types	Administration tab, Service Desk, Application Data, Codes
48	position	Positions	Administration tab, Service Desk, Application Data, Codes
49	pri	Priorities	Administration tab, Service Desk, Application Data, Codes
50	prod	Products	Administration tab, Service Desk, Application Data, Codes
51	typecnt	Reasons	Administration tab, Service Desk, Application Data, Codes
52	rptmeth	Reporting Methods	Administration tab, Service Desk, Application Data, Codes
53	resocode	Resolution Codes	Administration tab, Service Desk, Application Data, Codes
54	resomethod	Resolution Methods	Administration tab, Service Desk, Application Data, Codes
55	rc	Root Causes	Administration tab, Service Desk, Application Data, Codes
56	sev	Severities	Administration tab, Service Desk, Application Data, Codes
57	site	Sites	Administration tab, Service Desk, Application Data, Codes
58	special_handling	Special Handling Types	Administration tab, Service Desk, Application Data, Codes
59	state	States/Provinces	Administration tab, Service Desk, Application Data, Codes
60	symptom_code	Symptom Codes	Administration tab, Service Desk, Application Data, Codes
61	ctimer	Timer Setup	Administration tab, Service Desk, Application Data, Codes
62	tspan	Timespans	Administration tab, Service Desk, Application Data, Codes
63	tz	Timezones	Administration tab, Service Desk, Application Data, Codes

S. No.	Object Name	User Interface Label	User Interface Navigation Path
64	urg	Urgencies	Administration tab, Service Desk, Application Data, Codes
65	ca_cmpny	Companies	Administration tab, Service Desk, Application Data, Configuration Items
66	vpt	Company Types	Administration tab, Service Desk, Application Data, Configuration Items
67	chgcat	Categories	Administration tab, Service Desk, Change Orders
68	chg_trans	Change Order Transition	Administration tab, Service Desk, Change Orders
69	chgtype	Change Type	Administration tab, Service Desk, Change Orders
70	chgcnf_status	Change Conflict Status	Administration tab, Service Desk, Change Orders
71	risk_svy_tpl	Risk Survey Template	Administration tab, Service Desk, Change Orders
72	chgstat	Change Order Status	Administration tab, Service Desk, Change Orders
73	tskstat	Workflow Task Status Code	Administration tab, Service Desk, Change Orders
74	tskty	Workflow Task Types	Administration tab, Service Desk, Change Orders
75	fmgrp	Form Group	Administration tab, Service Desk
76	isscat	Issue Categories	Administration tab, Service Desk, Issue
77	iss_trans	Issue Transition	Administration tab, Service Desk, Issue
78	issstat	Issue Status	Administration tab, Service Desk, Issue
79	mobile_attrs	Mobile Attribute	Administration tab, Service Desk, Mobile
80	response	Personalized Responses	Administration tab, Service Desk
81	prpval_rule	Property Validation Rules	Administration tab, Service Desk
82	pcat	Areas	Administration tab, Service Desk,Request/Incident /Problems
83	in_trans	Incident Transitions	Administration tab, Service Desk,Request/Incident /Problems
84	pri_cal	Priority Calculation	Administration tab, Service Desk,Request/Incident /Problems
85	pr_trans	Problem Transitions	Administration tab, Service Desk,Request/Incident /Problems
86	cr_trans	Request Transitions	Administration tab, Service Desk,Request/Incident /Problems
87	transition_type	Transition Types	Administration tab, Service Desk,Request/Incident /Problems

S. No.	Object Name	User Interface Label	User Interface Navigation Path
88	seq	Sequence Numbers	Administration tab, Service Desk
89	svc_contract	Service Contracts	Administration tab, Service Desk
90	tgt_time_tpl	Service Target Templates	Administration tab, Service Desk
91	risk_level	Risk Level	Administration tab, Service Desk, Change Order
92	mgs	Managed Survey List	Administration tab, Service Desk Surveys, Managed Surveys, Managed Survey List
93	mgsstat	Managed Survey Status	Administration tab, Service Desk, Surveys, Managed Surveys
94	svy_tpl	Survey Templates	Administration tab, Service Desk, Surveys
95	saprobtyp	Error Types	Administration tab, SOAP Web Services Policy
96	sapolicy	Policies	Administration tab, SOAP Web Services Policy
97	closure_code	Closure Codes	Administration tab, Service Desk, Change Orders
98	org	Organizations	Administration tab, Service Desk, Application Data, Codes
99	wrkshft	Workshifts	Administration tab, Service Desk, Application Data, Codes
100	crsq	Stored Queries	Administration tab, Service Desk, Application Data
101	crs	Status	Administration tab, Service Desk,Request/Incident /Problems
102	evt	Events	dministration tab, Events and Macros
103	macro_type	Macro Types	Administration tab, Events and Macros
104	macro	Macros	Administration tab, Events and Macros
105	aty	Activity Notifications	Administration tab, Notifications
106	ntfr	Notification Rules	Administration tab, Notifications
107	ntfl	Object Contact Notification	Administration tab, Notifications
108	sdsc	Service Type	Administration tab, Service Desk

CA SDM Environment Promotion Limitations

The following limitations apply to CA SDM Environment Promotion:

1. Delete operation is not supported.
   For example, removing a role from an access type on the source system does not get promoted to the target system.

2. Selective customization promotion is not supported.
   For example, a user who has created multiple schema changes in the development system cannot promote selective changes to the target system.

3. Objects in the exclude list that are defined in the *NX_ROOT/pdmconf/export.cfg* file get linked to the promoted object only if those records are available in the target system.
   For example, OOTB cnt object is in the exclude list and you try exporting a pcat object with area *as testarea* having an assignee as *testuser*. After importing the pcat object to the target system, if the user (*testuser)* exists on the target system, the *testarea* record is linked to the *testuser* as an assignee. If the user (*testuser*) does not exist on the target system, the assignee field for this record is empty.

4. CA SDM administrators cannot promote a soft link on a Non-Windows system.

5. When you press **CTRL+C** on the console where the promotion operation is running, a confirmation message appears **(Y/N)** to terminate the job. The promotion operation is terminated irrespective of the selection.

6. When exporting or importing large amount of data, you may observe the following scenarios:

   a. If you encounter the error *Exception in thread "main" java.lang.OutOfMemoryError: Java heap space* during import, do the following tasks:

      - **Update the JVM:**

        - Navigate to the *NX_ROOT*/bin/ folder and open the *db_promote.bat* file in edit mode.

        - Add the memory heap size parameter to the data import manager jar file: % NX_JRE_INSTALL_DIR%/bin/java" -cp %JAVA_CP% com.ca.ServicePlus.dataimport.DataImportManager -a %*
          For example: Add the heap size as 1024MB to the data import manager jar file: %NX_JRE_INSTALL_DIR%/bin/java" **-Xmx1024M** -cp %JAVA_CP% com.ca.ServicePlus.dataimport.DataImportManager -a %*

          Note: For a 32-bit operating system, you can define the maximum heap size as 4 GB only.

      - **Reduce the export package size in the following ways:**

        - Select a smaller filter range from the User Interface.
          For example, search filter is set to 30 days, reduce the date range to 15 days and export again.

        - Decrease the value of the MAXDEPTH property in the *NX_ROOT/pdmconf/export.cfg* file.
          The objects that are exported are restricted to the defined maximum level. Manually export the dependent objects that are beyond the maximum depth level.

b. When large amount of MDB data is selected for promotion, export or import may take several hours to complete. Before you initiate export or import, perform MDB level setting. For more information about the MDB level setting, see How to Move the CA MDB Data from the Source to the Target Systems (see page 747).

Configuring CA Service Catalog

This section contains the following articles:

Manage Business Units and Tenant Administration

This article contains the following topics:

Understand Business Units and Catalog Access

Administrators create and maintain business units (tenants) as the organizational structure that controls access to data. Business units can be:

- A service provider (the highest level or *root* business unit).
- An external client company, if the service provider provides services to external customers.
- An internal corporate department or group within a department.

A business unit administrator can:

- Access the catalog that the business unit publishes.
- Subscribe accounts to services.
- Perform other administrative duties for the business unit and its child business units.

The following rules apply when you create your business unit structure:

- Business units can have child business units.
- Users can have roles in more than one business unit.

- Business units can have one or more accounts.
- Each account can have many users.
- Each user can have many accounts.
- Each user who has an account can be billed to that account.
- When you request a service, the parent business unit of your business unit defines the catalog that you see.
- When you subscribe an account to a service, the parent business unit defines the catalog that you access.

By default, users and accounts can request or subscribe to items *only* in the catalog of their parent business unit.

Example

Review the following example of a four-level hierarchy of business units, in a default configuration:

Service Provider (SP) is the top-level business unit.

- A is a child business unit of SP.
- B is a child business unit of A.
- C is a child business unit B.

In linear form, you can express the relationship as follows: SP-->A-->B-->C

- "A" Users and accounts can request or subscribe to items in the SP catalog *only*.
- "B" Users and accounts can request or subscribe to items in the A catalog *only*.
- "C" Users and accounts can request or subscribe to items in the B catalog *only*.

To change the default behavior, use the following configuration settings:

- The System configuration settings **Use Service Provider Configuration Only** and **Use Service Provider Catalog Only.**
- The Catalog configuration setting that is named **Pass Through Catalog.**

Note: For more information about how to modify configuration settings, see the System Configuration (see page 1461) and Catalog Configuration (see page 1449) section.

Decide Between Common And Stand-Alone Tenant Administration

Administrators decide between *common* or *stand-alone* tenant administration, as follows:

- In *common* tenant administration, you create and maintain a single tenant structure for CA Service Catalog and CA Service Desk Manager. Both parent and child tenants are created in CA Service Desk Manager *only*. You can edit common (shared) attributes (see page 1405) of tenants in CA Service Desk Manager *only*. CA Service Catalog "inherits" the tenants, their structure, and their common attributes from the CA Service Desk Manager. These features appear as read-only in CA Service Catalog. In CA Service Catalog, you can still edit the CA Service Catalog-specific attributes (see page 1405).

- In stand-alone tenant administration, you create and maintain tenants in CA Service Catalog only. The parent and child tenants apply only to CA Service Catalog. Tenant administration functions and tenant attributes are not shared between CA Service Catalog and any other product. If CA Service Desk Manager is installed, you create and maintain its tenant structures separately from CA Service Catalog. Stand-alone tenant administration is the default.

- Common tenant administration ensures efficiency and consistency in your tenant structures for applicable products providing a single point of administration. You can administer tenants once rather than multiple times in CA Service Catalog and CA Service Desk Manager. You can leverage a common data model and thus save costs for multiple service providers and other large organizations.

- Stand-alone administration provides flexibility for tenant structures across products. Thus, to use separate tenant structures for CA Service Catalog and CA Service Desk Manager, use stand-alone administration. For example,

  - You have installed CA Service Catalog *without* CA Service Desk Manager.

  - You have installed CA Service Catalog with CA Service Desk Manager. *However*, you want to administer the business units for CA Service Catalog separately from these other products.

- If you have already implemented separate tenant structures in both products, you perform synchronization activities to enable common tenant administration.

- Continue using your chosen option for the long term, preferably throughout the life cycles of the applicable products. Perform synchronization activities whenever you change from stand-alone tenant administration to common tenant administration.

- As a best practice for efficiency and consistency across applicable products, use common tenant administration.

Note: Common tenant administration has no effect on how you manage users and accounts.

Important! Do *not* move a CA Service Catalog tenant if it has a subscription or a request for an associated account. When such subscriptions exist, moving a tenant impacts its business rules and can cause problems in request management.

Configure Common Tenant Administration

This article contains the following topics:

Common tenant administration (also named multi-tenant administration) lets administrators use a single administration tool to simultaneously create and maintain business units (tenants) for multiple products, including CA Service Catalog and CA Service Desk Manager. To configure CA Service Catalog to use common tenant administration, follow this process:

Important! This topic applies *only* if your organization has CA Service Desk Manager installed.

1. Meet the prerequisites: Verify that CA Service Catalog and CA Service Desk Manager are installed and share the same MDB.
2. Configure the tenancy settings (see page 1399) in CA Service Desk Manager.

   Important! CA Service Catalog requires a tenant of type Service Provider in CA Service Desk Manager, as a prerequisite for completing this process.
3. Create the common tenant mapping file (see page 1399).
4. Prepare to run the common tenant merge utility.
   This utility uses the information in the common tenant mapping file to create a shared tenant structure between CA Service Catalog and CA Service Desk Manager.
5. Run the common tenant merge utility (see page 1400).
6. Set the configuration variables for common tenant administration (see page 1401).
7. (Optional)Implement a common terms of use agreement (see page 1403) for common tenants.

8. Note the effects of common multi-tenancy on business unit functions (see page 1405).

Configure the Tenancy Settings in CA Service Desk Manager

Configure the tenancy settings in CA Service Desk Manager to support the integration with CA Service Catalog.

Follow these steps:

1. Log in to CA Service Desk Manager as ServiceDesk(administrator).
2. Click Administration, Option Manager, Multi Tenancy.
3. Verify that the multi-tenancy option is on.
4. Verify that the multi-tenancy depth is 10.
5. Click Administration, Security and Role Management, Tenants.
6. Click Create New to create a tenant, if no tenant of type Service Provider exists. Enter a meaningful name for the new tenant.
7. Verify that Service Provider Checked is on and Subtenants Allowed is on.

You have configured the tenancy settings in CA Service Desk Manager to support the integration with CA Service Catalog.

Create the Common Tenant Mapping File

When you configure common tenant administration (see page 1398), a required task is creating the common tenant mapping file. Map tenants between CA Service Catalog and CA Service Desk Manager, so that both products use the same tenant structure.

Follow these steps:

1. Review the tenant structures in CA Service Catalog and CA Service Desk Manager. Plan the merged structure that you want to use.
2. Stop the CA Service Catalog services on the computer where MDB is installed.
3. Open the CA Service Catalog command prompt by clicking Start, Programs, CA, Service Delivery, Service Delivery Command Prompt.
4. At the CA Service Catalog command prompt, enter the following ant command:

   ```
   ant generate-merge-config
   ```

   The common tenant merge utility runs and creates the tenant mapping file, which is named merge-tenants.conf. The utility:

   - Creates the initial mapping entry, which maps the Service Provider business units for each product to each other. This entry is the only *required* entry. The CA Service Catalog entry is named ca_tenant, and the CA Service Desk Manager entry is named usm_tenant_ext.

- Lists the names and database IDs of all CA Service Catalog tenants
- Lists the names and database IDs of all CA Service Desk Manager tenants

You use these names and database IDs to create the mapping entries.

5. Open the merge-tenants.conf file that is located in USM_HOME, using a text editor. After the Service Provider mapping entry, add a new line for each new mapping entry that you create. Specify each entry using the following format, using the Service Provider entry as a model:

   ```
   <usdk> business unit ID=<bcsc> business unit ID
   ```

   For example:
   0x60B4EAC8B85E41DH97E647CF84A93CFA=87958EK983987D42AB2A4PAEF808C129

   Important! Mapping a parent tenant maps the parent *only*, *not* the children! Therefore, for automatic mapping, eit*her* map parents and children individually *or* omit the mapping of the parent.

6. Follow the rules for creating entries in the common tenant mapping file (see page 1401).

7. Review the sample common tenant mapping file (see page 1402) and verify the contents of your mapping file.

8. Restart the CA Service Catalog services that you stopped at the beginning of this procedure.

You have created the common tenant mapping file. You are ready to run the utility.

Run the Common Tenant Merge Utility

Follow these steps:

1. Open the CA Service Catalog command prompt on the computer where the MDB is installed. Click Start, Programs, CA, Service Delivery, Service Delivery Command Prompt.

2. Enter the following command:

   ```
   ant merge-tenants
   ```

   The utility prompts you for the name (**Default:** merge-tenant.conf) and location (**Default:** USM_HOME) of the common tenant mapping. The utility also prompts you for the password for any administrator with the Service Provider role in CA Service Catalog. An example is the default user named spadmin. If running the utility creates tenants in CA Service Desk Manager, you enter this password.

3. The utility summarizes the changes to be made in the tenant table in the MDB for each product. The utility also creates any missing tenants in those tables.

4. Restart the CA Service Catalog services that you stopped at the beginning of this procedure.

5. Start CA Service Catalog and CA Service Desk Manager. Verify that the tenant structure and common attributes (see page 1405) of tenants are the same in both products.

You have run the common tenant merge utility.

Important! If the same name is used for two or more tenants being created in CA Service Desk Manager the utility aborts. In such cases, check the tenant structure of each product. Rename any duplicate tenant names and ensure that they are unique. Run the utility again.

Set Configuration Variables

When you configure common tenant administration (see page 1398), setting the related configuration variables is a required task.

Follow these steps:

1. Log in to CA Service Catalog as a user with the Service Delivery Administrator role.
2. Click Administration, Configuration, System Information.
3. Verify that the value of the option *Common Tenant Data Synchronized* is Yes. This value is read-only. "No" indicates that a discrepancy exists between the tenant structures of CA Service Desk Manager and CA Service Catalog. Verify the accuracy of the common tenant mapping file and run the common tenant merge utility again.
4. Set the value of the option *Common Multi-tenant Administration Enabled* to Yes.
   When this setting is Yes, common multi-tenant administration is enabled for CA Service Catalog, through CA Service Desk Manager.

You have set the configuration variables for common tenant administration.

Rules for Mapping File Entries

When you configure common tenant administration (see page 1398), a required task is creating the common tenant mapping file (see page 1399). Follow these rules when creating entries in this file:

Important! Violations of any of these rules cause the common tenant merge utility to abort.

- Do not map business units that are at different levels in CA Service Desk Manager and CA Service Catalog.
- Do not map the same business unit more than once. If you have several business units, print the merge-tenants.conf file and mark each business unit after you map it and save the file.

- Map a child only after mapping all its parents. Map the parents from the tenant level directly above the child through the level directly under the Service Provider business unit.
- Verify that tenant names are unique across all products. For example, if you have a tenant AAA in CA Service Desk Manager and CA Service Catalog, rename at least one of them to a unique name.
- Verify that the values in CA Service Desk Manager for common attributes meet your requirements for CA Service Catalog. This requirement is for every tenant and sub-tenant that you map. Doing so is important because for common attributes, the CA Service Desk Manager values overwrite the CA Service Catalog values.
- Do *not* map that tenant or any of its sub-tenants explicitly in the merge-tenants.conf file, to add a complete tenant structure from one product to the other automatically. Instead, run the common tenant merge utility and confirm that you want to add any tenants that are not mapped in the merge-tenants.conf file. The utility then adds the complete structures of any unmapped tenants to each product automatically.

Sample Common Tenant Mapping File

Review the following sample common tenant mapping file and construct your own file:

```
...
# CA Service Catalog Tenants (id, name)
# ca.222.com   ca.222.com
# 00234A51DC4A4F70A03D3BDE5526278C   BB
# 9F6309A0CB654781B08080AD78C2280F   CC
# 9CF5655B4B8D4833A0C6E74EB56128C5   AA
#
# CA Service Desk Manager Tenants (id, name)
# 0xB3484A535A3D994B9FBCD28D3845F292   ca.111.com
# 0xBB83719AA93DFC48B909D7D72CF8B0CB   A
# 0xD9DC8FF2EB84CC43988FE71F4B489D3D   E
# 0x67958EA983987D42AB2A4BAEF808C029   D
#
# Service Provider tenants must map to each other. This mapping is mandatory.
0xB3484A535A3D994B9FBCD28D3845F292=ca.222.com
#
# Map A to AA
0xBB83719AA93DFC48B909D7D72CF8B0CB=9CF5655B4B8D4833A0C6E74EB56128C5
...
```

In this example, the following tenants exist:

- CA Service Desk Manager tenants: ca.111.com, A, D, and E.
- CA Service Catalog tenants: ca.222.com, AA, BB, and CC.

Service Provider tenants must map to each other. Hence, you merge the CA Service Desk Manager Service Provider tenant (ca.222.com) and the CA Service Catalog Service Provider tenant (ca.111.com).

Otherwise, you add a mapping entry only when you want to merge two tenants together. For example, in the sample file, you merge CA Service Desk Manager tenant A and CA Service Catalog tenant AA.

When you merge tenants, the CA Service Desk Manager tenant only overwrites common attributes in the CA Service Catalog tenant. The CA Service Catalog-specific attributes remain intact. After you run the common tenant merge utility with this sample file, the tenant ca.222.com in CA Service Catalog is renamed ca.111.com. Similarly, tenant AA in CA Service Catalog is renamed A. The tenants inherit the other common attributes (see page 1405) of the CA Service Desk Manager tenant with which it was merged.

If you are simply adding tenants from one product to the other, do not map them in the common tenant mapping file. For this reason, the sample file does not map any other tenants. Thus, the following changes occur when you run the common tenant merge utility with this sample file:

- CA Service Catalog tenants BB and CC are added to CA Service Desk Manager.
- CA Service Desk Manager tenants E and D are added to CA Service Catalog.

(Optional) Implement Common Terms of Use Agreement

You can optionally implement a common terms of use agreement for CA Service Catalog and CA Service Desk Manager. Doing so helps enforce a consistent login policy for all common tenants in both products. CA Service Desk Manager administrators create and maintain this agreement in CA Service Desk Manager. CA Service Catalog administrators configure CA Service Catalog to adopt this agreement.

Note: Verify that the CA Service Desk Manager setting meets the needs of your organization. For more information about configuring terms of use agreement in CA Service Desk Manager, see the CA Service Desk Manager documentation.

1. Select Administration, Configuration, System Information in CA Service Catalog.
2. Specify Yes for the setting *Terms of Usage Prompt Enabled*. If you specify No, then users attempting to log in to CA Service Catalog are *not* prompted to accept the terms of use agreement.
3. Review the effect of the CA Service Desk Manager setting on users logging in to CA Service Catalog. The effect depends on the terms of use agreement that is configured for the common tenant in CA Service Desk Manager.

- If the common tenant has an active, defined (not empty) terms of use agreement, prompt the user to accept it at every login.
- If the common tenant has no terms of use agreement that is defined, or if the agreement is inactive, review the parent hierarchy of the tenant. Then perform the following steps:

- If the nearest parent has active but empty terms of use agreement that is defined, then do not prompt the user with any terms of use agreement. Otherwise, prompt the user to accept the terms of use agreement of the nearest parent tenant that has an active terms of use agreement defined.

- If no parent tenant has an active, specified terms of use, do not prompt the user with any terms of use.

- If the common tenant has an active terms of use agreement defined but is configured to suppress it, then do *not* prompt the user to accept it.

- If users attempting to log in to CA Service Catalog receive the prompt to accept the terms of use agreement but do not accept it, they cannot access CA Service Catalog.

Manage Common Tenants

When common tenant administration is enabled, all tenants exist in both CA Service Catalog and CA Service Desk Manager. Administrators can manage these tenants using CA Service Desk Manager, but not CA Service Catalog. Here, *managing* means adding or deleting tenants, or editing their common attributes. In CA Service Catalog, you can *view* tenants and all their attributes. But you can edit only the CA Service Catalog-specific attributes.

Follow these steps:

1. In CA Service Catalog, view the business units by clicking Administration, Business Unit, and:

   - Verify that any new business units that you created in CA Service Desk Manager are visible in CA Service Catalog.

   - Verify that any inactive business units in CA Service Desk Manager are not visible in CA Service Catalog.

   - Verify that you cannot add or delete business units or edit their primary attributes in CA Service Catalog.

   - Note the effects of common multi-tenancy on business unit functions (see page 1405).

2. In CA Service Desk Manager, perform the following actions:

   - Create one or more new tenants, as needed.

   - Make inactive any tenants that you no longer want to use, if applicable.

   - Edit the common attributes such as description, contact, location, inactive.

   - Optionally, implement a common terms of use agreement (see page 1403).

   - Verify the CA Service Desk Manager and CA Service Catalog tenant and business unit settings that follow. Update these settings, if necessary. These settings enable the tenant mapping between the products.

To begin some of these tasks, select Administration, Security and Role Management, Tenants, Start. For more information about how to perform these tasks, see the CA Service Desk Manager documentation.

Tenant Setting for CA Service Desk Manager	CA Service Catalog Business Unit Setting
Service Provider selected (on)	Service Provider (SP), meaning root or highest level business unit
Subtenants Allowed selected (on)	Contains Sub Units: True, meaning Super Tenant. A super tenant is a tenant with at least one subtenant.
Subtenants Allowed not selected (off)	Contains Sub Units: False, meaning Tenant, also named leaf (end-of-tree) tenant. A subtenant is a tenant with at least one parent tenant.
Inactive Tenant	inactive, formerly deleted tenant
Parent Tenant is Empty	SP is the parent tenant

Effects of Common Tenant Administration

After you have completed configuring common tenant administration (see page 1398), the following results occur in CA Service Catalog:

- A new configuration item appears on the Administration, Configuration page. The name of this item is *Common Multi-Tenant Administration*. Its default setting is No. When you set this option to Yes, the following changes occur:
  - The *common attributes* of the tenant become read-only from CA Service Catalog. You can edit these common fields in CA Service Desk Manager *only*:
    - The Business Unit Name and Description in the General Information section
    - All fields in the Primary Contact Information section
    - All fields in the Location Information section
  - You can edit the *CA Service Catalog-specific attributes* in CA Service Catalog. These attributes include the following fields:
    - Federal Tax Payer ID, State Tax Payer ID, Tax Region
    - Timezone, Currency Name, Date Format, Time Format
    - Decimal Symbol, Opened Date, Email, Web Site
  - The options to add, delete, edit, cut, and paste tenants are disabled.
  - A message appears on the Administration, Business Units page explaining why these functions are disabled.
- If you implement a common terms of use agreement (see page 1403), then the terms of use settings in CA Service Desk Manager govern the attempts of users to log in to CA Service Catalog.

Configure Stand-Alone Business Units

Stand-alone administration means that you use CA Service Catalog alone to manage business units, as follows:

1. Select **Administration**, **Business Units**.
2. Expand the business unit tree and find the business unit that you want.
3. (If applicable) Click the Add icon to add a child business unit. Complete the fields on the **Add a New Business Unit page**, and click OK.

Add a New Business Unit Page

The following fields require explanation:

- **Business Unit Login ID**
  Specifies the value that you use to log in to a business unit (except the service provider business unit). You also use this value when running IXUtil import and export commands. This value must be unique.

- **Business Unit Name**
  Specifies the name of the business unit.
  This field defaults to the same name as the Business Unit Login ID. The Business Unit Name appears throughout the user interface and in all reports and invoices.

- **Business Unit ID**
  Identifies an automatically generated, read-only value, whether you are using common or stand-alone tenant administration (see page 1397).
  After you create the business unit, CA Service Catalog automatically fills in this field. The only exception is the service provider business unit. You specify its business unit ID during the Catalog Component installation and cannot change this ID afterwards.
  If necessary, use the Business Unit ID field for reference. For example, you change your method of tenant administration from stand-alone to common (see page 1397). In that case, you use the business unit ID when you create a common tenant mapping file (see page 1399). You also use the business unit ID with IXUtil and web services.

- **Opened Date**
  Specifies the date when the business unit becomes part of your organizational structure, in local time.

- **Currency Name, Date Format, Time Format, Decimal Symbol**
  Specify the currency name, date and time formats, and decimal symbol that must appear on the user interface. These specifications appear, for example, when users create and manage requests. They also appear when administrators create and maintain services, users, and so forth.

- **Contains Sub Units**
  Specifies whether this business unit can have sub business units (child business units).

  Note: You *cannot* change this setting after you have created the business unit.

- **Create Dashboard Library Namespace**
  Specifies whether to create a folder for the business unit in the Dashboard Library. Doing so helps organize the contents of the library.

- **Single Account Mode**
  Specifies whether the business unit can contain *only one* account.
  If you select this option, specify the name of the single account.

  Note: You *cannot* change this setting after you have created the business unit.

  Create Document Namespace
  Specifies whether to create a folder for the business unit in the Documents folder. Doing so helps organize the contents of the folder.

- **Primary Contact Information**
  Specifies the user ID of the primary contact for the business unit.

- **Theme**
  Specifies the settings for several look-and-feel elements, including images and icons (*except for* logos), menus, and tabs. When applicable, these elements include colors, font name and point size, highlighting, and related specifications. You customize these look-and-feel elements by editing the Cascading Style Sheet (CSS) files for the theme.
  The look-and-feel of the UI matches the theme of the business unit that you are logged in to. If a business unit does not have its own theme, it uses the theme of its closest parent business unit. You can use the same theme for all business units. Alternatively, you can optionally create and use different themes for different business units. If you update a theme for a specific business unit, the change affects the users of that business unit. The change also affects any child business units that do not have their own theme specified. For more information about customizing themes, see the Modify the Branding (see page 2020) section.

- **Logo**
  For each business unit, you can optionally specify a *business unit* logo. This logo replaces the *global* logo in the heading on product pages and request emails of the business unit. You can use a business unit logo to support the brand or other messaging uniquely for a business unit. You can update the logos for every business unit or only for specific business units. For example, you can decide to customize logos only for super tenants directly under the root business unit.

  Important! If you have enabled multi-tenancy with CA Service Desk Manager, CA Service Catalog uses the logo that CA Service Desk Manager specifies. If no CA Service Desk Manager logo applies, then each business unit uses the CA Service Catalog global logo.

  If the child business unit has its own logo, users who log in to it see the child logo. Else, users who log in to it see the global logo. Users with access to multiple business units can see different header logos when they log in to each business unit.

- **Location Information**
  Specifies the location of the business unit.

Manage Users and Assign Roles

This article contains the following topics:

Basic Information About Users

A user in CA Service Catalog typically represents a person who uses the product. A person must have a user ID to log in and use CA Service Catalog. Each user requires a role (see page 1414) and the user must belong to a business unit.

User Data in the MDB

The MDB stores user-related information for multiple CA products. For example, CA Service Catalog and other CA products share users and contacts. Therefore, use caution when managing users.

Some data in the MDB is product-specific and is not shared between products. For example, CA Service Catalog does not share role information. The MDB contains several users that CA Service Catalog does *not* use but that *other CA products* use. Examples are System_ADH_generated, System_AM_User, Systemt_Anonymous, System_Argis_User, System_MA_User, System_NSM_generated, System_SD_User, and UAPM Administrator.

The MDB stores user IDs and all other user data *except* passwords.

User Data in CA EEM

The user ID of each CA Service Catalog user maps to a matching user in CA EEM.

When a user logs in to CA Service Catalog, it passes the user ID to CA EEM for authentication. If CA EEM does *not* use an external directory, CA EEM authenticates the user ID. If CA EEM uses an external directory, the external directory authenticates the user ID.

If CA EEM uses an external directory, the Catalog system fetches important user details from the external directory. Examples include the first name, last name, email address, and organizational hierarchy. This fetching helps create the user quickly and efficiently.

CA EEM also controls access for each role to CA Service Catalog components.

External Directories

If you use an external directory to maintain CA Service Catalog users, perform the following tasks:

- Configure CA EEM to use an external directory.
- Synchronize the MDB users with the external directory users.

These tasks help verify that all CA EEM users have matching CA Service Catalog users.

Single Sign-On

If your organization uses a Windows domain, you can configure CA Service Catalog to use Single Sign-On. For more information, see the section Configure Single Sign-On Using Windows NTLM authentication (see page 1429).

User Groups

You or other administrators can organize CA Service Catalog users into the following types of user groups:

- Global and Application user groups in CA EEM

An application group that CA Service Catalog uses is the Super User.

Note: For information about creating these groups and assigning users to them, see your CA EEM documentation.

- User-defined groups in CA EEM

You create user-defined groups, in either your external directory (if applicable) or CA EEM. You can apply the same action to all users in the user-defined group, instead of modifying the users individually. Once you create a user-defined group in CA EEM or your external directory, it is available in CA Service Catalog.

User group memberships appear as *read-only* data in user profiles.

Note: For information about creating user-defined groups, see the Manage Users with CA EEM (see page 1418) section.

Authorization Level

You can specify an authorization level for each business unit in which the user has a role. The system approval process is the only approval process that uses the authorization level. By default, the following levels are available with the text and numeric values shown:

- Level 0 (0)
- Level 10 (10)
- Level 20 (20)
- Level 30 (30)
- Level 40 (40)
- Level 50 (50)

In the system approval process, each *user* has an authorization level and each *service* has an approval level. The Catalog system automatically approves requests from users whose authorization level matches or exceeds the approval level of the service. Otherwise, the system follows a managerial hierarchy. The request proceeds to request managers until it reaches one whose authorization level matches or exceeds the approval level of the service.

Example:

If a service has an approval level of 40, then a user requesting the service requires *one* of the following criteria:

- The user must have an authorization level of 40.
- The user must obtain approval from a request manager who has an authorization level of 40.

Note: The Requested For user can have different roles - and therefore different authorization levels - in multiple business units. The Catalog system uses the authorization level of that user in the business unit to which the requested *service* belongs.

Administrators create users to let them access CA Service Catalog. Administrators assign a role to each user to specify the access rights of the user.

Follow this process to manage users and roles:

- Step 1 - Manage Users (see page 1410)
- Step 2 - Assign Roles (see page 1413)

Step 1 - Manage Users

This article contains the following topics:

To define the user in CA EEM, use one of the following methods:

- If CA EEM uses an external directory:
  The administrator of the external directory must define the user in the external directory. For more information, see the documentation for the external directory. An example of an external directory is Microsoft Active Directory.
- If CA EEM uses its own repository:
  CA EEM automatically creates a new Global user in the USM/users folder when you add a new CA Service Catalog user. The Create EEM User action on the User Create event rule sets this behavior. Optionally perform one of the following tasks:
  - Disable the action that creates the CA EEM user automatically.
  - Set the format of automatically created passwords (see page 1411).

Administrators create and maintain users to let them access CA Service Catalog. As an administrator, you typically add a user when a new employee starts working in your organization.

Follow these steps

1. Select **Administration**, **Users** from the main menu.
2. Click **Add**.
3. Enter the data for the new user on the Add a New User page (see page 1412), and click OK.

You typically edit a user when an existing employee changes roles or titles or transfers to a new department. You can only edit users who have a role in the business units within the scope of your role.

Important! Do *not* change the user ID of a user. Do *not* reuse deleted user IDs, because all deleted users are maintained as *inactive* in the user database.

Review the Effects of Deleting a User (see page 1413) before you delete a user.

Set the Format of Automatically Created Passwords

You can configure CA EEM to use its own repository. By default, the password is the same as the user ID. You can optionally change the format of the passwords that CA EEM creates automatically.

Follow these steps:

1. Select Administration, Tools, Events.
2. Disable the Create EEM User rule. Create a rule to use in its place, for the User Create event.
3. Disable the associated rule action that is named Create New EEM User or Modify EEM User. Create an action to use in its place.
4. Open your replacement action and locate the Java class field, which appears similar to the following text.

   ```
   com.ca.usm.ruleEngine.action.CreateEiamUserAction,passwordTemplate=valu
   ```

   The passwordTemplate parameter specifies the text to be used as the initial password. The password is set to the user ID that is created when the passwordTemplate parameter is empty.
5. Set this parameter to a specific text value or to an available event variable.

   For example, to set the password to the user ID followed by the letter *a*, specify the following text:

   ```
   com.ca.usm.ruleEngine.action.CreateEiamUserAction,passwordTemplate=$use
   ```

Add a New User Page

You complete several fields when you add a new user in your organization. The following fields require explanation:

> **Note:** If CA EEM is configured to use an external directory, data is auto-populated from the external directory data, if applicable.

- **User ID**
  Specifies the ID by which CA Service Catalog identifies the user.
  The User ID value must be unique.

- **Manager**
  Specifies the manager for the user being creating.
  For system approval process, the manager must approve requests that the user submits. For other approval process, the manager can be a required approver, depending on how you configure the approval process.

- **Request Auto-Delegation: Delegate**
  Specifies the user to whom your requests pending action are delegated automatically when you auto-delegate your own requests pending action. Administrators can also auto-delegate the requests pending action of other users.
  When you clear this field in your own user profile, your requests pending action stop being auto-delegated. The requests remain in your queue. When you clear this field in the profile of another user, the requests pending action of that user stop being auto-delegated. The requests remain in the queue of that user.
  Clearing this field *does not affect* requests pending actions that were already delegated to previously assigned delegates. Therefore, after clearing this field, instruct the former delegates to handle requests pending action promptly. Alternatively, as an administrator, you can also handle them yourself or transfer them to other users.

- **Delegate Use of Catalog: Delegates**
  Specifies the users to whom you delegate the use of your catalog. These users can create and submit requests from your catalog on your behalf. In addition, administrators can delegate the catalog of one user to another user.
  This field is valid only if you or another administrator has enabled delegation of catalogs for your business unit.
  When you clear this field in your user profile, your catalog is no longer delegated. Your former delegates can no longer create and submit requests on your behalf from your catalog. When you clear this field of another user, the catalog of that user is no longer delegated. The former delegates of that user can no longer create and submit requests on behalf of that user from the catalog of that user.

- **User Location**
  Specifies the location details for the user.

  > **Note:** All CA products using the same MDB share the location. Therefore, use caution when modifying the location.

- **Select Business Unit**
  Specifies the business unit (see page 1395) of the new user.
  The default is the business unit that you are currently logged in to.
  Only a Service Delivery Administrator or Super Business Unit administrator can change the business unit of the new user. Otherwise, you *can* create the user but *cannot* change the business unit of the user.
  Users can belong to multiple business units. However, a user can have only one role and one authorization level in each business unit.

- **Select Role**
  Specifies the role (see page 1414) for the new user in the current business unit.
  By default, new users receive the default role for all users (see page 1417). Administrators can optionally assign a different role.
  Select an available role and click the *Add Row* icon to add the role for the user.

- **(Optional) Select Authorization Level**
  Specifies the authorization level (see page 1409) of the new user. This setting applies *only* if you use system approval as the approval process.

Effects of Deleting a User

Deleting a user affects its account, including its subscriptions and requests, as follows:

- **Account**
  The account remains open when you delete the user, because future transactions can exist for an account. As an administrator, you can optionally close the account or leave it open.

- **Subscriptions**
  The status of subscriptions for the deleted user change to the default cancellation status (Pending Cancellation or Cancel).

- **Requests**
  The status of requested service options for the deleted user change as follows:

Original Status	New Status
Not Submitted	None: Request is deleted
Submitted. An Approval status, Fulfillment Status, Pending Resource Assignment or Resource Assigned	Cancelled
Completed	Default Cancellation Status (Pending Cancellation or Cancel) if Accounting Component is installed Cancelled if Accounting Component is not installed
Pending Cancellation or Cancelled	Same as Original Status

Step 2 - Assign Roles

This article contains the following topics:

Relationship Between Users, Roles, and Login

Users, roles, and login have the following relationship:

- A user typically belongs to one business unit, but can optionally belong to multiple business units. A user can have only one role in a business unit.
- A user can optionally have different roles in different business units.
  Example: User A can have a catalog user role in the Finance business unit. The same user can have a catalog administrator role in the IT business unit.
- If the user does not specify a business unit at login, CA Service Catalog logs the user in to the default business unit defined for the user. The user has the role that is assigned to the user in that business unit.
- If an integrating product created the user, then the user is *not* assigned to a role or business unit. Instead, after the user logs in, the user receives the default role for all users (see page 1417). Examples of integrating products include CA Service Desk Manager, CA APM, and CA Business Service Insight.

Roles and Default Access Rights

Users can have one role in each business unit in which they are defined. Users can have different roles in different business units.

- Service Delivery administrators can change some default access rights for the *entire* Catalog system as follows:
  Log in to the root (highest level) business unit, select Administration, Configuration, and change the Access Control configuration settings.
- Service Delivery administrators and business unit administrators can change several default access rights for *specific business units* as follows:
  Log in to the business unit, select Catalog, Configuration, and change the Access Control configuration settings.
- All users can also delegate the use of their catalogs to other users to create requests on their behalf.
- The Catalog system creates only one user at installation time. This user, named *spadmin*, has the Service Delivery Administrator role.

Request-related functionality is available when CA Service Catalog is installed. Subscription and invoice-related functionality is available when Accounting Component is installed.

- **Catalog User**
  Is the user role for requesting services *without* subscriptions. These users can manage their own requests, such as approve, reject, fulfill, and other actions to handle requests pending action.

Most users in the organization use this role *only*.
This role is predefined as the default role for new users. However, administrators can optionally change the default role for new users from the catalog user to another role.
This role is most suitable when you are *not* using subscriptions or billing in your implementation.

- **End User**
  Is the end user for all functions available through the catalog. This user includes all the same access rights as the catalog user. The end user can subscribe to services and view invoices. This role can also view and add news messages, documents, and reports.

- **Request Manager**
  Is the administrator role for managing requests, such as viewing and handling all requests in the business unit and applicable subbusiness units. Request managers handle both their own requests pending action and the requests pending action of other users. Request managers can search *all* requests in the Catalog system. But catalog users can search *only* their own requests.

- **Services Manager**
  Creates, defines, and manages services (not requests) for a specific tenant or business unit. This user also has administrative access to configure reports, dashboards, documents, and message alerts.
  This role is most suitable when you want a user to create and maintain services. This user cannot request or subscribe to services.
  This user can also handle requests pending actions, for example, by approving and rejecting requests.

- **Catalog Administrator**
  Creates, defines, and manages services for a specific tenant or business unit.
  This user also has the same access rights as the request manager role.
  This user can request services but cannot subscribe to them.

- **Super Business Unit Administrator**
  Is the "root" user in a specific super tenant (super business unit). A super business unit is a business unit that contains one or more child business units. This administrator has *almost* complete access to the super business unit and all its sub business units. For example, anywhere in the super business unit, this administrator can create business units, create new users, and assign roles.

- **Service Delivery Administrator**
  Is the "root" (highest level) user in the Service Provider (highest level) business unit. This user has complete system access to all business units. For example, this user can specify default settings that apply to all users by logging in to the root business and accessing the Administration, Configuration, User Default tab. This role is available only for the Service Provider business unit, the default business unit that is created during installation.
  Only this administrator has access to data mediation, system configuration, events, rules, and actions.
  By default, at installation time, the Catalog system creates a user ID named *spadmin* with this role.

- **Default Role Specification**
  Service Delivery administrators can specify a default role for all users (see page 1417).

Tasks that Each Role Can Perform

The roles provide default access rights to various functions. Administrators use configuration settings to add default access rights to a role or remove default access rights from a role.

The following table lists the tasks that each role can perform. The letter **X** indicates that the role *can* perform the task. The dash (**-**) indicates that the user *cannot* perform the task.

	Roles							
Tasks	**Cat U sr**	**Req Mgr**	**Cat Adm**	**End Usr**	**Add m**	**Svc Mgr**	**SB Adm**	**SD Adm**
Shopping								
By default, all users have all shopping functions, except as noted in Roles and Default Access Rights. However, administrators can configure the access rights of each role to create proxy requests, edit requests, and so forth. All users can also delegate the use of their catalogs to create requests on their behalf.	X	X	X	X	X	-	X	X
Managing Requests								
View, edit, delete, and cancel requests	X	X	X	X	X	X	X	X
Act on assigned requests pending action	X	X	X	X	X	X	X	X
Search for requests	X	X	X	X	X	X	X	X
View all items in a request	X	X	X	X	X	X	X	X
View request tracking and audit trail information	-	X	X	-	X	-	X	X
General								
View dashboards	X	X	X	X	X	X	X	X
Add personal dashboards	X	X	X	X	X	X	X	X
Create shared dashboards	-	-	X	-	X	-	X	X
View subscriptions and invoices	-	-	-	X	X	-	X	X
During checkout, change the Requested For user from the current setting to another account or user. That account or user requires a role in the business unit scope of the logged in user.	-	X	X	-	X	-	X	X
View and add News Messages	-	-	-	X	X	X	X	X
View Documents (if enabled) and View Reports	-	-	-	-	-	X	X	X
Managing the Catalog								
View and alter catalog services and service option groups	-	-	X	-	-	X	X	X
View and alter CA Service Catalog configuration settings	-	-	X	-	-	-	X	X
Manage catalog entries or configuration	-	-	-	-	-	X	X	X
Manage subscriptions or invoices	-	-	-	-	X	-	X	X
Managing other elements								

Manage accounts within your business unit scope	-	-	-	-	X	-	X	X
Manage users with roles in your business unit scope	-	-	-	-	X	-	X	X
Manage the dashboard library for the business unit	-	-	-	-	X	-	X	X
Manage scheduled tasks	-	-	-	-	X	-	X	X
Manage reports	-	-	-	-	X	X	X	X
Manage Change Events and Alerts	-	-	-	-	X	-	X	X

Roles Key

Code	Role
Adm	Administrator
Cat Adm	Catalog Administrator
Cat Usr	Catalog User (none)
End Usr	end user
Req Mgr	request manager
Svc Mgr	service manager
SB Adm	Super Business Unit administrator
SD Adm	Service Delivery administrator

Tasks that Each Role Can Perform for Other Users

The following table displays the roles that can perform authorized tasks for themselves and for other accounts and users.

	Roles							
Can Perform Tasks for Themselves and	**Cat Usr**	**Req Mgr**	**Cat Adm**	**End Usr**	**Adm**	**Svc Mgr**	**SBU Adm**	**SD Adm**
Other accounts and users with roles in their business unit	-	X	X	-	X	X	X	X
Other accounts and users with roles in their business unit *and* any of its child business units.	-	X	X	-	-	X	X	X
Other accounts and users with roles in *all* business units, including *all* child business units	-	-	-	-	-	X	-	X

Default Role for All Users

The default role for all users applies to every user in the entire Catalog system. This default role applies to *all* users in *all* business units, including all child business units.

Only the Service Delivery administrators can set this default role. To set the role, the administrator logs in to the *root* business unit and selects Administration, Configuration, User Default Role.

The Catalog system automatically assigns this default role to every new user. However, administrators can optionally specify a different role for a user when they add or edit the user.

Manage Users with CA EEM

CA Service Catalog uses CA EEM to authenticate and authorize users. You can configure CA EEM to use an external directory, such as Microsoft Active Directory, for authentication of users.

Use the CA EEM user interface of CA Service Catalog to manage CA EEM users and groups. Start CA EEM from the Users option of the Administration Quick Start dashboard.

Integrating with embedded CA EEM and optionally with an external directory is the only required integration for CA Service Catalog. You use CA EEM and optionally an external directory to manage the CA Service Catalog user database.

After you have installed CA Service Catalog, its required components (including embedded CA EEM), and your external directory (if used), perform the following actions:

1. Import Users into the Database (see page 1418)
2. (Optional) Create User-Defined Groups (see page 1427)
3. (Optional) Update the host name of the CA EEM computer or the application names it uses. Perform this step periodically after CA Service Catalog has been installed and is running.
4. (Optional) Add High Availability and Failover Support as follows:
    a. Verify that you have installed CA EEM on at least two computers in your CA Service Catalog implementation.
    b. Set up high availability and failover support for CA EEM.

Note: For more information, see Configuring Failover (https://wiki.ca.com/display/CAEEM/Failover+Configuration).

    c. Run the setup utility and configure CA EEM.

Note: If you have installed other CA products that use CA EEM, see the documentation for each of those products for information about setting up failover support for CA EEM.

Step 1 - Import Users into the Database

After you install CA Service Catalog, the user database contains no data. To populate the database with user information, configure and run the LDAP utility. Running the utility populates your CA Service Catalog database with the users that you specify from your LDAP server. Run the utility at regular intervals to synchronize updates in the user database from the LDAP server to the CA Service Catalog database. You can optionally use a scheduler to synchronize.

Follow these steps:

Step 1a - Perform Transition Tasks

These tasks apply if you were previously using the CA EEM synchronization utility (syncuputil) to import and synchronize users in the CA Service Catalog user database. Examples include implementations that obtained the LDAP Importer utility by upgrading CA Service Catalog or applying a patch.

These tasks help you transition efficiently from the CA EEM synchronization utility to the LDAP Importer utility.

- Stop using the CA EEM synchronization utility and its properties file (syncuputil.properties).
- Remove scheduled tasks for that utility.
- Run the LDAP Importer utility.

These tasks do *not* apply to first-time installations of CA Service Catalog.

Step 1b - Configure CA EEM to Use an External Directory

Configuring CA EEM to use an external directory is a prerequisite for using the LDAP Importer utility.

Follow these steps:

1. Verify that the external directory contains at least one user ID that matches the user ID of a Service Delivery Administrator in CA Service Catalog:

   a. Log in to CA Service Catalog as the spadmin user and create at least one user ID with the Service Delivery Administrator role.
   This user ID must match a user name in the external directory.

   b. If CA EEM is configured for multiple active directories, create a user ID as Domain Name\userid in CA Service Catalog. Verify that the domain name is part of the principal name of the CA EEM user ID in the CA EEM active directory.

2. Configure the User Store in CA EEM to reference all applicable Active Directory sources.

Note: For more information, see your CA EEM documentation.

3. (For single sign-on) Verify that the domain name for Active Directory matches the domain name of the single sign-on user.
4. Select Manage Identities, Users, and validate that the users returned from a search are from the external directory. If your user base is large, limit the list of users returned.
5. Restart the CA Service Catalog service.
6. Log in to CA Service Catalog as the Service Delivery Administrator whose user name matches a user name in the external directory.

You have configured CA EEM to use an external directory.

Step 1c - (Optional) Determine the Number and Purpose of Configuration Files

If you are using multiple domains, you can use multiple configuration files. In that case, determine the number of configuration files and the purpose of each one. For example, large organizations can use several LDAP servers, one for each business unit, region, or domain. A managed service provider can use one group of LDAP servers for their internal organization and another group for their client organizations.

In such cases, as an administrator, you can use a unique configuration file for each server. You can configure the name and settings of each file to match its purpose. For example, consider a Managed Service Provider (MSP) with three internal LDAP servers and many LDAP servers for their clients. The MSP can decide to copy and customize the default file (LDAPImporter_server1.properties) as follows:

- Internal configuration files
  - LDAPImporter_Internal_Asia.properties
  - LDAPImporter_Internal_Europe.properties
  - LDAPImporter_Internal_NorthAmerica.properties
- Configuration files for clients that are retail companies in Asia.
  - LDAPImporter_Client_Azerbaijan_Retail.properties
  - LDAPImporter_Client_India_Retail.properties
  - LDAPImporter_Client_Singapore_Retail.properties

Note: Clustering alone does *not* require extra configuration files. If CA Service Catalog is clustered, verify that the properties file is available from the computers from which you run the utility.

Step 1d - Create the LDAP User

The LDAP Importer utility requires an LDAP user to connect to the LDAP server and import the LDAP users into the CA Service Catalog database. You specify the login credentials of the LDAP user in the configuration file properties (see page) for the utility.

Note: For more information about how to create LDAP users, see your LDAP documentation.

Step 1e - Create the CA Service Catalog User

To import users from the LDAP server to CA Service Catalog, the LDAP Importer requires a CA Service Catalog user. You create a CA Service Catalog user for this purpose and specify its login credentials in the configuration file properties (see page) for the utility.

Note: If an existing user meets the following specifications, you can use that user.

Follow these steps:

1. Log in to the *root* business unit.

   Important! Creating this user in the root business unit is required for the proper role assignment and access rights.

2. Select Administration, Users from the main menu.
3. Click Add.
4. Enter the data for the new user, as follows:

   - **User Name**
     Specify the same user name, including case, as the LDAP user that you use to connect to the LDAP server.
     If your catalog works with multiple LDAP servers, include the domain name, for example, MyDomain\MyUser.
   - **Role**
     Service Delivery Administrator.

The user is added.

Step 1f - Specify the Configuration File Properties

Replace the default properties in the file with your custom values. See the comments in the file for assistance.

The default configuration file is named LDAPImporter_server1.properties. This file resides in the USM_HOME folder. Copy and modify it to create all the custom configuration files that you require for your organization.

Important! The configuration file includes placeholder values that you *must* customize before running the utility.

Format

Properties in the configuration file follow this format: *name*=*value*. For example, LDAP. LastSynchronizationDate=2013-12-13.

Names *must not* contain spaces. If a name contains one or more spaces, replace each space with an underscore (_).

Values *can* contain spaces and you do not need to replace spaces with underscores.

You do not need to enclose spaces or underscores in quotation marks.

LDAP Properties

- **LDAP.Base.Provider.Url=*value***
  Specifies the URL of the LDAP server. If the LDAP server is *not* using SSL, use this format: LDAP.Base.Provider.Url= ldap://LDAP-server-name:389
  If the LDAP server *is using* SSL, use this format: LDAP.Base.Provider.Url=ldaps://*LDAP-server-name* :636
  If the LDAP server or CA Service Catalog uses SSL, complete the SSL parameters.

- **LDAP.User.DN=*value* and LDAP.User.Domain=*domain-name***
  Specify the name of the LDAP user that you created earlier (see page) for accessing the LDAP database.
  The domain name is required if CA EEM is configured to use multiple domains.
  If you are using multiple LDAP servers, the domain name must match the domain name for the LDAP server in CA EEM.

- **Catalog.User=*domain-name**username***
  Specifies the name of the CA Service Catalog user that you created earlier (see page) for importing the users from the LDAP server into the CA Service Catalog database.
  The domain name is required if CA EEM is configured to use multiple domains.

- **LDAP.User.Password=*password* and Catalog.User.Password=*password***
  Specify the encrypted passwords for each user in the appropriate parameter.
  To generate each encrypted password, enter the following command at the CA Service Catalog command prompt:

```
USM_HOME/SCRIPTS ENCRYPTER.BAT password
```

Copy each encrypted value from the command line and paste it to the appropriate entry in the configuration file.

- **InsertOrUpdateUsersAfterLastSyncDateOnly=True|False**
  We recommend that you specify True. *S*pecify True if you plan to run the utility regularly with a scheduling tool. This setting helps run the synchronization process in optimized mode.
  Alternatively, specify False if you do *not* plan to run the utility regularly with a scheduling tool.

- **LDAP.LastSynchronizationDate=*yyyy-mm-dd***
  This parameter is required if you specify True for the previous parameter, InsertOrUpdateUsersAfterLastSyncDateOnly.
  We recommend that you specify this parameter when you run the file for the first time. Afterwards, this parameter is updated automatically whenever you run the utility with a scheduling tool.
  Specifying this parameter provides more efficient processing. If you use this parameter, the utility imports *only* users that were added or updated since the last time the utility ran. The utility processes deleted users according to your specifications for the next parameter, DeactivateMDBUsersUponLDAPUserDeletion.

Catalog Properties

- **DeactivateMDBUsersUponLDAPUserDeletion=True|False**
  Specifies how to process CA Service Catalog users that were deleted from the LDAP database:

  - **True**
    (Recommended) *D*eactivates these users in the CA Service Catalog database. The user IDs are no longer available in the CA Service Catalog UI.

  - **False**
    Keeps these deleted users active in the CA Service Catalog database and UI.

  In either case, these deleted users cannot log in to CA Service Catalog, because they cannot be authenticated in the LDAP database.
  This setting does not apply the *first* time that you run the utility.

- CatalogUser.Country.*xx*=*country*

  - ***xx***
    Specifies the two-letter country code from the LDAP server.

  - ***country***
    Specifies the country name from the MDB.
    To obtain country names from the MDB, query the ca_country table.

    Note: If the LDAP server does not specify the country code, then the country name is set to NULL in the MDB.

  Examples:

- CatalogUser.Country.IN=India
- CatalogUser.Country.US=United States

- **CatalogUser.*country*.*city*=*location***
  Specifies a custom location name.

  - ***country***
    Specifies the country name from the MDB, as explained in the previous entry.

  - ***city***
    Specifies the city name from the LDAP server.

    Note: If the LDAP server does not specify the city, then the city is set to NULL in the MDB. If the LDAP server does specify the city, but the city is not mapped in this parameter, then the city is set to NULL in the MDB.

  - ***location***
    Specifies any custom location name relevant to your organization, for example, the name of a branch or unit in the *city*.
    If the location does not exist in the MDB, it is created.

    Note: As a best practice, specify a location name that is known to other administrators in your organization. This location and all other user attributes appear when you view user attributes in the CA Service Catalog UI.

  Examples:

  - CatalogUser.United_States.Islandia=UnitedStates1
  - CatalogUser.United_States.New_York=UnitedStates2

- **CatalogUser.DefaultBusinessUnit=*business-unit***
  Specifies the CA Service Catalog business unit to which users are assigned when they are imported for the first time.
  Once the users are imported for the first time, their business unit assignment is the same. Only when you use the CA Service Catalog UI to change the business unit, does this value also change. This restriction applies even if you change the value of this parameter and import the users again. This restriction helps maintain the ability of users to log in to CA Service Catalog.

- **CatalogUser.DefaultRole=*role***
  Specifies the CA Service Catalog role that users are assigned when they are imported for the first time.
  Once the users are imported for the first time, their role assignment is the same. Only when you use the CA Service Catalog UI to change the role assignment, does this value also change. This restriction applies even if you change the value of this parameter and import the users again. This restriction helps maintain the ability of users to log in to CA Service Catalog.
  The following table lists the valid role names for the CatalogUser.DefaultRole parameter, according to the type of business unit.

Role	Root BU	*Node BU	**Leaf BU
spadministrator (Service Delivery Administrator)	x		
servicemanager (Service Manager)	x		
catadministrator (Catalog Administrator)	x	x	
stadministrator (Super Business Unit Administrator)		x	
administrator (Administrator)	x	x	x
requestmanager (Request Manager)	x	x	x
catalogenduser (Catalog User)	x	x	x
enduser (End User)	x	x	x

*A Node BU is a child business unit that contains one or more of its own child business units.

**A Leaf BU is a child business unit that contains no child business units of its own.

- **SSL.KeyStoreLocation=*value***
  Specifies the complete path name of the keystore file that contains the SSL Server certificates of CA Service Catalog and the LDAP server. This parameter is required if CA Service Catalog or the LDAP server use SSL. If the LDAP server uses SSL, configure the LDAP.Base.Provider.Url parameter to use SSL.
  Delimit folder names with double backslashes (\\). The standard path name follows:

```
C:\\Program_Files\\CA\\Service_Catalog\\ssl.keystore
```

Important! Verify that you have imported the complete chain of Certification Authority (CA) certificates for CA Service Catalog and the LDAP server into the Java keystore.

- **SSL.KeyStorePassword=*value***
  Specifies the encrypted password for the CA Service Catalog keystore file.
  To generate the encrypted password, enter the following command at the CA Service Catalog command prompt:

```
USM_HOME/SCRIPTS ENCRYPTER.BAT password
```

Copy the encrypted value from the command line and paste it to this entry.

Step 19 - Run the Utility

Run the LDAP Importer utility regularly to import users from the LDAP server into the CA Service Catalog database. As a CA Service Catalog administrator, determine how often you must run this utility. For example, large organizations or organizations with frequent personnel changes want to run the utility daily. However, other organizations with fewer personnel changes want to run the utility weekly or every two weeks.

The file name of the utility is LDAPImporter.bat. The file resides in the USM_HOME\scripts folder.

You can optionally use *any* of the following methods to run the utility regularly:

- Run the utility manually from the command line of any CA Service Catalog computer.
- Run the utility as a batch job at scheduled times. Use the CA Service Catalog Scheduler or any standard scheduler, such as Windows Scheduler.
  To access the CA Service Catalog Scheduler, click Administration, Tools, Scheduler. Use the following specifications when you complete the fields:
  For Action Type, select Execute Command Line.
  For Cmd Line, enter the path names of the utility and the configuration file or files. The Cmd Line field accepts a limited number of characters. If necessary, specify relative path names (from USM_HOME\view\bin) or specify folder names only, as shown in the following examples:

```
..\..\scripts\LDAPImporter.bat ..\..\scheduler.properties

..\..\scripts\LDAPImporter.bat C:\LDAPFolder\
```

Note: For more information about the CA Service Catalog Scheduler, see the Manage the Scheduler (see page 3068) section. For more information about the Windows Scheduler, see your Windows documentation.

To run the LDAP Importer utility, enter the following command at the command prompt or in a scheduling tool:

```
LDAPImporter.bat properties-files
```

The utility processes all levels of nested groups of users. The utility imports each user and the users *above* it in organizational hierarchy, up to the top, even if the manager is not part of that group.

The utility does *not* import the users *below* the user in organizational hierarchy. For example, the utility does not import the direct reports of the user.

Logging

The log file for the utility is named LDAPImporter.log. This file resides in the USM_HOME\logs\LDAPImporter folder.

The level of logging for the utility is specified in the LDAPImporter.log4j.xml file. This file resides in the USM_HOME\scripts folder.

Examples

Examples of Running Configuration Files:

In this example, you run multiple configuration files in the USM_HOME folder:

```
LDAPImporter.bat USM_HOME\LDAPImporter_server1.properties
USM_HOME\LDAPImporter_server2.properties USM_HOME\LDAPImporter_server3.properties
```

In this example, you store all LDAP server properties in the MyFolder folder. Each LDAP server properties file name within this folder must use this format: ldapimporter_*name*.properties.

```
LDAPImporter.bat USM_HOME\MyFolder
```

Examples of Specifying Configuration File Properties

In this example, you populate the root business unit (ca.com) with users whose location is New York and who have direct reports. Assign the Service Delivery Administrator role to these users.

```
LDAP.ImportType=User
LDAP.MicrosoftAD.User.Filter = (&(objectClass=user)(!(objectClass=computer)))
LDAP.User.Filter= (&(l=New York)(directReports=*))
CatalogUser.DefaultBusinessUnit=ca.com
CatalogUser.DefaultRole= spadministrator
```

In this example, you populate the business unit that is named Europe with users who belong to the group named All Managers Europe. Assign the Super Business Unit Administrator role to these users.

```
LDAP.ImportType=Group
LDAP.Group.Name = All Managers Europe
CatalogUser.DefaultBusinessUnit=Europe
CatalogUser.DefaultRole= stadministrator
```

Step 1h - Verify the Import

Verify that the database has been populated correctly by logging in to CA Service Catalog as a user-defined in the database. A successful login indicates that the database was populated correctly.

Step 2 - (Optional) Create User-Defined Groups

Create user-defined groups in CA EEM to apply the same action to many CA Service Catalog users at once. Once you create the UDG in CA EEM, it is available in CA Service Catalog. You can then administer the UDG much like you would administer an individual user.

When you set the permissions for the UDG, those settings are applied to all individual users in the group. For example, you want to assign read-write access to a service to a group and read-only access to the service to another group. Use UDGs, to group users according to their function and purpose.

As an administrator, you can optionally assign users to one or more UDGs. The product does not require that users belong to any UDG. User who belongs to multiple UDGs have access to all resources authorized by their UDG memberships. If any UDG membership provides a user with access to a resource, then the user is granted access to that resource, regardless of whether other UDGs also grant access to the resource.

You can create and maintain user-defined groups (UDGs) in either CA EEM or your external directory (if applicable). You cannot create and maintain UDGs in CA Service Catalog directly.

Follow these steps:

Note: If the following steps do not match your version of CA EEM, see your CA EEM documentation for more information about assigning users to user groups in CA EEM.

1. Log in to the Service Delivery application of CA EEM. Do *not* log in to the global application of CA EEM.
2. Click Manage Identities, Groups.
3. Click Show Application Groups and click Go, in the Search Groups box on the left side of the screen.
4. Locate the Application Groups folder, in that tree; this folder contains the CA Service Catalog user groups, including the UDGs.
5. Find and click the "people" icon.
6. Enter the name and description for the new group in the fields provided.
7. Click Save to save your changes.

An important administrative task of user-defined groups (UDGs) is assigning rights to the following CA Service Catalog objects:

- Reports, including the data, data view, and layout objects
- Services, service options, and service option groups, including rights to edit, request, and subscribe to these elements.
- Documents
- Dashboards

An administrator can set permissions to a specific object (such as a service) according to the role of a user. The administrator can also set permissions to that object according to UDG.

For example, open a service in CA Service Catalog. Click Permissions, and search for a UDG or all users with a specific role. Next, you can assign rights to the service for the users and groups that are returned in the search results.

Note: When you search for UDGs, CA Service Catalog searches its own portions of CA EEM.

If a user has *either* a role or a group membership for which a permission has been set, the user is granted that permission. If a user has *both* a role and a group membership for which a permission has been set, the user is granted that permission.

You can optionally view the profile of an individual user who is a member of the UDG. While this step is not practical for verification on a large scale, it is helpful for spot checks.

You can assign rights to user-defined groups. By doing so, you ensure that all members of the group are assigned the same rights in a single operation.

Follow these steps:

1. Open the Set Permissions dialog for the Catalog object (such as a service) and click Groups.
2. Click Search EEM Groups.
3. Search for the group.
4. Click the group name in the search results.
   The dialog displays a new EEM Group list below the search results. The new list includes the group name that you clicked. The adjacent columns show the rights of the group to the object.
5. Select or unselect the options in the columns to grant or remove rights for the group to the object.

You have assigned right to the user-defined groups.

Enable External Authentication of Users

This article contains the following topics:

By default, CA Service Catalog uses CA EEM to authenticate users. You can configure CA Service Catalog to authenticate users with external applications such as CA SiteMinder, IBM Tivoli, and others. The process consists of the following tasks:

1. Install and implement the external authentication application, according to its documentation.
2. Review the following examples and understand how these applications typically send user authentication to CA Service Catalog. If applicable, adjust your settings to match these examples.
   - CA SiteMinder sends user identity information (authenticated user) with sm-user artifact name in the request header.
   - IBM Tivoli sends user identity information with iv_user artifact name in the request header.
   - Microsoft Internet Information Server (IIS) sends user identity information with request when configured for Windows NTLM.
   - Apache sends user identity information with request when configured for Windows NTLM.
3. Test the configuration on both CA Service Catalog and the external authentication application.
4. Verify that CA Service Catalog successfully receives and processes the authenticated users that the external authentication application passes. If necessary, adjust the parameters on both systems as needed.
5. Optionally configure Single Sign-On for the authentication method that you are using:

- Windows NTLM authentication (see page 1430)
- External authentication (see page 1432)

Configure Single Sign-on Using Windows NTLM Authentication

When you use Windows NTLM authentication, you can perform this procedure to enable Single Sign-On for CA Service Catalog. Users log in to the Windows domain, they can access CA Service Catalog without logging in to it.

Follow these steps:

1. Verify that you are *not* planning to use clustering. If you are using clustering, instead of performing this procedure, you set up NTLM authentication for each cluster.
2. Verify that your environment meets the following requirements:
   - You are using Windows domain authentication.
   - CA Service Catalog and CA EEM are installed in the same Windows domain.
   - You have configured CA EEM to use Active Directory.
     You are running a version of HTTP *higher* than 1.0.
   - If you are using Windows Server, perform one of the following tasks to use single sign-on using NTLM:
     - Use HTTP instead of HTTPS.
     - Uninstall the Internet Explorer Enhanced Security Configuration Windows Component.
   - If both of the following conditions exist, you cannot use single sign-on using NTLM with HTTPS:
     - The client computer operating system is Windows Server.
     - The Internet Explorer Enhanced Security Configuration Windows Component is installed.
3. Perform the following actions:
   a. Click **Administration**, **Configuration**, **Single Sign On Authentication**.
   b. Locate the **Single Sign On Type** and click the Modify icon.
   c. Select the option **NTLM (NT LAN Manager)** and click **Update Configuration**.
      The dialog closes, and you return to the Single Sign On Authentication page.
4. Verify that all affected users can use single sign-on to access CA Service Catalog on this computer.

You have configured NTLM Authentication.

Implement Single Sign-on for One Group of Users and Manual Login for Another Group

In this use case, you want to enable single Sign-on for one group of users. For example, internal users (Group 1) You also want to force manual login for another group of users. For example, external users such as contractors, vendors, and customers (Group 2).

Follow these steps:

1. Verify that you have two CA Service Catalog computers using the same instances of the MDB and CA EEM. This procedure calls the CA Service Catalog computers *Server 1* and *Server 2*.

2. Verify the following requirements:

   - Group 1 users log in to Server 1 *only*.
   - Group 2 users log in to Server 2 *only*.
   - If necessary, notify users in each group of this requirement.

3. On Server 2, edit the USM_HOME\webapps\usm\WEB-INF\web.xml file. Comment the following lines:

```
<!--
    <filter>
      <filter-name>NtlmAuthFilter</filter-name>
      <filter-class>com.ca.usm.httpfilter.NtlmAuthenticationFilter</filter-
class>
      <init-param>
        <param-name>debug</param-name>
        <param-value>false</param-value>
      </init-param>
    </filter>
-->
 <!--
   <filter-mapping> <filter-name>NtlmAuthFilter</filter-name> <url-pattern>*.
rpc</url-pattern> </filter-mapping>
    <filter-mapping> <filter-name>NtlmAuthFilter</filter-name> <url-pattern>/wpf
/*</url-pattern> </filter-mapping>
    <filter-mapping> <filter-name>NtlmAuthFilter</filter-name> <url-pattern>
/uslm/*</url-pattern> </filter-mapping>
    <filter-mapping> <filter-name>NtlmAuthFilter</filter-name> <url-pattern>
/assure/*</url-pattern> </filter-mapping>
    <filter-mapping> <filter-name>NtlmAuthFilter</filter-name> <url-pattern>
/documents/*</url-pattern> </filter-mapping>
    <filter-mapping> <filter-name>NtlmAuthFilter</filter-name> <url-pattern>
/FileStore/*</url-pattern> </filter-mapping>
-->
```

   Commenting these lines deactivates SSO functionality from this CA Service Catalog computer.

4. Restart CA Service Catalog.

Configure Single Sign-on Using External Authentication

When you use external authentication, you can perform this procedure to enable Single Sign-On for CA Service Catalog. Users who are set up in your external authentication system can access CA Service Catalog without logging in to it.

Follow these steps:

1. Verify that CA Service Catalog and CA EEM are installed in the same Windows domain.
2. Log in to CA Service Catalog running on this computer.
3. Perform the following actions:
    a. Click **Administration**, **Configuration**, **Single Sign On Authentication**.
    b. Locate the property **Single Sign On Type** and click the Modify icon.
    c. Select the option **Artifact Based Single Sign On** and click **Update Configuration**. The dialog closes, and you return to the Single Sign On Authentication page.
4. Verify that all affected users can use single sign-on to access CA Service Catalog on this computer.

You have configured external authentication other than Windows NTLM.

Configure CA Service Catalog to Use Secure Socket Layer

You can optionally configure CA Service Catalog to use Secure Socket Layer (SSL). SSL establishes an encrypted link between a server and a client. For example, a web server and a browser; or a mail server and a mail client. This link helps ensure that all data passed between the server and client remain private and integral. When you configure a product to use SSL, you change its communication method from HTTP to HTTPS.

Follow these steps:

1. Create a keystore file (see page 1433).
2. Use a single keystore for all integrated products. This approach is recommended.
   If you have multiple keystores for different products and cannot use a single keystore for all of them, you can merge keystore files (see page 1433).
3. Configure CA Service Catalog.
4. If you are integrating CA Service Catalog with CA Process Automation, perform the following steps:
    a. Configure CA Process Automation to use Secure Socket Layer. For more information, see your CA Process Automation documentation.

b. Configure CA Process Automation to communicate with CA Service Catalog using Secure Socket Layer (see page 1436)

5. If you are integrating CA Service Catalog with CA Business Intelligence, perform the following steps:

   a. Configure CA Business Intelligence to use Secure Socket Layer. For more information, see your CA Business Intelligence documentation.

   b. Configure CA Business Intelligence to communicate with CA Service Catalog using Secure Socket Layer. (see page)

6. (Optional) Add self-signed certificates to the keystore (see page 1438)

Step 1 - Create a Keystore File

A keystore file is required to enable SSL. Create a keystore file if you do not have one already for another CA product that integrates with CA Service Catalog. You can use a keystore file for a single product or for multiple products. If you must create individual keystores for each product, you can optionally merge your keystore files (see page 1433).

Follow these steps:

1. Open a command window on the Catalog Component server.

2. Enter the following command:

   ```
   keytool -genkey -alias alias_name -keyalg RSA -keystore "USM_HOME\.keys
   ```

   alias_name
   Specifies the logical name for the certificate that you are using for CA Service Catalog and possibly for other products. Record this alias name for reference.

3. Enter the password at the “Enter keystore password” prompt. To make configuring Tomcat easier, you can use “changeit” as the password.

4. Record your password for reference.

5. Enter your password at the prompt.

You have created the keystore file.

Step 2 - (Optional) Merge Keystore Files

A keystore file is required to enable SSL. If you are using SSL for two or more products and have two or more keystore files, use a single keystore for all integrated products. However, if you have multiple keystores for different products and cannot use a single keystore for them all, you can merge the contents of the individual keystore files.

Follow these steps:

1. Copy all keystore files to the USM_HOME folder. For example, any keystore files for CA Process Automation, CA CMDB, or other products that integrate with CA Service Catalog.

2. Find and record all required keystore files, keystore aliases, and keystore passwords for the products of interest. For example, for CA Process Automation, you can retrieve the c2okeystore password from KEYSTOREID property of the OasisConfig.properties file.

3. Restart Catalog Component.

4. Enter the keytool command to merge the keystore of the first product, using the following command as a model:

   ```
   keytool -importkeystore -srckeystore "product1_keystore" -destkeystore
   "USM_HOME\.keystore" -srcalias product1_alias -destalias alias_name-srckeypass
   "product1_password" -destkeypass "changeit"
   ```

   - **"*product1_keystore*"**
     Specifies the name of keystore file (including the complete path name) for the product you are merging.

   - ***product1_alias***
     Specifies the keystore alias for the product you are merging.

   - ***product1_password***
     Specifies the keystore password for the product you are merging.

   - ***alias_name***
     Specifies the *alias_name* that you specified when you created a keystore file for CA Service Catalog.

   The following command merges the contents of the CA Process Automation keystore (c2okeystore) into the CA Service Catalog keystore:

   ```
   keytool -importkeystore -srckeystore "%ITPAM_HOME%\server\c2o\.
   config\c2okeystore" -destkeystore "USM_HOME\.keystore" -srcalias c2o-j -
   destalias tomcat -srckeypass "475ba811-62cd-4ec8-b757-cd7710de3fa8" -
   destkeypass "changeit"
   ```

   The following command merges the contents of the CA CMDB keystore (.cmdb_keystore) into the CA Service Catalog keystore:

   ```
   keytool -importkeystore -srckeystore ".cmbd_keystore" -destkeystore
   "USM_HOME\.keystore" -srcalias cmdb -destalias tomcat
   -srckeypass "changeit" -destkeypass "changeit"
   ```

5. Respond No when you are prompted to overwrite the source alias.

6. Repeat the previous two steps for each product whose keystores you are merging.

7. Verify if all the certificates that you want are in one keystore, using the following command:

   ```
   keytool -list -keystore "USM_HOME\.keystore"
   ```

   This command lists the contents of the merged keystore.

You have merged keystore files.

Step 3 - Configure CA Service Catalog to Use Secure Socket Layer

Configure CA Service Catalog to use Secure Socket Layer (SSL).

Follow these steps:

1. Edit the server.xml file to support SSL (see page 1435).
   The file is updated to help support SSL for CA Service Catalog.
2. Open the USM_HOME\view\conf\viewService.conf file, using a text editor.
3. Update the following line with the path name and file name of the keystore file:

   ```
   wrapper.java.additional.number=-Djavax.net.ssl.trustStore="USM_HOME/.key
   ```
4. Update the following line with the password of the keystore file:

   ```
   wrapper.java.additional.number=-Djavax.net.ssl.trustPass=changeit
   ```
5. Save and close the viewService.conf file.
6. Select Administration, Configuration, Server Information on the CA Service Catalog GUI.
7. Complete the fields in this section as follows:
   For Host Name, specify the name of the host where CA Service Catalog is installed.
   For Port Number, specify the port where HTTPS is configured.
   For Enable HTTPS, specify Yes. Restart CA Service Catalog.
8. Log in to CA Service Catalog using the following URL:
   https://hostname:port/usm/wpf
9. You see a trusted certificate prompt, which indicates that you are using HTTPS.
10. Optionally, disable HTTP access by commenting the section for the HTTP connector, as shown in the following example:

```
<!--
<Connector port="8080" enableLookups="false" redirectPort="8443"
tomcatAuthentication="false"
      maxThreads="400" minSpareThreads="25" maxSpareThreads="100" debug="0"
connectionTimeout="15000"
      disableUploadTimeout="true" compression="on" compressionMinSize="2048"
      compressableMimeType="text/html,text/plain,text/xml,text/css,text/javascript,
image/png,image/gif,image/jpeg,application/json"
      useBodyEncodingForURI="false" URIEncoding="UTF-8" />
-->
```

You have configured CA Service Catalog to use SSL.

Edit the Server.xml File to Support SSL

As part of configuring CA Service Catalog to use Secure Socket Layer (SSL), edit the server.xml file to support SSL.

Follow these steps:

1. Open the USM_HOME\view\conf\server.xml file.

2. Search for the following section. Enable the commented section by removing "<!--" and "-->" from the first and last lines, as shown in the following example:

```
 <!--
    <Connector port="8443" enableLookups="false" tomcatAuthentication="false"
maxHttpHeaderSize="8192"
      maxThreads="400" minSpareThreads="25" maxSpareThreads="100" debug="0"
connectionTimeout="15000"
      disableUploadTimeout="true" compression="on" compressionMinSize="2048"
      compressableMimeType="text/html,text/plain,text/xml,text/css,text
/javascript,image/png,image/gif,image/jpeg,application/json"
      scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
SSLEnabled="true"
      keystoreFile="__USMHOME__\.keystore" keyAlias="alias_name" keystorePass="
changeit"/>
    -->
```

   - ***alias name***
     Specifies the logical name for the certificate that you are using for CA Service Catalog and possibly for other products.

3. Update the default port (8444) to another secure socket layer port, if necessary.

4. Verify whether either or both of the following conditions exist:

   - You are using an existing keystore.
   - You have changed either the CA Service Catalog installation path or generated keystore name.

5. Perform the following actions, if either or both of the conditions in the previous step exist:

   - Update the keystoreFile parameter with the correct path and file name, typically USM_HOME\.keystore.
   - Update the keyAlias parameter with the *alias_name* that you specified when you created a keystore file (see page 1433) for CA Service Catalog.

6. Save and close the server.xml file.

You have edited the server.xml file. You can continue configuring CA Service Catalog (see page 1435) to use Secure Socket Layer (SSL).

Step 4 - (Optional) Configure CA Process Automation to Communicate with CA Service Catalog Using Secure Socket Layer

Configure CA Process Automation to communicate with CA Service Catalog using SSL.

Follow these steps:

1. On the CA Service Catalog GUI, select Administration, Configuration, CA Process Automation.

2. Complete the fields in this section as follows:
   For Host Name, specify the name of the host where CA Process Automation is installed.
   For Port Number, specify the CA Process Automation port where HTTPS is configured.
   For Enable HTTPS, specify Yes.

3. Recycle Catalog Component.

4. Click Test.
   The connection is tested, using the new values that you specified.
   If the connection fails, try using a different value.

5. Click Configure.
   The CA Process Automation configuration details are updated with the new values that you specified.

6. Perform this step if you are using content packs. Otherwise, you can skip this step.
   Edit the USM_HOME\build.xml file, and verify that the following parameters are correct. Update them, if applicable.

   - The file name and path name of the keystore
     For example, if the keystore is located in USM_HOME and the keystore file name is. mykeystore, update this line as follows:

     ```
     <sysproperty key="javax.net.ssl.trustStore" value="${env.USM_HOME}/.mykeystore" />
     ```

   - The keystore password
     For example, if the keystore password is mykeystorepw, update this line as follows:

     ```
     <sysproperty key="javax.net.ssl.trustPass" value="mykeystorepw" />
     ```

You have configured CA Process Automation to communicate with CA Service Catalog using SSL.

Step 5 - (Optional) Configure CA Business Intelligence to Communicate with CA Service Catalog Using Secure Socket Layer

As part of configuring CA Service Catalog to use Secure Socket Layer (SSL), you configure BusinessObjects Enterprise to communicate with CA Service Catalog using SSL.

Follow these steps:

1. Select Administration, Configuration, CA Business Intelligence, on the CA Service Catalog GUI.

2. Complete the fields in this section as follows:
   For Host Name, specify the computer name on which the Business Intelligence Launch Pad component of CA Business Intelligence is hosted.
   For Port Number, specify the port number on which CA Business Intelligence is running.
   For Enable HTTPS, specify Yes.

3. Recycle Catalog Component.

4. Click Launch.

5. The connection is tested, using the new values that you specified. If the connection fails, try using a different value.
   The BusinessObjects Enterprise configuration details are updated with the new values that you specified.

Step 6 - Add Self-Signed Certificates to the Keystore

When you use self-signed certificates for any computer that connects directly to CA Service Catalog or that CA Service Catalog connects to, add these certificates to the keystore. For example, suppose that you are using clustering with load balancing for CA Service Catalog. In that case, if you are using a self-signed certificate for the load balancing computer, add them to the keystore.

Note: If you are using trusted certificates for these computers, you do not need to add them to the keystore.

Follow these steps:

1. Verify the computer to be trusted, that is, the computer that has direct connection with CA Service Catalog.
   For example, suppose that you integrate CA Service Catalog with CA Service Desk Manager through a load balancing computer. In that case, CA Service Catalog connects directly to the load balancer (not CA Service Desk Manager). Therefore, the computer to be trusted is the load balancer (not the CA Service Desk Manager computer).

2. Go to a Catalog Component computer. Download the DER encoded binary X.509 file (the certificate) for the computer to be trusted.
   For example, use your web browser to visit the computer and obtain the certificate.

3. Open the CA Service Catalog command prompt and enter the following command:

   ```
   keytool -importcert -alias aliasname -file pathname-to-certificate -keystore
   USM_HOME\.keystore
   ```

   - ***alias_name***
     Specifies the logical name for the certificate that you are using for CA Service Catalog and possibly for other products.

   - ***pathname-to-certificate***
     Specifies the complete path name to the certificate file that you downloaded in the previous step.

   You are prompted to enter a password.

4. Perform one of the following actions:

   - Enter changeit as the keystore password.

   - Enter a different keystore password.

The password is saved.

5. Complete this step if you entered a different password than changeit in the previous step. Otherwise, skip this step.

    a. Open the viewService.conf file for editing.

    b. Find the line that contains the following phrase:

    ```
    -Djavax.net.ssl.trustPass=keystore-password
    ```

    a. Update the keystore-password to match the new password that you specified in the previous step.

    The viewService.conf file is updated with the new password.

6. Remain at this Catalog Component computer. Repeat the previous steps for every computer to be trusted which has self-signed certificates.
   The keystore file is updated with the new self-signed certificates from each applicable computer to be trusted.

7. Perform the following actions on of every other Catalog Component computer:

    a. Update the viewService.conf file to use a password other than *changeit*, if applicable.

    b. Copy the updated keystore file from this Catalog Component computer to all the remaining Catalog Component computers.

You have added self-signed certificates to the keystore.

Reconfigure the CA Service Catalog Computer using the Setup Utility

Run the CA Service Catalog setup utility to set up your database, reconfigure CA EEM, and reconfigure the product components. The product components are Catalog Component, Catalog Content, and Service Accounting Component.

Important! Run the CA Service Catalog setup utility on all CA Service Catalog computers in the correct sequence, as explained in this topic.

Follow these steps:

1. Run the setup utility on each CA Service Catalog computer, in the following sequence:

    a. The *first* (formerly *primary*) Service View computer

    b. All *additional* (formerly *secondary*) Service View computers

c. All other CA Service Catalog computers, in any order

Note: To run the setup utility, perform *all* the following steps on each computer, one computer at a time. For example, the first Service View computer is Host1, the additional Service View computers are Hosts 2 and 3, and the remaining CA Service Catalog computers are Hosts 4-6. First, run the setup utility on Host1. Next, run the setup utility on Hosts 2 and 3, one computer at a time, in any order. Third, run the setup utility on Hosts 4-6, one computer at a time, in any order.

2. Start the setup utility using one of the following methods:

   - Click the option to start the setup utility *after* you have run the installation or upgrade program on the last applicable computer. The last applicable computer is the final computer on which you run the installation or upgrade program for CA Service Catalog.
   - Start the setup utility from the Windows Start menu. For example, click Start, Programs, CA, Service Catalog, Setup Utility.

Note: If your browser blocks access to the setup utility web page for security reasons, add the CA Service Catalog computer to the trusted web sites for the browser. Use the following format for the CA Service Catalog computer: http://*hostname*:*port*.

3. Specify the following parameters and log in to the utility:

   - **Password**
     Specifies the password for logging in to the utility and running it using either of the methods in the previous step.

     Note: Record the password for reference, because the utility requires you to specify the password each time you start it.

     If necessary, you can reset the password, as follows:
     Enter the following command:

     ```
     USM_HOME\scripts\configurator.bat -resetpwd
     ```

     The Catalog system resets the password and prompts you to perform the next action: Restart the utility and specify the new password.

   - **Remote Configuration**
     (Optional) If you have run the utility successfully on another computer (a remote computer), you can use the same configuration on this computer (the local computer). To

do so, select this option and enter the URL of the remote computer. Use the following format: http://*server*:*port*/*context*. An example is http://localhost:8080/usm.
The database setup page appears.

4. Complete this step *only* if you selected the Remote Configuration option in the previous step. Otherwise, skip to the next step.
   Supply the password for the setup utility on the remote computer.
   The local setup utility copies configuration data from the remote computer and pre-populates the corresponding local fields with this data. The local utility copies the data for the database setup, CA EEM configuration, and the name of the top-level business unit. Therefore, you do not need to enter this data manually. However, you can optionally update the copied values, if necessary. This data appears on the remaining tabs of the local setup utility and is described in the remaining steps.
   You typically use the Remote Configuration option when you plan to install multiple instances of CA Service Catalog.

5. Reconfigure the Database (see page 1441)

6. Reconfigure CA EEM (see page 1445)

7. Reconfigure the CA Service Catalog Components (see page 1445)

You have completed the steps for running the setup utility on all CA Service Catalog computers.

Note: If you are installing CA Service Catalog for the first time on a computer, the setup utility pre-populates the fields that require input with default values. If you are re-installing or upgrading CA Service Catalog, the setup utility pre-populates these fields with the values from the current installation. The Remote Configuration option overwrites any default values or existing values with the values from the remote computer.

Reconfigure the Database

You can reconfigure database so that CA Service Catalog users and the Catalog system can function correctly.

Follow these steps:

1. Log in to the setup utility and click Database on the left menu.
   The utility displays the page for connecting to the database and configuring it.

2. Select the DBMS that you are using and provide the information to complete the fields.

3. Complete the fields for the Database Connectivity section.
   This step verifies that you can connect to the database. If the connection fails, perform these actions:

   a. Verify that the parameter values are correct. For more information about these parameter values, see Parameters for SQL Server (see page 1442) and Parameters for Oracle (see page 1439).

b. Verify that you prepared the catalog database and the DBMS (see page 582).

4. Specify the name of the CA Service Catalog database, typically MDB, in the Database Settings section.
   This step installs or upgrades the MDB, if necessary. This step also configures the CA Service Catalog database in the MDB.

5. Complete the remaining database fields.

6. Specify the details for the application user that you created earlier.

7. Save and confirm your updates.

8. (Optional) Review the log files, as follows:

   - For log information for SQL Server, see the following sources:
     - See the install_mdb.log file in your MDB target installation directory. This directory is specified in %TEMP%\MDB1.5, where %TEMP% is a Windows environment variable. If the MDB installation fails, review the log files in this location.
     - After a successful installation of the MDB, the install_mdb.log file is copied to the %ProgramFiles%\CA\SC\Mdb\Windows\logs folder. This log file is renamed to install_mdb_*mm-dd,hh_mm_ss*.log (for example, install_mdb_12-03,15_29_05.log).
     - See the view.log file. Its default location is the C:\Program Files\CA\Service Catalog\logs folder.
   - For log information for Oracle, see the following sources:
     - See the install_connectionID.log file in your MDB target installation directory. For example, if the connection ID is myhost_orcl, the install_connectionID.log file name is install_myhost_orcl.log. The MDB target installation directory is specified in %TEMP%\MDB1.5, where %TEMP% is a Windows environment variable. If the MDB installation fails, review the log files in this location.
     - After a successful installation of the MDB, the install_connectionID.log file is copied to %ProgramFiles%\CA\SC\Mdb\Windows\logs. This log file is renamed to install_connectionID_*mm-dd,hh_mm_ss*.log, for example, install_myhost_orcl_12-03,15_29_05.log.
     - See the view.log file. Its default location is the C:\Program Files\CA\Service Catalog\logs folder.

You have reconfigured the database.

Parameters for SQL Server

Before you install CA Service Catalog, you specify values for several parameters to establish the connection to an SQL Server database. The following parameters may require explanation:

Important! For a migration model upgrade, when you are prompted for information about the Catalog database, use the *existing* Catalog database specifications.

For the Database Connection

- **Host Name**
  Defines the computer name of the Microsoft SQL Server (SQL Server) server.

- **Port**
  Defines the TCP Port number of the database server.
  If you are using an instance name, verify the following requirements:

  - The instance name has a port number set.

  - Your implementation is *not* using dynamic ports.

- **User Name and Password fields**
  Define the user name and password of the SQL Server database administrator (DBA). The setup utility uses these credentials to set up the CA Service Catalog database.
  You can use the login credentials of either of the following users:

  - System administrator (sa). This user requires dbo as its default schema.

  - The user named installuser that you created. You can optionally create this user so that the setup utility uses this user (instead of sa) to set up the CA Service Catalog database.

- **Instance Name**
  Defines the SQL Server instance name for the MDB. For example, myinstance. You can specify either a primary instance or a named instance.

For the Database Configuration

- **Database Name**
  Specifies the name of the CA Service Catalog database: MDB.

  Important! The name of the Catalog database must be MDB. This requirement is especially important if you integrate CA Service Catalog with another CA product, such as CA Service Desk Manager, CA APM, or CA Process Automation.

Application User Settings

- **User Name and Password fields**
  Define the user name and password that CA Service Catalog uses for accessing this database. This user name and password are created in the database.
  This user is the first application user. For increased flexibility, you can optionally create a second application user.

Parameters for Oracle

Before you install CA Service Catalog, you specify values for several parameters to establish the connection to an Oracle database. The following parameters may require explanation:

Important! For a migration model upgrade, when you are prompted for information about the Catalog database, use the *existing* Catalog database specifications.

Note: These parameters apply to Oracle running on both Windows and Linux.

For the Database Connection

- **Host Name**
  Defines the computer name of the Oracle server.
- **Port**
  Defines the TCP Port number of the database.
- **User Name and Password fields**
  Define the user name and password of the Oracle database administrator (DBA).
- **Service Name**
  Defines the service name. Every Oracle database or service has a service name. The service name of an Oracle database is typically its global database name. Enter the service name of the database or other service that you want to access.
  A non-RAC deployment typically includes one service, one instance, and one database, each with the same name. However, in a RAC deployment, multiple instances can provide multiple services, all connecting to a single database.
- **Connection SID**
  Defines the connection ID (such as orcl) for connecting to the Oracle server, as follows:
  - For a local database, this value is typically the SID.
  - For a remote database, this value is typically the Net Service Name.

For the Database Configuration

- **Database Name**
  Specifies the name of the CA Service Catalog database: MDB.

Important! The name of the Catalog database must be MDB. This requirement is especially important if you integrate CA Service Catalog with another CA product, such as CA Service Desk Manager, CA APM, or CA Process Automation. CA Service Catalog embeds CA MDB r1.5.

- **Tablespace Path**
  Defines the complete path name of the tablespace for Oracle.

- **Data Tablespace Name**
  (Optional) Defines the tablespace name for the data.

- **Index Tablespace Name**
  (Optional) Defines the tablespace name for the indexes.
  The installer verifies whether the data and index tablespaces exist in the MDB. These tablespaces exist when either of the following conditions are met:

  - The MDB is being upgraded.

  - The CA Service Catalog database is being installed in an existing MDB, typically from an already installed CA product or group of products.

  If the data and index tablespaces exist, the installer displays their names. The installer also prompts you to specify whether to continue using the existing names or overwrite them with new names.

Application User Settings

- **User Name and Password fields**
  Define the user name and password that CA Service Catalog uses for accessing this database. This user name and password are created in the database.

Reconfigure CA EEM

You can reconfigure CA EEM for use with CA Service Catalog using the setup utility.

Note: Use the Setup Utility if you have only CA Service Catalog in your environment. Use the Service Management Administration, Common Configuration option to reconfigure CA EEM if you have integrated CA Service Catalog with at least one other CA Service Management product.

For more information, see Integrate CA Service Catalog with CA EEM Manually (see page 3292)

CA EEM has been reconfigured for use with CA Service Catalog.

Reconfigure the CA Service Catalog Components

You can reconfigure the CA Service Catalog product components that you want on this computer.

Note: If you are installing CA Service Catalog on this computer for the first time, you can use the utility to reconfigure the product components. However, if you are upgrading or installing CA Service Catalog on this computer a second time, this value is read-only and you cannot reconfigure the product components.

Follow these steps:

1. Log in to the setup utility and click Components in the the left menu.
2. Enter the name of the service provider business unit. It is the “root” business unit above all other business units. As a best practice, specify your company domain name or a short version of your company name for the business unit ID.
3. Select each component that you want to use on this computer:
   - **Catalog Component**
     Lets you create service options and service option groups, which you use to create services that users can request from the catalog.
     This option includes the Catalog Content, which supplies the predefined services in the catalog. Examples include services for requesting hardware, software, and other IT essentials from your business unit. You can use these services as-is, or you can copy and customize them.
     This option installs a Windows service named CA Service Catalog.
   - **Service Accounting Component**
     Lets you provide billing and chargeback for the services that users request from the catalog. You can also use Service Accounting Component to allocate costs, prepare budgets, and plan IT services.
     This option installs a Windows service named CA Service Accounting.
4. Click Save.
5. Follow the prompts and complete the setup.

Note: You can optionally review the installation log file, view.log. Its default location is the USM_HOME\logs folder. This log file is visible after you have completed all tasks of the installation or upgrade program and have closed the program. For information about uninstallation and aborted or canceled installations (when applicable), see the CA_Service_Catalog_Uninstallation.log file in the Windows Temp folder.

CA Service Catalog components have been reconfigured.

Configuration Files

The configuration files and locations are as follows:

- Database connection configuration file: USM_HOME\DBSource.properties
- CA EEM connectivity configuration file: USM_HOME\Eiam.properties
- IXUtil utility configuration file: USM_HOME\scripts\ixutil.cfg

USM_HOME is the documentation convention that specifies the local CA Service Catalog installation directory. For 32-bit computers, the default path name is C:\Program Files\CA\Service Catalog. For 64-bit computers, the default path name is C:\Program Files (x86)\CA\Service Catalog for 32-bit installations or C:\Program Files\CA\Service Catalog for 64-bit installations.

- Configuration Settings (see page 1447)
- Set CA Service Catalog Configuration Options (see page 1449)
- Set Accounting Configuration Options (see page 1461)
- Set Administration Configuration Options (see page 1477)

Configuration Settings

This article contains the following topics:

- Inheritance of Configuration Settings Through the Business Unit Hierarchy (see page 1447)
- Change the Business Unit (see page 1448)

After the CA Service Catalog installation is complete, verify the configuration settings. Doing so helps ensure that the product functions according to the needs of your organization.

Verify the settings by group, as follows:

- Set CA Service Catalog Configuration Options (see page 1449)
- Set Accounting Configuration Options (see page 1461)
- Set Administration Configuration Options (see page 1477)
  These include Integration-Specific Options (see page 1478)
- Location of shared files (filestore)

Important! With one exception, CA Service Catalog sends emails in HTML format only. To receive legible emails from CA Service Catalog, recipients must configure their email software to accept emails in HTML format. Otherwise, emails from CA Service Catalog display indecipherable messages when opened. The one exception to this HTML-only rule is invoice history. You can choose to view and email invoice history in HTML, CSV, or XML format. The HTML-only rule applies to all other invoice-related areas of CA Service Catalog, including invoice generation.

Inheritance of Configuration Settings Through the Business Unit Hierarchy

The following rules govern the relationship between parent and child business units (children), including the inheritance of configuration settings:

- The child business units directly under the top-level business unit (the service provider) are named super business units. Super business units *always* inherit their configuration settings from the service provider business unit.
- If the configuration parameter *Contains Sub Units* is enabled, a super business unit can have children.
- If the *Contains Sub Units* parameter of the super business unit is enabled, you *can* edit the configuration settings of the super business unit.
- If you edit the configuration settings of a super business unit, your changes do *not* apply to the super business unit. Instead, your changes apply to its children. A child "inherits" its configuration settings from its parent.
- You can optionally create unlimited levels of children under super business units. If the *Contains Sub Units* setting of the business unit is enabled, you can edit its configuration settings. Your configuration changes do *not* apply to the business unit itself but instead apply to its children. Conversely, if the *Contains Sub Units* setting of the business unit is disabled, you cannot edit its configuration settings.

Thus, the following summary applies to all business units except for the service provider:

- A business unit always inherits its configuration settings from its parent.
- You can edit the configuration settings of a business unit *only* if its Contains Sub Units setting is enabled. Your changes apply *only* to its children.

Change the Business Unit

By default, the Catalog system displays settings for the business unit that you logged in to. If your role permits, you can change to a different business unit.

When common multi-tenant administration is enabled, you can add tenants, delete tenants, or edit the common attributes *only* through CA Service Desk Manager. When common multi-tenant administration is enabled, you can *view* tenants and all their attributes in CA Service Catalog. But you can edit only the CA Service Catalog-specific attributes.

Follow these steps:

1. Click Catalog, Configuration.
2. Click the Change Business Unit button.
   The Search Business Units dialog appears.
3. Use the Expand and Collapse icons to navigate the business unit tree. Alternatively, use the selection criteria and Search button to locate the desired business unit.
   The list includes only the business units that your role permits you to access.
4. To select a business unit, click its name in the tree.
   The window closes, and the configuration settings for that business unit appear.

Set CA Service Catalog Configuration Options

You configure CA Service Catalog to customize settings for request management, access control, request emails, and so forth. These settings specify how the Catalog system processes requests in your organization.

Follow these steps:

1. Click Catalog, Configuration.
2. Perform one of the following actions:
   - To manage configuration options for a different business unit, change the business unit (see page 1448) before performing the next step.
   - To manage configuration options for the current business unit, go directly to the next step.
3. Click one of the following links for the category of options that you want to update:
   - Catalog Configuration (see page 1449)
   - Request Management Configuration (see page 1450)
   - System Configuration (see page 1461)
4. View the options for the category, and click the Modify icon for the option that you want to update.
5. Update the setting as required and click Update Configuration.

You have set the CA Service Catalog configuration options. These settings apply to the children of the business unit that you updated, according to the inheritance of configuration settings through the business unit hierarchy (see page 1447).

Catalog Configuration

As part of setting the CA Service Catalog configuration options (see page 1449), you specify the following Catalog Configuration options. These settings control the behavior of the catalog.

- **Default Effect of Service Option Element Changes**
  Specifies when to reflect changes to service option elements for accounts that have subscribed to or requested services that include them.
  Select one of the following options to use when the service option element changes:
  - **Specify when the Service Option Element Changes - Allow User to Choose**
    Enables the administrator to specify the effect of the change on existing subscribers or requestors.
  - **Beginning of Accounts' Current Billing Period - No Audit Trail**
    Implements the change retroactively to the beginning of the current billing period for existing subscribers or requestors. No audit trail applies.

- **Beginning of Accounts' Current Billing Period**
  Implements the change retroactively to the beginning of the current billing period for existing subscribers or requestors.

- **Beginning of Accounts' Next Billing Period**
  Implements the change at the beginning of the next billing period for existing subscribers or requestors.

- **Immediately during Accounts' Billing Period**
  Implements the change immediately for existing subscribers or requestors.

- **Specify a Future Effective Date**
  Enables the Administrator to specify a date on which the change takes effect for existing subscribers or requestors.

Default: Specify when the Service Option Element Changes - Allow User to Choose.

- **Pass Through Catalog**
  Specifies whether to include the catalog of the parent business unit.
  If you select this option, the parent catalog is passed down to the child business unit. This setting is useful in a multiple-level business unit organization. This setting applies only to the settings for a child business unit.
  Default: No

Request Management Configuration

As part of setting the CA Service Catalog configuration options (see page 1449), you specify the Request Management Configuration options. These settings that control the behavior of requests for the following groups of parameters:

- Access Control Parameters (see page 1450)
- Other Parameters (see page 1453)
- Request Email Parameters (see page 1458)

Access Control Parameters

As part of setting the CA Service Catalog configuration options (see page 1449), you specify the following Access Control parameters:

- **Access Control: Add Request**
  Specifies which user roles can add a request.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, End User, Catalog User, Request Manager, Catalog Administrator

- **Access Control: Edit Request**
  Specifies which user roles can edit a request. All users can edit their own requests, if the status of the request is in the not submitted range.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, End User, Catalog User, Request Manager, Catalog Administrator

- **Access Control: Delete Request**
  Specifies which user roles can delete a request or a requested service. All users can delete their own requests, if the status of the request is in the not submitted range. Once a requested service is in a canceled state, only users with Delete Request permission can delete a canceled service.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

- **Access Control: Cancel Request**
  Specifies which user roles can cancel a request.
  This parameter works together with the Allow Cancellation Through parameter, which is described later in this list.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

- **Access Control: Show Amount Column**
  Specifies which user roles can view the Amount Column when viewing a request.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

- **Access Control: Show Period Column**
  Specifies which user roles can view the Period Column when viewing a request or shopping cart.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

- **Access Control: Show Related Ticket Column**
  Specifies which user roles can view the Related Ticket Column when viewing a request or shopping cart.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

- **Access Control: Show General Information**
  Specifies which user roles can control whether the general information form is visible when you create a request.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator, Service Manager, End User, Catalog User

- **Access Control: Show Request Information**
  Specifies which user roles can control whether the request information form is visible when you create a request.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator, Service Manager, End User, Catalog User

- **Access Control: Save Cart As Request**
  Specifies which user roles can view the button allowing the user to save the shopping cart as a request, clearing the cart for reuse.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

- **Access Control: Proxy Request**
  Specifies which user roles can view the link to change the Requested For field from your own user ID or account to another user ID or account.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

- **Access Control: Proxy Action**
  Specifies which user roles can see the link to approve, reject, fulfill, or transfer requests pending action that is assigned to other users.

- **Access Control: Show Fulfillment Details**
  Specifies which user roles can view statistical information regarding the time that is required to fulfill a service option in the past.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

- **Access Control: Take/Return Request Pending Action**
  Specifies which user roles can take or return ownership of requests pending action. They can take ownership of requests pending action from the following options:

  - A group queue
  - The queue of another user in the same business unit or child business unit

  Similarly, they can return ownership of requests pending action from their own queue to their group queue.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

- **Access Control: Transfer Request Pending Action**
  Specifies which user roles can transfer ownership of requests pending action from the assigned user to either of the following options:

  - Another user in the same group
  - Another user in the same business unit or child business unit

  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

- **Access Control: Delegate Request Pending Action**
  Specifies which user roles can delegate ownership of requests pending action from a group queue to either of the following options:

  - A specific user in that group
  - Another user in the same business unit or child business unit

  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

- **Access Control: Push Through Requests**
  Specifies which user roles can push through ("force") a stuck request to the next level of approval or fulfillment.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

- **Access Control: Display Request Warning**
  Specifies which user roles can view the warning icon indicating that a request is stuck. **Default:** Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator, End User, Catalog User

- **Access Control: Hold/Resume Request**
  Specifies which user roles can hold a request that is in progress and can resume a request that is in Hold status.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator, End User, Catalog User

Other Parameters

As part of setting the CA Service Catalog configuration options (see page 1449), you specify the following miscellaneous parameters:

- **Allow Attachments at Service Option Level**
  Lets users add attachments to individual service options. This setting must be Yes if you want to make attachments mandatory for any service option.

- **Allow Cancellation Through**
  Defines the status through which users can cancel requests. After the request moves to the next status, it cannot be canceled. This parameter works together with the *Access Control: Cancel Request* parameter.
  Default: Fulfilled

- **Allow Discrete Handling for Reject**
  Specifies the effect of the rejection of a single service or service option upon other services and service options in the same request, as follows:

  - **Yes**
    Specifies that when you reject a service or service option, the remaining services or service options can advance if they are approved. If the following options are approved, they can advance in the request life cycle:

    - Other services in the same request

    - Other service options in the same service

  - **No**

  Specifies that when you reject a service or service option, the entire request is rejected. All services in the same request are rejected and can no longer advance in the request life cycle, even if they were previously approved. Similarly, all service options in the same service are rejected and can no longer advance in the request life cycle, even if they were previously approved.

Default: No

Note: For more information about discrete request life cycle, see the Manage Discrete Request Life Cycle (see page 2120) section.

- **Allow Discrete Handling of Service Options After**
  Specifies the status at which request managers (approvers and fulfillers) can handle requests pending action (approval, rejection, or fulfillment) *discretely*. When the request reaches the status you specify, request managers can discretely approve, reject, or fulfill each service option in every service in the request.
  Use this parameter to specify that pending actions are assigned at the service option level, rather than the service level.
  The setting applies to the request *from* the starting status that you specify *through* the remainder of the request life cycle.
  Valid values: Submitted, Pending Fulfillment, or Completed.
  Default: Pending Fulfillment

  Note: For more information about using a discrete request life cycle, see the Manage Discrete Request Life Cycle (see page 2120) section.

- **Allow Discrete Request Life Cycle After**
  Specifies the status at which individual service options in a service and individual services in a request advance independently. *Independently* means *without* requiring or waiting for any other service option in the same service or any other service in the same request to advance its status. When the request reaches the specified status, the service options that you approve or fulfill can complete the remainder of the request life cycle. This condition exists even if other service options in the same service do not advance in status.
  As soon as the request reaches the specified status, the services that you approve or fulfill can complete the remainder of the request life cycle. This condition exists even if other services in the same request are rejected or are not updated.
  Valid values: Submitted, Pending Fulfillment, or Completed.
  Default: Completed
  The setting applies to the request *from* the starting status that you specify *through* the remainder of the request life cycle.

  Note: For more information about using a discrete request life cycle, including sample settings and their meanings, see the Manage Discrete Request Life Cycle (see page 2120) section.

- **Allow Multi Service/Service Option Approval**
  Lets users approve or reject multiple, selected services or service options (including all) with a single click. This ability is *multi-item approval*. Discrete approval is required to approve or reject service options using multi-item approval.

- **Allow Notes at Service Option Level**
  Controls whether a user can add notes at the service and service option levels.
  If this option is set to Yes, then the Add Note icon appears in the Action column for requests. Therefore, the user can add a note for a specific service or service option.
  If this option is set to No, then the user can add notes for the entire request but not for a specific service or service option.
  Default: No

- **Allow Only One Service Per Request**
  Specifies whether a user can include more than one service in a request or cart.
  If this option is set to Yes, then a user can have only one service in a cart or request. Also, the user must submit the cart or request before creating a new one.
  If this option is set to No, then a user can select multiple services from the catalog. The user can add them to the cart or request before submitting the request.
  Default: No

- **Browse Catalog Layout**
  Specifies the look-and-feel for the Requests page. On this page, users can create, customize, submit, and manage requests.
  Specify *one* of the following options. Click Home, Requests to verify the resulting look-and-feel on the Requests page.
  The Service View and Service View without Browse Section options provide the best performance. These options provide *links to* the requests, while the other options display the requests directly.

  - **Service View**
    Configures the Requests page to display the catalog, featured services, and a search-for-services field in boxes.
    A My Requests link opens a drop-down list. The list includes options to search requests, review open requests, and act on pending requests.

  - **Service View without Browse Section**
    Configures the Requests page to display the catalog alone. Featured services and the search-for-services field do *not* appear.
    A My Requests link appears, as described for the Service View option.

  - **Request View**
    Configures the Requests page to display the catalog (categories and lists of services) in a column on the left.
    Boxes to the right of the column enable users to do the following tasks:

    - Search for services.
    - View and request featured services.
    - Review their own recent requests and, if applicable, act on them.
    - Use links to review open, pending, and completed requests.
    - Search for requests.

- **Grid View**
  Configures the Requests page to display the catalog in a grid.
  Boxes surrounding the grid enable users to perform the same tasks as listed for the Request View option.

Default: Service View

- **Browse Catalog: Show Folder Icon**
  Specifies whether images associated with catalog folders appear in the Browse section of the Requests page.
  If this option is set to Yes, folder images appear in the Browse section. If this option is set to No, they do not appear.
  Default: No

- **Browse Catalog: Show Subfolders**
  Specifies whether the top-level subfolders under each catalog folder appear in the Browse section of the Requests page.
  If this option is set to Yes, the first level of subfolders appear under each catalog folder in the Browse section.
  If this option is set to No, only the catalog folders appear.
  Default: Yes

> **Note:** For any individual catalog folder, you can override this default by changing its folder details on the Catalog, Service Offerings page.

- **Default User for Request Actions**
  Specifies the user who must be assigned a pending action when no other user is available. This setting is typically used for request approvals when the user needs manager approval and no manager exists in the system for the user. When this setting is used with the system approval process, verify that this user has the highest authorization level.
  Default: spadmin

- **Display Service Health**
  This parameter applies *only* if you are integrating CA Service Catalog with CA Business Service Insight.
  Specifies whether to enable catalog users requesting a service to view actual, current data regarding the quality or "health" of a service. The health is based on the level of compliance of the service to its associated metrics. This data includes the contractual metrics, incentive metrics, and the SLA health period. This information is specified in the contract-specific details for the service option elements in the service being requested.
  The metric data includes both the performance criteria and the actual number of violations, including the time increments measured.
  If you enable this option, catalog users can view this actual and current metric data for the service they are requesting.

- **Edit Cancelled Requests**
  Specifies that if the value is set to **Yes**, you can edit a cancelled request. If the value is set to **No**, the cancelled request cannot be edited.

Notes: This parameter is available only if you have installed the CA Service Catalog 14.1.01 patch updates from CA Support.

- **Edit Completed Requests**
  Specifies that if the value is set to **Yes**, you can edit a completed request. If the value is set to **No**, the completed request cannot be edited.

  Notes: This parameter is available only if you have installed the CA Service Catalog 14.1.01 patch updates from CA Support.

- **Enable Delegation of Catalog**
  Specifies whether to enable the delegation of catalogs: Yes or No.
  When this option is enabled, no users are *required to* delegate use of their catalogs. But they can *optionally* do so.

  Note: The delegation of a catalog does *not* affect the Catalog configuration of the CA Service Catalog, such as the *Use Service Provider Catalog Only* and *Pass Through Catalog* configuration parameters. Similarly, the delegation of a catalog is *not* directly related to the configuration options such as *Access Control: Add Request* in this Request Management Configuration section. For more information about delegation of catalogs, see the Delegate Catalog (see page 2222) section.

- **Notify users when they complete their own pending actions**
  Specifies whether request managers receive a notification email every time they address a pending action by approving, rejecting, or fulfilling a service option, service, or request.
  If you specify Yes, request managers receive such emails confirming their own actions.
  If you specify No, request managers do not receive such emails.
  This setting is especially relevant if you are using discrete approval and the *Allow Request Life Cycle to Continue After* parameter is set to Submitted. If this parameter parameter is set to Yes, request managers are likely to receive several notification emails.
  For example, if a service has five service options and the request manager approves each option, the request manager receives five confirmation emails. To prevent request managers from receiving such emails, set *Notify users when they complete their own pending actions* to No.
  The Requested For users and Requested By users always receive these notification emails, regardless of the setting of these parameters.

- **Number of Requests per Page**
  For individual users (not administrators), specifies the maximum number of requests that appear on Request List pages. When a user moves to a new Request List page, the default setting replaces their custom settings. Users can optionally customize the display for each new Request List page they view.
  Request List pages appear when you click Home, Requests, and click any of the following options:

  - Open Requests
  - My Recent Requests

- Completed Requests
- Pending My Action

Advanced Search - after you search for requests and view the results.
Administrators can set the following options for all users: The individual columns that appear on Request List pages and the default maximum number of requests per page.

- **PDA Support: Enable**
  Specifies whether to enable PDA support.
  When you specify Yes, PDA users can click the links that are provided in PDA-compliant request approval emails to access the requests. The users can approve or reject them. Support for forms are limited when you enable PDA Approval.
  When you specify No, the links for accessing the requests and approving or rejecting them do *not* appear in the request approval emails that PDA users receive. The absence of such links implicitly guides PDA users to use an office computer to view, approve, and reject requests.

- **Request Details Link for E-Mail Notifications:**

  Notes: This parameter is available only if you have installed the CA Service Catalog 14.1.01 patch updates from CA Support.

  By default, value for this parameter is not configured. You can configure this parameter in the following format if CA Service Catalog is configured with USS:
  http://<USS HostName>:<PortNumber>/web/frontoffice/myrequest-catalog?ServiceCatalogRequestID=
  If you configure the Unified Self-Service (USS) URL for **Request Details Link for E-Mail Notifications**, clicking on the request details hyperlinks in the email notification will take you to the Unified Self-Service login page instead of CA Service Catalog login page. If this parameter is not configured, clicking on the hyperlinks in email notification with request details takes you to the CA Service Catalog login page.

- **Request Home Page: Include Request Information**
  Specifies which roles can view the Request Lookup and My Recent Requests sections on the Home or Requests menu option page.
  Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, End User, Catalog User, Request Manager, Catalog Administrator, Service Manager

- **Request General Information Column Configuration**
  Default: Name, ID, Requested For, Date Created, Date Required, Requested By, Priority, Last Modified, Status

Request Email Parameters

As part of setting the CA Service Catalog configuration options (see page 1449), you specify the following Request Email parameters:

- **Request Email: From Address**
  Specifies the email address from which the Catalog system sends emails about requests.

- **User Defined**
  Uses the email address that the user specifies. Selecting this option with no email address specified sets this setting to EMPTY.

- **Service Provider Email**
  Uses the email address for the service provider business unit.

Default: CatalogSystem@serviceprovider.com, where "*serviceprovider*" is the root business unit that is specified during installation.

- **Request Email: From Name**
  Specifies the email address *name* from which emails about requests are sent.
  Default: CatalogSystem

- **Request Email: To**
  Specifies the primary recipient email address to which emails about requests are sent.

  - **User Defined**
    Uses the email address that the user specifies. Multiple email addresses can be specified, separated by a semi-colon. Selecting this option with no email address specified sets this setting to EMPTY.

  - **Requested For User/Account Email**
    Uses the email address of the user or account to which this request applies.

  - **Requested By User/Account Email**
    Uses the email address of the user or account that created this request.

  Default: EMPTY, meaning this value is set when email options are used.

- **Request Email: CC**
  Specifies the "CC" recipient email address to which emails about requests are sent.

  - **User Defined**
    Uses the email address that the user specifies. Multiple email addresses can be specified, separated by a semi-colon. Selecting this option with no email address specified sets this setting to EMPTY.

  - **Requested For User/Account Email**
    Uses the email address of the user or account to which this request applies.

  - **Requested By User/Account Email**
    Uses the email address of the user or account that created this request.

  Default: EMPTY, meaning this value is set when email options are used.

- **Request Email: BCC**
  Specifies the "BCC" recipient email address to which emails about requests are sent.

- **User Defined**
  Uses the email address that the user specifies. Multiple email addresses can be specified, separated by a semi-colon. Selecting this option with no email address specified sets this setting to EMPTY.

- **Requested For User/Account Email**
  Uses the email address of the user or account to which this request applies.

- **Requested By User/Account Email**
  Uses the email address of the user or account that created this request.

Default: EMPTY, meaning this value is set when email options are used.

- **Request Email: Subject**
  Specifies the email subject that is used when emails about requests are sent.
  In addition to specific text, you can include dynamically substituted values in the subject text. The syntax for including dynamically substituted values is $Request.*variable_name*$.

  - ***variable_name***
    Specifies the name of the variable value to use.

  You can specify the following variables in the subject text:

  - **request_id**
    Specifies the internal Request ID, such as “10001”.

  - **name**
    Specifies the request name that the user specifies.

  - **status**
    Specifies the status of the request, such as “Pending Approval.”

  - **created_date**
    Specifies the date and time the request was created.

  - **modified_date**
    Specifies the date and time the request was last modified.

  - **completion_date**
    Specifies the date and time the request was completed.

  - **desired_date**
    Specifies the date and time in the Date Required field of the request.

  - **comments**
    Specifies the request Description that the user specifies.

  - **priority**
    Specifies the priority of the request.

  - **req_for_account_id**
    Specifies the internal account ID for the Requested For user or account.

- **req_by_account_id**
  Specifies the internal account ID for the Requested By user or account.

- **req_for_user_id**
  Specifies the user ID of the Requested For user, if the request is for a user not an account.

- **req_by_user_id**
  Specifies the user ID of the Requested By user.

Default: Email of Request ($Request.request_id$) - $Request.name$

- **Request Email: Message**
  Specifies the email message that is used when emails about requests are sent. You can override this text.
  In addition to specific text, you can include dynamically substituted values in the subject text. The syntax for including dynamically substituted values is $Request.*variable_name*$ where *variable_name* is the name of the variable value to use.The variables available for use are the same as in the *Request Email: Subject* setting.
  Default: Request ($Request.request_id$) created on $Request.created_date$

System Configuration

As part of setting the CA Service Catalog configuration options (see page 1449), you specify the following System Configuration parameters. These settings control the behavior of the system, regardless of business unit. This category is displayed *only* when you are logged in to the service provider (root) business unit.

- **Use Service Provider Configuration Only**
  Specifies whether a child business unit can have its own CA Service Catalog configuration settings.
  If this setting is Yes, the Catalog system ignores all CA Service Catalog configuration settings for a business unit. So, each business unit uses the configuration settings for the service provider.
  If this setting is No, then each business unit can have its own CA Service Catalog configuration settings.
  Default: No

- **Use Service Provider Catalog Only**
  Specifies whether the service provider business unit catalog is available to all business units in the hierarchy.
  If this setting is Yes, the subscribing or requesting user of a child business unit sees only the catalog of the service provider (root) business unit. That is, the child business unit cannot have its own catalog.
  If this setting is No, the child business unit can have its own catalog.
  Default: No

Set Accounting Configuration Options

You can optionally customize several options for accounting configuration. These options cover invoicing and subscription details, to meet the requirements of your organization.

Follow these steps:

1. Log in as a user with the Service Delivery Administrator role.

2. Click Accounting, Configuration.
3. Check for the name of the current business unit, and perform one of the following actions:
   - To set the accounting configuration options for a different business unit, change the business unit before performing the next step.
   - To set the accounting configuration options for the current business unit, go directly to the next step.
4. Click the link for the category of options that you want to update:
   - Accounting Profile Defaults (see page 1462)
   - Billing Cycles (see page 1466)
   - General (see page 1467)
   - Invoice Engine Configuration (see page 1467)
   - Invoice Methods (see page 1475)
   - Payment Methods (see page 1475)
   - Subscription Configuration (see page 1476)
5. View the options for the category, and click the Modify icon for the option that you want to update.
6. Update the setting as required and click Update Configuration.
7. Repeat the previous steps for each accounting configuration option that you want to update.

You have set the accounting configuration options. These settings apply to the children of the business unit that you updated, according to the inheritance of configuration settings through the business unit hierarchy (see page 1447).

Accounting Profile Defaults

As part of setting accounting configuration options (see page 1461), you specify the Accounting Profile Default settings. These settings indicate default values for newly created accounts for the current business unit. The following options require explanation:

- **Account Type**
  Specifies the type of account. This setting controls how outstanding balances are handled on invoices, as follows:
  - **Open Item**
    Specifies that every invoice is unique. Once a charge appears on an invoice, it does not appear on any future invoices.
  - **Balance Forward**
    Specifies that the remaining balance of a previous invoice is added to the next invoice.

- **Zero Balance**
  Specifies that the account is a zero balance account. A zero balance account can have charges appear on its invoice, but the total remaining balance is always zero. You cannot post payments to zero balance accounts.
  This option is commonly used when an aggregating account holds the charges for one or more zero balance accounts.

Default: Open Item

- **Aggregate**
  Specifies the role of the account in charge aggregation for invoicing, as follows:

  - **No**
    Specifies that the charges for the account appear *only* in the invoice of the account. The charges do *not* appear on an invoice for a related aggregating account.

  - **Yes**
    Specifies that the charges for the account appear in the invoices for all of the following options:

    - The original account

    - Each aggregating account in the same business unit or a parent business unit, up through the hierarchy of business units

  - **Aggregating Account**
    Specifies that the invoice for the account shows charges for all accounts in the same business unit or child business units. These business units must have Aggregate set to Yes or Aggregating Account.

    Note: To avoid double invoicing, do *not* specify more than one aggregating account in each business unit.

Default: No

- **Automatic Invoicing**
  Specifies whether to create an invoice for the account, as follows:

  - **Yes**
    Specifies that the account has an invoice that is generated during a bill run.

  - **No**
    Specifies that the account does not have an invoice that is generated during a bill run.

Default: Yes

- **Billing Cycle**
  Specifies the account invoicing cycle. Options are daily, weekly, and monthly.
  Note: This field works with the Billing Cycle Interval, which is described later in this topic.
  Default: Monthly

- **Period Start Date**
  Specifies how to set the start date for the invoice period for the account. Select from the following options:

  - **Business Unit Opened Date**
    Sets the start date as the date the business unit of the account was created (the Opened Date).

  - **Account Opened Date**
    Sets the start date as the date the account was opened (the Accounting Profile Opened Date).

  - **Current Date**
    Sets the start date to be the date that the accounting profile (account) was created.

  - **Current Date of Next Period**
    Sets the start date as the addition of both of the following options:

    - The date the accounting profile (account) was created.

    - The interval that the Billing Cycle and the Billing Cycle Interval determine.

  - **Day of Week**
    Sets the start date as the same day of the week on which the accounting profile (account) was created.

  - **Day of Month**
    Sets the start date as the same day of the month on which the accounting profile (account) was created.

  - **Day of Year**
    Sets the start date as the same day of the year on which the accounting profile (account) was created.

  - **Day of Week Adjusted from Current Date**
    Sets the start date as the specified day of the next week after the accounting profile (account) was created.

  - **Day of Month Adjusted from Current Date**
    Sets the start date as the specified day of the next month after the accounting profile (account) was created.

  - **Day of Year Adjusted from Current Date**
    Sets the start date as the specified day of the next year after the accounting profile (account) was created.

  - **Last Day of Current Month**
    Sets the start date as the last day of the month during which the accounting profile (account) was created.

  - **First Day of Next Month**
    Sets the start date as the first day of the next month after the accounting profile (account) was created.

- **Specify Date**
  Sets the start date as the date that you specify manually.

Default: Account Opened Date

- **Billing Cycle Interval**
  Specifies the number of billing cycles between invoices.
  For example, to bill the account quarterly, select a Billing Cycle of Monthly and a Billing Cycle Interval of 3. The Billing Cycle field is described earlier in this topic.
  Default: 1

- **Default Days Due**
  Specifies the number of days after the invoice date to use as the payment due date.
  Default: 10

- **Grace Days**
  Specifies the number of days that are permitted past the invoice date without a payment. If the invoice is not paid before the grace days expire, the account incurs extra fees and penalties.
  Default: 10

- **Invoice Method**
  Specifies how to send invoices. Select one of the following options:

  - **Email**
    Sends the invoice as an email attachment to the email address of the account.
    The Catalog system:

    - Uses the format that is specified in Invoice Output Type setting.
    - Uses the delivery mechanism that is specified in the Invoice Generation Email Attachment Type setting.
    - Saves the attachment in the Invoice Email Location server folder.

  - **Fax**
    Saves the invoice using the format that is specified in Invoice Output Type setting in the Invoice Fax Location server folder.

  - **Postal**
    Saves the invoice using the format that is specified in Invoice Output Type setting in the Invoice Postal Location server folder.

  - **Printer**
    Saves the invoice using the format that is specified in Invoice Output Type setting in the Invoice Printer Location server folder.

  Default: Email

- **Period End Date**
  Specifies how to set the end date for the invoice period for the account. Select one of the following options:

- **Compute from Start Date Using Billing Cycle**
  Specifies an end date that is based on the period start date, the billing cycle, and the billing cycle interval. Each of these settings is described earlier in this topic.

- ***other options***
  Specifies an end date equivalent to the options for period start date. That setting is described earlier in this topic.

The dates settings presume that each new day begins at a time of 00:00:00. Specify a Period End Date that includes the last full day. For example, to bill for the entire month of July, make your period 7/1/yyyy - 8/1/yyyy to include the entire last day of the month.
Default: Compute from Start Date Using Billing Cycle

- **Status**
  Specifies the status of the account when it is created: Closed, Opened, or Suspended. Invoicing occurs only when this setting is Opened.
  Default: Opened

- **Status Reason**
  Specifies the reason for the value of the Status option. You enter this text manually.
  Limit: 1024 characters
  Default: New account waiting approval

- **Taxable**
  Specifies whether the account is taxable.
  Specify Yes or No.
  Default: No

Billing Cycles

As part of setting accounting configuration options (see page 1461), you specify the settings for the billing cycles. You specify which billing cycle choices are available on the Accounting Profile of the account.

- **Daily**
  Specifies whether users can generate an invoice daily. If this option is set to Yes, Daily appears in the list of options for specifying the billing cycle.
  Default: Yes

- **Monthly**
  Specifies whether users can generate an invoice monthly. If this option is set to Yes, Monthly appears in the list of options for specifying the billing cycle.
  Default: Yes

- **Weekly**
  Specifies whether users can generate an invoice weekly. If this option is set to Yes, Weekly appears in the list of options for specifying the billing cycle.
  Default: Yes

General

As part of setting accounting configuration options (see page 1461), you specify the General settings. This value applies to all accounts in the current business unit.

- **Default Post Payment Method**
  Specifies the default option for posting a payment: cash, check, or credit card.
  Default: Check

Invoice Engine Configuration

As part of setting accounting configuration options (see page 1461), you specify the Invoice Engine Configuration settings. These settings control the behavior of the invoice engine during bill runs. These values apply to transactions and invoices for all accounts in the current business unit. The following settings require explanation:

- **Invoice Style for Aggregation**
  Specifies how totals appear on invoices for aggregating accounts.
  Select from the following options:

  - **All Details**
    Displays all details.
  - **Account Totals**
    Displays only the total of the aggregating account.
  - **Drill Down Account Totals**
    Displays subtotals by account by service. Users can drill down to view details for each account.
  - **Service by Account Totals**
    Displays subtotals by account by service, without drill-down functions.
  - **Service Totals**
    Displays subtotals by service for all accounts.
  - **Type by Account Totals**
    Displays subtotals by account by service option element type.
  - **Type Totals**
    Displays subtotals by service option element type.

  Default: All Details

- **Aggregate Advanced Charges**
  Specifies how advanced charges appear on an invoice. Advanced charges span multiple periods as defined by the period start and end dates in the Accounting Profile of the account.

  - **Yes**
    Displays the total of the advanced charges on one line.
  - **No**
    Displays the advanced charges individually on multiple lines.

For example, suppose that the cycle for a subscription is monthly and the billing cycle for an account is yearly. In this case, a Yes setting summarizes the charges on one line. Conversely, a No setting displays 12 lines instead.
Default: Yes

- **Aggregate Current Charges**
  Specifies how to present current charges on an invoice. Current charges apply only to the current period as defined by the period start and end dates in the Accounting Profile.

  - **Yes**
    Displays the total of the current charges on one line.

  - **No**
    Displays the current charges individually on multiple lines.

  This setting is similar to Aggregate Advanced Charges, but it applies to current charges instead.
  Default: Yes

- **Allow No Activity Invoices**
  Specifies whether to generate invoices for accounts with no charges.

  - **Yes**
    Generates invoices for *all* accounts, including accounts with no charges.

  - **No**
    Generates invoices *only* for accounts with charges.

  Default: No

- **Bill Run Capacity**
  Specifies the number of accounts to process for transaction and invoice generation until a commit is performed and all processing is persisted.
  The larger the value, the more server memory is required and the faster the invoices are processed. The smaller the value, the less server memory is required, and the slower the invoices are processed.
  Default: 100

- **Exclude Invoice Item**
  Specifies whether to include a chargeable item on an invoice if the quantity, unit cost, or both is 0. Select from the following options:

  - **Always Include**
    Invoices all items, regardless of the value for quantity and unit cost.

  - **Where Quantity is 0**
    Exclude items when the quantity is 0.

  - **Where Rate is 0**
    Exclude items when the unit cost is 0.

  - **Where Quantity and Rate are 0**
    Excludes items when *both* the quantity and unit cost are 0.

- **Where Quantity or Rate is 00**
  Excludes items where *either* the quantity or unit cost is 0.

Default: Always Include

- **Uninvoiced Transactions**
  Specifies whether to include a transaction on an invoice. The decision is based on a comparison of the transaction date with the period start date and end date on the Accounting Profile of the account.
  Select from the following options:

  - **Include All Uninvoiced Transactions**
    Includes all transactions that have not yet been invoiced, regardless of transaction date.

  - **Exclude Past Uninvoiced Transactions**
    Does not include transactions whose date is before the period start date, even if the transactions are not yet invoiced.

  - **Exclude Future Uninvoiced Transactions**
    Does not include transactions whose date is after the period end date, even if the transactions are not yet invoiced.

  - **Exclude Both Past and Future Uninvoiced Transactions**
    Does not include transactions whose date matches one of the following options, even if the transactions are not yet invoiced:

    - Before the period start date

    - After the period end date

    Both of these dates are outside the current period.

  Default: Include All Uninvoiced Transactions

- **Invoice From Address**
  Specifies the address for the "From" field on the invoice.
  Select from the following options: Service Provider Address and Business Unit Address.
  Business Unit Address is available for a child business unit only.
  Default: Service Provider Address

- **Invoice Generation Email Attachment Type**
  Specifies the delivery mechanism for the invoice when emails about invoices are sent.
  Select from the following options:

  - **Attachment**
    Includes the invoice as an attachment in the email. The format is specified in the Invoice Output Type setting.

  - **Inline**
    Includes the invoice in HTML format in the text of the email.

  - **Link**
    Includes a link to the invoice in the text of the email.

Default: Attachment

- **Invoice Generation Email Body Message**
  Specifies the body text for emails about invoices.
  You can specify both literal text and dynamically substituted values.
  The syntax for dynamically substituted values follows:

  - ***$object_name.variable_name$***
    Specifies the name of the variable.
    You can specify the following values:

    - "statements" object:
      statement_label - The label of the account plus an invoice statement ID, such as "acnt1: 10012"
      period_from - The Accounting Profile Period Start Date of the account
      period_to - The Accounting Profile Period End Date of the account
      due_date - The due date of the invoice

    - "billing_account" object:
      account_label - The label of the account, such as "acnt1"

  Limit: 1024 characters
  Default: Invoice Generated for $statements.statement_label$ for $statements.period_from$ - $statements.period_to$

- **Invoice Generation Email CC**
  Specifies the addresses of carbon copy (CC) recipients of emails about invoices.
  You can specify multiple email addresses. Separate each email address with a semi-colon.
  Limit: 1024 characters
  Default: EMPTY

- **Invoice Generation Email From**
  Specifies the email address that sends emails about invoices.
  Select from the following options:

  - **User Defined**
    Specifies a custom email address that you enter manually. If you select this option but enter no email address, this setting changes to the literal value of EMPTY.

  - **Service Provider Email**
    Specifies the email address of the service provider business unit.

  - **System**
    Specifies that the Catalog system determines which one of the following email addresses to use: the Services Group or the super business unit.

  Default: Service Provider Email

- **Invoice Generation Email Subject**
  Specifies the text for the subject line of emails about invoices.
  You can specify both literal text and dynamically substituted values.
  The syntax for dynamically substituted values is the same as the Invoice Generation Email Body Message setting. That setting is described earlier in this topic.

Limits: 1024 characters
Default: Invoice: $statements.statement_label$ processed for account: $billing_account.account_label$, Due date: $statements.due_date$

- **Invoice Generation Email To**
  Specifies the primary recipient of emails about invoices.
  Select from the following options:

  - **System**
    Uses the email address of the Send Invoice To field in the Accounting Profile of the account.

  - **User Defined**
    Specifies a custom email address that you enter manually. If you select this option but enter no email address, this setting changes to the literal value of EMPTY.
    You can specify multiple email addresses. Separate each email address with a semi-colon.

  Default: System

- **Invoice History Email Attachment Type**
  Specifies the delivery mechanism for the invoice when you send emails from the Invoice History page.
  Select from the following options:

  - **Attachment**
    Includes the invoice as an attachment in the email. The format is specified in the Invoice Output Type setting.

  - **Inline**
    Includes the invoice in HTML format in the text of the email.

  - **Link**
    Includes a link to the invoice in the text of the email.

  Default: Attachment

- **Invoice History Email Body Message**
  Specifies the body text for emails about invoices, when you send these emails from the Invoice History page.
  You can specify both literal text and dynamically substituted values.
  The syntax for dynamically substituted values follows:

  - **$*object_name*.*variable_name*$**
    Specifies the name of the variable.

  You can specify the same variables as for the Invoice Generation Email Subject setting.
  In addition, you can specify the following variables:

  - "invoice_history" object:
    account_label - The label of the account

Limit: 1024 characters
Default: Invoices Generated During $invoice_history.start_date$ - $invoice_history.end_date$ total number of invoices: $invoice_history.num_invoices$ number of phases processed = $invoice_history.phases$

- **Invoice History Email CC**
  Specifies the addresses of carbon copy (CC) recipients of emails from the Invoice History page. You can specify multiple email addresses. Separate each email address with a semi-colon.
  Limit: 1024 characters
  Default: EMPTY

- **Invoice History Email From**
  Specifies the email address that sends emails about invoice history.
  Select from the following options:

  - **User Defined**
    Specifies a custom email address that you enter manually. If you select this option but you enter no email address, this setting changes to the literal value of EMPTY.

  - **Service Provider Email**
    Specifies the email address of the service provider business unit.

  - **System**

  Specifies that the Catalog system determines which one of the following email addresses to use: the Services Group or the super business unit.
  Default: System

- **Invoice History Email Subject**
  Specifies the text for the subject of emails from the Invoice History page.
  You can specify both literal text and dynamically substituted values.
  The syntax for dynamically substituted values follows:

  - ***$object_name.variable_name$***
    Specifies the name of the variable.
    You can specify the same variables as for the Invoice Generation Email Subject setting.
    In addition, you can specify the following variables:

    - "invoice_history" object:
      account_label - The label of the account

  Limit: 1024 characters
  Default: Invoices Generated During $invoice_history.start_date$ - $invoice_history.end_date$

- **Invoice History Email To**
  Specifies the primary recipient email addresses when emails are sent from the Invoice History page. You can specify multiple email addresses, which are separated by a semi-colon.
  Limit: 1024 characters
  Default: EMPTY

- **Invoice Email Location**
  Specifies a directory path on the local file system. This path stores invoices for the account when its Accounting Profile Invoice Method is set to Email.
  Each invoice file name includes the account label and invoice statement ID.
  For example, you could specify the following setting for a Windows environment:
  USM_HOME\accounting\outbox\email.
  Limit: 1024 characters
  Default: EMPTY

- **Invoice Fax Location**
  Specifies a directory path on the local file system. This path stores invoices for the account when its Accounting Profile Invoice Method is set to Fax.
  Limit: 1024 characters
  Default: EMPTY

- **Invoice Postal Location**
  Specifies a directory path on the local file system. This path stores invoices for the account when its Accounting Profile Invoice Method is set to Postal.
  Limit: 1024 characters
  Default: EMPTY

- **Invoice Printer Location**
  Specifies a directory path on the local file system. This path stores invoices for the account when its Accounting Profile Invoice Method is set to Printer.
  Limit: 1024 characters
  Default: EMPTY

- **Invoice Output Type**
  Specifies the format to use when saving invoices as files.
  Select from the following options:

  - HTML
  - CSV
  - XML
  - HTML and CSV
  - HTML and XML

  The file format that you select is used for the previous two settings, Invoice Postal Location and Invoice Printer Location.
  Default: HTML

- **Invoice Style**
  Specifies the style to use for viewing an invoice through the user interface.
  Select from the following options:

  - Style 1 - One option for invoice format.
  - Style 2 - Another option for invoice format.

Default: Style 1

- **Invoice URL**
  Specifies an absolute URL path to the location that stores invoices for use by the Accounting, Invoices, Batch Printing menu option.
  Limit: 1024 characters
  Default: EMPTY

- **Output Invoices**
  Specifies whether to store the invoices for the account on the server file system, as follows:
  With either setting, you can view invoices through the user interface.

  - **Yes**
    Stores the invoices on the server file system. Depending on the Invoice Method setting, the invoices are stored in the locations that are indicated in the various "location" configuration settings.

  - **No**
    Does not store invoices on the server file system.

  Default: No

- **Payment Response**
  Specifies the text to print on an invoice when payment is posted.
  Limit: 1024 characters
  Default: Payment received - Thank you

- **Pro Rate Batch**
  Specifies whether to prorate invoice charges if the service start date does not align with the Accounting Profile period of the account.

  - **No**
    Charges the invoice *only* after a full charge period has passed.

  - **Yes**
    Prorates the charges.

  For example, suppose that both of the following options are true:

  - This setting is Yes

  - The charge and the Accounting Profile period of the account are both monthly

  In this example, if you generate an invoice half way through the billing period, only half the charge appears on the invoice.
  Default: Yes

- **Pro Rate Online**
  Specifies the same options as the previous setting (Pro Rate Batch), except that this setting applies to invoices that you view through the user interface.
  Default: Yes

- **Use Time (requires restart)**
  Specifies whether to use the time portion of a transaction date and time stamp when determining the period for which to bill a transaction.
  Default: Yes

Invoice Methods

As part of setting accounting configuration options (see page 1461), you specify the Invoice Methods settings. These settings specify which methods of sending invoices are available on the Accounting Profile of the account.

- **Email**
  Specifies whether users can send invoices through email. If this option is set to Yes, Email appears in the list of options for specifying the delivery mechanism.
  Default: Yes

- **Fax**
  Specifies whether users can send invoices through fax. If this option is set to Yes, Fax appears in the list of options for specifying the delivery mechanism.
  Default: Yes

- **Postal**
  Specifies whether users can send invoices through the postal service. If this option is set to Yes, Postal appears in the list of options for specifying the delivery mechanism.
  Default: Yes

- **Printer**
  Specifies whether users can send an invoice by printing. If this option is set to Yes, Printer appears in the list of options for specifying the delivery mechanism\.
  Default: Yes

Payment Methods

As part of setting accounting configuration options (see page 1461), you specify the Payment Methods settings. These settings specify which payment methods are available for applying a payment to an invoice.

- **Cash**
  Specifies whether Cash is a payment option for an invoice.
  Default: Yes

- **Check**
  Specifies whether Check is a payment option for an invoice.
  Default: Yes

- **Coupon**
  Specifies whether Coupon is a payment option for an invoice.
  Default: No

- **Credit Card**
  Specifies whether Credit Card is a payment option for an invoice.
  Default: Yes

- **Direct**
  Specifies whether Direct is a payment option for an invoice.
  Default: No

- **Tip**
  Specifies whether Tip is a payment option for an invoice.
  Default: No

Subscription Configuration

As part of setting accounting configuration options (see page 1461), you specify the Subscription Configuration settings. These settings specify how the Catalog system handles subscriptions.

- **Default Subscribe State**
  Specifies the status to which the selected service options are set when an account is subscribed to a service.

  - Completed
  - Pending

  Default: Completed

- **Default Cancellation State**
  Specifies the status to which the selected service options are set when the subscription of an account to a service is cancelled.
  Select from the following options:

  - Cancel - Charges for the current billing period do not appear on the next invoice.
  - Pending Cancellation - Charges for the current billing period appear on the next invoice, at which point the status is changed to Cancelled.

  Default: Pending Cancellation

- **Default Subscription Page**
  Specifies the initial page that is displayed when the Subscriptions tab is selected.
  Select from the following options:

  - Create New Subscriptions - Show catalog of services to which the account can subscribe.
  - Existing Subscriptions - Show services to which the account is subscribed.

  Default: Create New Subscriptions

- **Allow Instance Names**
  Specifies whether a name can be associated with a subscription instance.
  If this option is set to Yes, when an account is subscribed to a service, you can add some text to the subscription to name the instance.
  Default: No

- **Enable Subscription Notes**
  Specifies whether a note can be associated with a subscription instance.
  If this option is set to Yes, when an account is subscribed to a service, you can add notes to the subscription.
  This setting is available for the service provider business unit only, and it applies to all business units.
  Default: No

Set Administration Configuration Options

To meet the requirements of your organization, you can customize several administration configuration options. The options include those for integrations, portals, request SLAs, authentication, and others.

Follow these steps:

1. Log in as a user with the Service Delivery Administrator role. Updates to these options apply to the *entire* system. You *cannot* specify different administration configuration options for different business units.
2. Click Administration, Configuration.
3. Click the link for the category of options that you want to update:
   - Integration-specific options (see page 1478)
   - Event Manager (see page 1478)
   - File Store Information (see page 1479)
   - Mail Server (see page 1479)
   - Portal (see page 1480)
   - Request SLA (see page 1481)
   - Rule Engine (see page 1481)
   - Server Information (see page 1481)
   - Single Sign On Authentication (see page 1482)
   - System Information (see page 1483)
   - User Default (see page 1484)
4. View the options for the category, and click the Modify icon for the option that you want to update.
5. Update the setting as required and click Update Configuration.

6. Repeat the previous steps for each administration configuration option that you want to update.

You have set the administration configuration options. These settings apply to the children of the business unit that you updated, according to the inheritance of configuration settings through the business unit hierarchy (see page 1447).

Integration-Specific Options

If you are integrating CA Service Catalog with any of the following products, set the related configuration parameters to ensure CA Service Catalog and the integrating product work together correctly. This task is part of setting the administration configuration options (see page 1477).

- CA APM
- CA Business Intelligence

> **Note:** CA Business Intelligence packages and delivers BusinessObjects Enterprise. So, you use these CA Business Intelligence parameters to configure the integration of CA Service Catalog with BusinessObjects Enterprise.

- CMDB
- CMDB Visualizer
- CA Process Automation
- CA Business Service Insight
- CA Service Desk Manager
- Reservation Manager

> **Note:** For more information about setting these parameters, see the relevant sections in Integrating CA Service Catalog (see page 3425).

Event Manager

As part of setting the administration configuration options (see page 1477), you configure the following parameters for the Event Manager. The Event Manager processes events. An event occurs when one or more conditions that are specified in a rule are met.

For more information about events, rules, and actions, see the Manage Events-Rules-Actions (see page 3040) section.

- **Email From**
  Sends an email *from* this address if the Event Manager has a problem.
  Default: spadmin@*serviceprovider*, where "*serviceprovider*" is the root business unit that is specified during installation.

- **Email To**
  Sends an email *to* this address if the Event Manager has a problem.
  Default: spadmin@*serviceprovider*, where *serviceprovider* is the root business unit that is specified during installation.

- **Audit Trail Level**
  Indicates the level of detail that is logged in the audit trail tables. Typically, system performance decreases as the level of log detail increases. Conversely, system performance typically increases as the level of log detail decreases.
  Select one of the following options:

  - **No Audit Trail**
    Stores no information about the event in the database.

  - **Only Object ID**
    Stores the event information, including the object ID, in the usm_system_change table. This option stores only minimal information.

  - **Include Attributes**
    Stores the event information, including the object ID, in the usm_system_change table. This option stores detailed old and new values for the object attributes in the usm_system_change_detail table.

  - **Include Multiple Attributes**
    Stores the event information, including the object ID, in the usm_system_change table. This option stores detailed old and new values for the object attributes in the usm_system_change_detail table. If any attributes have multiple values, the old and new values are stored in the usm_system_change_detail_ext table.
    Default: Include Attributes.

File Store Information

As part of setting the administration configuration options (see page 1477), you configure the following parameter for the File Store Information. You can set up a custom location for shared files. Having a common location improves the accuracy and efficiency of sharing files between computers.

- **File Store Location**
  Specifies the UNC path name of the shared drive.
  Default: USM_HOME\filestore

Mail Server

Important! Any mail-related settings in custom rule actions override these mail server parameters. For more information about events, rules, and actions, see the section Manage Events-Rules-Actions (see page 3040).

As part of setting the administration configuration options (see page 1477), you configure the following parameters for the mail server. The mail server sends automated messages from CA Service Catalog. These settings apply to the children of the business unit that you updated, according to the inheritance of configuration settings through the business unit hierarchy (see page 1447).

- **From Address**
  Specifies the address that emails are sent from.
- **Host Name**
  Specifies the host name of the mail server.
- **Port Number**
  Specifies the port number on the mail server that listens for incoming calls from CA Service Catalog.
- **User ID**
  Specifies the user ID for accessing the mail server.
- **User Password**
  Specifies the password for accessing the mail server.

Note: Specify these parameters and click the Test button to verify the connection between CA Service Catalog and the mail server. If the test fails, review the view.log file in the USM_HOME\logs folder.

Portal

As part of setting the administration configuration options (see page 1477), you configure the following parameters for the Portal. The Portal settings specify how the dashboard library and document entries are made available.

- **Allow New Document Domain Namespaces**
  Specifies whether business units can have their own document name spaces. If this parameter is set to Yes, the Add A New Business Unit page contains the "Create Document Namespace" check box.
  If a business unit has its own document namespace, you can segregate documents in separate business units. This segregation allows only users in that business unit to have access to the document.
  Default: Yes
- **Allow New Library Namespaces**
  Specifies whether business units can have their own library name spaces.
  If this parameter is set to Yes, the Add A New Business Unit page contains the "Create Dashboard Library Namespace" check box.
  If a business unit has its own library namespace, you can segregate dashboard library content. This segregation allows only users in that business unit have access to the library content when they add a dashboard.
  Default: Yes

- **Show Resource Tree**
  Specifies whether the Resource Explorer appears in the dashboard library tree.
  If this parameter is set to Yes, the Resource Explorer appears in the dashboard library tree. This option applies *only* if CA Service Catalog is integrated with CA Business Service Insight.
  Default: Yes

Request SLA Processor

As part of setting the administration configuration options (see page 1477), you configure the following parameter for the request SLA processor. These settings specify how the Catalog system processes request SLAs.

For information about setting up request SLA processing, see the Manage Request SLAs (see page 2168) section .

- **Maximum Delay for Request SLA Alerts**
  Specifies how frequently the request SLA processor checks for SLA warnings or violations. This setting applies to all SLA instances managed by a Catalog Component computer.
  To minimize possible delays in SLA processing time when a Catalog Component clustered computer fails, configure this parameter. Therefore, set a smaller interval, such as one hour, to receive SLA warnings and violations quickly. Otherwise, set a larger interval, for example, one day, to receive them when the failed clustered computer is restored.

Rule Engine

As part of setting the administration configuration options (see page 1477), you configure the following parameter for the Rule Engine. Administrators use rules to define actions to take when a specific event occurs. These actions can be running scripts or Java programs, sending emails, and so forth. The rule engine manages the execution of the actions.

For information about events, rules, and actions, see the Manage Events-Rules-Actions (see page 3040 section.

- **Action Default Timeout (in seconds)**
  Specifies the default timeout value in seconds for rule actions.
  Default: 300

Server Information

As part of setting the administration configuration options (see page 1477), you configure the following parameters for the Catalog Component server. These settings apply *only* when you configure Catalog Component for use with HTTPS or for use as a load balancer in clustering. Otherwise, Catalog Component is configured automatically and the following parameters do *not* apply.

- **Enable HTTPS**
  Defines whether CA Service Catalog uses HTTPS when communicating with this Catalog Component computer.
  Default: No

- **Host Name**
  Specifies the host name accessible to catalog users, typically one of the following host names:

- The Catalog Component computer
- The load balancer computer (applies if you are clustering).
- The computer that redirects catalog users (applies if you are using DNS aliases for redirection).

- **Port Number**
  Specifies the port number for communicating with the host named in the previous parameter.

Important! If you use clustering, replace the host name and port number in the Server Information section with the host name and port number of the load balancer. If you use DNS aliases for redirection, replace the host name and port number in the Server Information section with the host name and port number of the computer that redirects catalog users.

Single Sign On Authentication

You configure the following single sign-on authentication parameters.

- **Allow Login with GET**
  Specifies whether users can log in using an HTTP GET request.
- **External Authentication Parameters**

  The external authentication parameters follow. To enable external authentication of users, configure these parameter values to match the external application that you are using.

  - **Artifact Name**
    Specifies the name of the cookie, header, or request parameter that contains the authenticated user ID. This name varies according to the external authentication system and your site-specific implementation.
    The default value is sm-user.
    For example, if you are using CA SiteMinder, select Header as the authentication type and sm-user as the artifact name. With this configuration, CA Service Catalog checks the header named sm-user whose value is the userid.
    When the Artifact Type is request, the artifact name is ignored.
  - **Artifact Type**
    Specifies the mechanism that the external application uses to send the authenticated user ID to CA Service Catalog, as follows:
    - Cookie: Cookie in the request
    - Header: Header in the request
    - Parameter: request parameter
    - Request: request user

- **Bypass Nodes**
  Specifies the GUI nodes that you want the authentication check to skip. These GUI nodes typically do not require the user to log in.
  Examples include the following: icguinode.login, icguinode.logout, iclaunchpad.launch, icguinode.changepwdlockout, and icguinode.lockout.

- **Login Page**
  Specifies the page that displays to the user when either the artifact type is set incorrectly or CA Service Catalog does not find an authenticated user.
  An example is wpf?Node=icguinode.login.

- **Single Sign-on Type**
  Specifies *one* of the following options:

  - Disabled: Specifies that CA Service Catalog does *not* use single sign-on.
  - Artifact Based Single Sign-on: Configures CA Service Catalog to use single sign-on based on the artifacts specified on this page.
  - NTLM (NT LAN Manager): Configures CA Service Catalog to use single sign-on based on Windows NT authentication.

System Information

As part of setting the administration configuration options (see page 1477), you configure the following settings that are related to common multi-tenant administration for CA Service Catalog business units:

Important! These settings apply *only* if you are *both* integrating CA Service Catalog with CA Service Desk Manager *and* using common multi-tenant administration of CA Service Catalog business units. For more information about setting up common multi-tenant administration, see the section Configure Common Tenant Administration (see page 1397).

- **Terms Of Usage Prompt Enabled**
  Specifies that common tenants in CA Service Catalog must implement the terms of use (if any) that are created and maintained in CA Service Desk Manager. The specific effect on users attempting to log in to CA Service Catalog depends on the terms of use settings that are specified in CA Service Desk Manager.
  If this setting is Yes, the users attempting to log in to CA Service Catalog receive the terms of use prompt. If the users do not accept the terms of use, they cannot access CA Service Catalog.
  If this setting is No, the users attempting to log in to CA Service Catalog are not prompted with terms of use, regardless of the terms of use settings that are specified in CA Service Desk Manager.

- **Common Multi-Tenant Administration Enabled**
  Specifies whether you manage CA Service Catalog business units with the common multi-tenant administration framework supplied through CA Service Desk Manager.
  When this option is set to No, you manage CA Service Catalog business units directly through CA Service Catalog, and these business units are not synchronized with CA Service Desk Manager.

When this option is set to Yes, you cannot manage CA Service Catalog business units directly through CA Service Catalog, except for CA Service Catalog-specific attributes. You use the tenant administration tool of CA Service Desk Manager to manage all business units of CA Service Catalog and CA Service Desk Manager and their common attributes.
You cannot set this option to Yes unless the Common Multi-Tenancy Model option is set to Yes.

- **Common Tenant Data Synchronized (read-only)**
  Specifies whether the CA Service Catalog tenant (business unit) structure is synchronized with the tenant structure of CA Service Desk Manager.
  CA Service Catalog sets this option to Yes when all of the following conditions are met:

  - CA Service Desk Manager is installed.
  - The common multi-tenancy merge utility has run successfully.
  - Since the utility was last run, no business unit has been created, deleted, or had a change in a common attribute through CA Service Catalog directly.

  Conversely, CA Service Catalog sets this option to No when one or more of the following conditions exist:

  - The common multi-tenancy merge utility has not run successfully.
  - Since the utility was last run, one or more business units have been created, deleted, or had a change in a common attribute through CA Service Catalog directly.

User Default

As part of setting the administration configuration options (see page 1477), you configure the following settings that are related to users, roles, searches, and sessions:

- **CA EEM Max Search Size**
  Defines the maximum number of users that are queried during searches in CA EEM.
- **Access Control: Allow Request Auto-Delegation via User Management**
  Defines which user roles are able to view and set auto-delegation for other users. Typically, administrator roles use this ability to set auto-delegation for users who are unable to set it for themselves. Examples of such employees:

  - Users who suddenly became unavailable due to emergency.
  - Users who left for a long absence without setting their own auto-delegation.
  - Users whose roles have no rights to set their own auto-delegation.

  The default value is the Service Delivery Administrator user role.
- **Access Control: Allow Request Auto-Delegation via User Profile**
  Defines which user roles have the Request Auto-Delegation setting appear on their User Profile window. Users with these roles can view and optionally configure this setting for themselves. The default value is all user roles, so that all users can change at minimum their own auto-delegation settings.

- **User Default Role**
  Defines the default business-unit role that is assigned to a user when an administrator creates or edits the user.
  If both of the following conditions are true, the Catalog system assigns the default role to the user logging in:

  - The user has an MDB record that is created by another product.
  - That MDB record has never been edited through CA Service Catalog.

  A change of this setting requires a restart of the Catalog Component service to take effect.
  The default value of this setting depends on the products installed:

  - If CA Service Catalog is installed, the default value for this setting is Catalog User.
  - If only Accounting Component is installed, the default value for this setting is End User.

- **User Search Scope**
  Defines how the scope of the "search user" functionality works for the Catalog User and End User roles. "Search user" functionality for these roles is available in the following areas:

  - When emailing a request, users can populate the To, CC, and BCC fields by searching from a list of users or accounts.
  - When editing the cart or a request, if the logged in user can create requests for other users or accounts (proxy requests), the user can override the Requested For value by choosing from a list of users or accounts.

Note: The scope of "search account" functionality for Catalog End Users and End Users includes *only* accounts in the same business unit as the logged in user. This scope does *not* include child business units.

Select one of the following options:

- Enterprise - All users who have a User ID specified without regard to the role of the user. This setting is suitable for enterprise customers where business units represent departments in one company.
  The scope of the "search user" functionality works as follows:

  - A user who can change the Requested For user for a cart or a request can select from all users.

  When a request is emailed, the list of users includes all users.

- Business Unit - All users who have a user ID and a role in the business unit of the logged in user. This setting is suitable for customers whose business units represent separate companies or departments within those companies.
  The scope of the "search user" functionality works as follows:

- A user who can change the Requested For user for a cart or a request can select from users who have a role in the same business unit as the logged in user.
- When a request is emailed, the list of users includes only users who have a role in the same business unit as the logged in user.

Default: Enterprise

- **Session Timeout**
  Defines the number of minutes of inactivity after which users are logged out. For the change to take effect, recycle the Windows service named CA Service Catalog.

Administering CA Service Catalog

This section contains the following articles:

Migrate Data Between CA Service Catalog Systems using the Import Export Utility

Administrators can use the Import Export utility to export CA Service Catalog data between two CA Service Catalog computers. This migration is primarily intended for either:

- Moving data from test to production, when both computers are running the same release of CA Service Catalog.
- Moving data from a computer running the previous release of CA Service Catalog to a computer running a newer release of CA Service Catalog.

Follow these steps:

Step 1 - Verify the Prerequisites for Data Migration using the Import Export Utility

Before you begin to migrate data between the CA Service Catalog systems:

- Verify that CA Service Catalog is installed and running.

- Integrate CA Service Catalog with CA Service Desk Manager or CA CMDB, to export services that have CMDB CI associations.
- Understand the different object type attributes (see page 1488) that can be exported or imported.

Step 2 - Export the Data

The Import Export utility exports the data in a proprietary XML format. The same XML format must be used in the data files when importing. You can determine the correct XML formats for each object type by examining an exported XML file.

Follow these steps:

1. Click Administration, Tools.
2. Select Import Export Utility from the left pane.
3. Select Export action in the Action and Object type.
4. In the Object Type drop-down list select the object for which, you want to export the data.
5. Specify the attributes (see page 1488) for the selected object.
6. Click Start Export.
   The exported data for the selected object type is saved as an XML file in the format: *ixutil_{object_name}_{YYYYMMDD}_{HHMMSS}.*xml.
   You have successfully exported the data between CA Service Catalog systems.

Step 3 - Import the Data

You can use the Import Export utility to migrate new and updated objects from one computer to another. All the object types that are exported can be imported.

Follow these steps:

1. Click Administration, Tools.
2. Select Import Export Utility from the left pane.
3. Select Import action in the Action and Object type.
4. Select the object type that you want to import in the Object Type drop-down list.
5. (Optional) Select Quick Import check box, if you do not want to specify any other attributes as inputs to import.
6. Specify the attributes (see page 1488) for the selected object, if you do not want to perform a Quick Import.
7. Click Browse and select the xml file as input for the selected object type.

Note: For the Service Offering object type, select the exported zip file, if, the Include Translations option was selected during import.

8. Click Start Import.
   The file is imported to the business unit specified in the file.

Important! If you export report data objects that are based external data sources, verify that they are imported correctly on the target computer. To verify, review the IXUtil log file in the USM_HOME\logs\install folder on the target computer. If necessary, recreate these report data objects on the target computer.

Note: The Import Export utility does *not* import *images* of offerings. The import fails because of the variation of the image file path names on the source and target computers. To retain such images, copy and paste them manually, after the initial migration is complete.

You have successfully imported the object type.

Step 4 - Verify the Exported or Imported Data

You can verify the imported data through the corresponding objects section in CA Service Catalog, or by querying the database.

Follow these steps:

1. Log in to CA Service Catalog on the computer where you imported the policies. If applicable, log in to the business unit to which you exported the policy or policies.
2. Click Catalog, Policies.
3. Expand the policy folders.
4. Verify that the CA Service Catalog imported the policy or policies as you want. Verify if the import was successful in Forms, Service Offerings, Events, Report Data, Business Units, and Configurations in Administration, Accounting, and Catalog.

Object Type Attributes

This article contains the following topics:

- Report Data Attributes (see page 1490)
- Service Offerings Attributes (see page 1491)

Depending on the selected object type to export or import, specify the information in the fields available for each attribute.

Business Unit Attribute

This section describes the business unit attribute.

- **Business Unit ID**
  Specifies the business unit login ID, the name that is used to log in to the business unit. When you use the business unit id attribute while exporting, verify that the business unit specified exists in the source. For importing a business unit, the parent business unit must exist in the target system. If it does not exist, the business unit being imported becomes a child business unit of the root business unit.
  When you import a business unit that has one or more sub-business units, first import all the business units. Then import all the accounts.

Configuration Attributes

This section describes the configuration attributes.

- **Group Name**
  Specifies the configurations that are grouped under various categories. Many groups are configured in the Administration Configurations, Accounting Configurations, Catalog Configurations, and Custom Configurations. The Configuration name to be provided as input in the Group Name text box is displayed in brackets beside the configuration name in the header section. You can import or export multiple groups at the same time. To export multiple groups, separate the names with commas.
  For example, to export a CMDB configuration group, provide the input as CMDB. All the configurations under this group are exported or imported. Leave this field blank to export all the configurations irrespective of the group.

- **Business Unit ID**
  Specifies the configurations of a group of Business Units that are exported or imported as a group. Leave this field blank to export all the configurations of the groups irrespective of the Business Unit.

Event Attributes

This section describes the event attributes.

- **Event Name**
  Specifies the name of the event as seen in the Event Type list. This option is used to export and import an event information about the specified event type.

- **Rule Name**
  Specifies the name of the rule as seen in the Rule Type list. This option is used to export and import a rule information about the specified event type.

- **Action Name**
  Specifies the name of the action as seen in the Action Type list. This option is used to export and import action information about the specified event type.

Form Attributes

The form attributes export either an individual Form Designer form or all Form Designer forms from a specified folder.

- **Form Designer Folder Name**
  Exports all the Form Designer forms from a specific folder.

- **Form Designer Form Name**
  Exports an individual Form Designer form.

  Note: For Form Designer forms and folders, use only the form name or folder name; path name is not applicable.

- **Business Unit ID**
  Specifies the business unit login ID, the name that is used to log in to the business unit. Use this option to export all forms in a domain. If you omit this option, IXUtil exports all forms in all domains.
  For example, if the business unit ID is subBud, specify subBud in the text box.

Policy Attributes

This section describes the policy attributes.

- **Folder Name**
  Specifies the folder name. To export multiple folders, separate the names with commas.

- **Policy Name**
  Specifies the policy name. To export multiple policies, separate the names with commas.

- **Business Unit ID**
  Specifies the business unit login id that contains the policies being exported. If you are exporting all policies in all the business units, omit this attribute. Otherwise, this attribute is required.
  To import the policy files, optionally specify this parameter to import all the policies into a single business unit.
  If the specified business unit does not exist, the policies that are assigned to it are instead assigned to the root business unit.

Report Data Attributes

This section describes the report data attributes.

- **Folder Name**
  Specfies the folder name. To export multiple folders, separate the names with a comma.

- **ID**
  Specifies an identification of the data objects. To export multiple data objects, separate the id's with a comma.

Service Offerings Attributes

This section describes the service offering attributes.

- **Object Classifier**
  Specifies whether the folders or Service offerings are chosen specifically.

- **Business Unit ID**
  Specifies the business unit login id that contains the folders or service offerings being exported. To export all folders or service offerings in all business units, omit this attribute; otherwise, this attribute is required.
  To import folders or service offerings files, you can specify this parameter to import all the folders or service offerings into a single business unit.
  If the specified business unit does not exist, the folders or service offerings that is assigned to it is instead assigned to the root business unit.

- **Include Forms**
  Associates export of the included forms, with the export of service offerings.

- **Include CMDB CI Mapping**
  Specifies that the associations between CA Service Catalog services and CMDB configuration items are exported.
  This option applies *only* when you have integrated CA Service Catalog with CMDB.

  Important! Verify that the CMDB configuration items are already present on the target computer *before* you export. Also verify that the UUIDs of these configuration items are the same on both the source and target computers. For more information about how to copy the configuration items and verify the UUIDs, see your CMDB documentation.

- **Include Permissions**
  Exports or Imports the permissions for each service (offering) while exporting or importing services through service offerings.

- **Include Request SLA**
  Exports or imports the associated request SLAs for each service (offering) while exporting or importing services.

- **Include Service Hour**
  Exports or imports the associated service hours (outage calendars and business hours) for each service (offering) while exporting or importing services through service offerings.

- **Include Resource Type**
  Exports or Imports the resource type that is associated with the service (offering).

- **Include Application Metric**
  Exports or Imports the application and its metric, along with the definition of the service that is associated with the Application Rate item.

- **Include Associated Policies and Actions**
  Exports or imports the associated policies and actions for each service (offering) while exporting or importing services through service offerings.

- **Include Translations**
  Creates the output as a zip file instead of xml file during export. The zip file includes the default properties file associated with the xml file.
  During Import, if you select this option, provide the zip file as input (instead of single xml file). The zip file internally must contain the properties files corresponding to different locales with the xml file.

Archive and Purge Historical Data

Administrators can archive and purge historical data concerning requests and audits from the CA Service Catalog database. Purging historical data regularly helps improve the performance of CA Service Catalog and the database.

Important! Once you archive the data, you cannot restore the data to production tables.

Follow these steps:

1. Step 1 - Complete the Prerequisites (see page 1492)
2. Step 2 - Prepare the MDB for Archive and Purge for the First Time (see page 1493)
3. Step 3 - Archive the Data (see page 1493)
4. Step 4 - Purge the Data (see page 1495)

Step 1 - Complete the Prerequisites

Complete these prerequisites so that you can archive and purge data successfully.

Follow these steps:

1. Understand the database-related terms that are used in this scenario, as follows:
   When you install CA Service Catalog, you install the Catalog database. The Catalog database includes the following tables:

   - The CA Management Database (MDB) tables that apply to CA Service Catalog. The names of such tables typically begin with a CA_ prefix. The MDB is the common, shared database for CA Technologies products. The MDB provides the database schema for CA Service Catalog and other CA Technologies products.

- The CA Service Catalog-specific tables. The names of such tables typically begin with a USM_ prefix.

2. Back up the Catalog database.

> **Note:** Log in to the Catalog database as the database application user; the user name is typically usm_user or mdbadmin.

3. Configure your DBMS to run with a minimal level of logging. This configuration helps expedite database processing for CA Service Catalog.

> **Note:** For more information about backup procedures and how to set logging levels, see your DBMS documentation.

4. (Optional) Stop all antivirus services.

Step 2 - Prepare the MDB

To improve the performance of archive and purge activity, prepare the Catalog database. This procedure creates an index that helps the database fetch the records faster.

> **Important!** Before you archive or purge data *for the first time*, perform this procedure *once* . Repeating this procedure is unnecessary. For information about how to prepare the MDB, see *Optimize the System Change Detail Tables* in Prepare for Upgrade (see page 580) section.

Step 3 - Archive the Data

Archiving the data moves the archival data from production tables to archival tables. After you archive the data, the data does not appear in CA Service Catalog UI.

> **Important!** The data in archival tables cannot be restored to production tables. So, ensure that you no longer need the data you want to archive.

Use one of the following procedures:

- Archive the Data in SQL Server 2008 (see page 1494)

- Archive the Data in Oracle (see page 1495)

Archive the Data in SQL Server 2008

This section describes archiving the data in SQL Server 2008.

Note: We recommend that you Use MS SQL Server Management Studio to execute the stored procedure.

Follow these steps:

1. Log in to MDB as usm_user or sa using MS SQL Server Management Studio.
2. Click New Query and enter the following code in the new query window.

```
USE [<mdb instance name>]
GO
DECLARE    @return_value int
EXEC    @return_value = [dbo].[usm_sp_archive_data]
        @p_object_type = N'< Object Type >',
        @p_date = N'<Completion Date on or before  -  yyyy-mm-dd>',
        @p_bu = N'<Business Unit>'

SELECT    'Return Value' = @return_value
GO
```

   Replace the values inside the carets (< >) with the required data.

   - **MDB Instance Name**
     Specifies the MDB instance name that CA Service Catalog uses.
   - **Object Type**
     Specifies the type of objects to archive and purge, as follows:
     - **Request**
       Archives or purges requests that are in completed status and related data (including audit data).
     - **Audit**
       Archives or purges audit entries for all objects.
   - **Completion Date on or before - yyyy-mm-dd**
     Archives or purges only requests that are completed on or before this date.
   - **Business Unit**
     Archives or purges the records of this business unit.

3. Click Execute.
   The result appears on the Messages tab.

The data is archived.

Archive the Data in Oracle

This section describes archiving the data in Oracle.

Note: We recommend that you use Oracle SQL Developer to execute the stored procedure.

Follow these steps:

1. Log in to MDB as usm_user or sa using Oracle SQL Developer.
2. Navigate to Connections, connection name, Procedures.
   a.
      - USM_SP_ARCHIVE_DATA
      - USM_SP_PURGE_DATA
3. Right-click one of the procedures and select Run.
4. In the Run PL/SQL window, replace the values inside the carets (< >) with required data.

   Note: If you are using SQLPlus on command prompt, execute the SET SERVEROUT ON statement before executing the stored procedure.

```
DECLARE
  P_OBJECT_TYPE VARCHAR2(200);
  P_DATE DATE;
  P_BU VARCHAR2(200);
BEGIN
  P_OBJECT_TYPE := '<Object Type>';
  P_DATE := '<Completion Date on or before  -  DD-MON-YYYY>';
  P_BU := '<Business Unit>';

  USM_SP_ARCHIVE_DATA(
    P_OBJECT_TYPE => P_OBJECT_TYPE,
    P_DATE => P_DATE,
    P_BU => P_BU
  );
END;
```

5. Click OK.
6. The result is displayed in the Running - Log tab.

The data is archived.

Step 4 - Purge the Data

You can purge the data to remove the archived data permanently from the database.

Follow these steps:

1. Follow the instructions in the Archive the Data procedure and replace the USM_SP_ARCHIVE_DATA stored procedure with USM_SP_PURGE_DATA procedure. When the stored procedure is successfully completed, the data is purged.

Diagnose the Health of the Product

Administrators can use the diagnostic framework to assess the health of CA Service Catalog in a clustered environment. The diagnostic framework includes web service methods, CA Remote Engineer, and the JMX client.

Follow these steps:

Step 1 - Verify the Prerequisites (see page 1496)

Step 2 - Implement the Web Service Methods (see page 1496)

Step 3 - Download and Run CA Remote Engineer (see page 1499)

Step 4 - Use JMX Client to Monitor Status (see page 1500)

Step 5 - Verify the Diagnostic Framework (see page 1500)

Step 1 - Verify the Prerequisites

Before you use the diagnostic framework, meet the following prerequisites for each component:

- For web services, a utility to connect to the web services is required. Examples include Java Client and Simple Object Access Protocol client.
- For CA Remote Engineer, the Java Runtime Environment (JRE) version for CA Service Catalog is required. This JRE version is installed automatically when you install CA Service Catalog.
- For JVM Metrics, a Java Management Extension (JMX) client is required. An example is JConsole, which is included in the Java Development Kit (JDK).

Step 2 - Implement the Web Service Methods

Web service methods help you diagnose problems by verifying the health of the connection between CA Service Catalog and its components. The following web service methods apply during the connection time between CA Service Catalog and its components:

- Web service method for CA Embedded Entitlements Manager (see page)
- Web service method for the database (see page)
- Web service method for CA Process Automation (see page 1498)

Web Service Method for CA Embedded Entitlements Manager

This web service method tests the connectivity of CA Service Catalog with Embedded Entitlements Manager server.

Web Service Method

```
long getEEMConnectionStatus()
```

Input Parameter

None

Return Parameter

Time that is taken in milliseconds by CA Service Catalog to connect to Embedded Entitlements Manager. If the connectivity fails, then an exception is displayed.

Pseudocode to use Embedded Entitlements Manager connectivity web service

```
URL endpoint1 = null;
AdministratorServiceSoapBindingStub adminStub = null;
endpoint1 =
new java.net.URL("http://catalog:8080/usm/services/AdministratorService");
adminStub = (AdministratorServiceSoapBindingStub) new AdminServiceImplService

long eemLatency;
try {
        eemLatency = adminStub.getEEMConnectionStatus();
        System.out.println("Connection successful. Time taken(milliseconds):

} catch (Exception ex) {
        System.out.println("Connection to EEM failed. " + ex.getMessage());
}
```

Web Service Method for the Database

This web service method tests the connectivity of CA Service Catalog with the database server.

Web Service Method

```
long getDBConnectionStatus()
```

Input Parameter

None

Return Parameter

Time that is taken in milliseconds by CA Service Catalog to connect to Database. If the connectivity fails, then an exception is displayed.

Pseudocode to use database connectivity web service

```
URL endpoint1 = null;
AdministratorServiceSoapBindingStub adminStub = null;
endpoint1 =
new java.net.URL("http://catalog:8080/usm/services/AdministratorService");
adminStub = (AdministratorServiceSoapBindingStub) new AdminServiceImplService
```

```
long dbLatency;
try {
        dbLatency = adminStub.getDBConnectionStatus();
        System.out.println("Connection successful. Time taken(milliseconds):

} catch (Exception ex) {
        System.out.println("Connection to database failed. " + ex.getMessage(

}
```

Web Service Method for CA Process Automation

This web service method tests two-way connectivity from CA Service Catalog to CA Process Automation.

Web Service Method

```
long getITPAMConnectionStatus(String configName, String nodeUrl)
```

Input Parameter

- **configName**
  (Optional) Defines the configuration name, which is the group name of CA Process Automation as defined in Administration, Configuration, CA Process Automation. You can remove this parameter to test the default configuration.

- **nodeURL**
  (Optional) Specifies the value for connecting from CA Process Automation to CA Service Catalog. Use this parameter in a clustered setup to verify the connection to an individual node.

  Note: To use this parameter, enable the HTTP connector port that is disabled while setting up a cluster. Disable the HTTP connector port again once the diagnosis is complete.

  If the nodeURL parameter is ignored, it picks CA Service Catalog URL configured with CA Process Automation.

For example:

```
http://host_name:port_no
```

For Secure Sockets Layer (SSL):

```
https://host_name:port_no
```

Return Parameter

Returns an array of the time in milliseconds taken to connect to CA Process Automation and CA Service Catalog respectively. A value of -1 is returned if there are exceptions while connecting.

Pseudocode to use CA Process Automation connectivity web service

```
URL endpoint1 = null;
AdministratorServiceSoapBindingStub adminStub = null;
endpoint1 =
new java.net.URL("http://catalog:8080/usm/services/AdministratorService");
```

```
adminStub = (AdministratorServiceSoapBindingStub) new AdminServiceImplService

long[] millSecs = new long[2];
try {
        millSecs = adminStub.getITPAMConnectionStatus("subton", null);
        System.out.println(String.format("Time taken for connection from Cata

} catch (Exception ex) {
        System.out.println("Connection to ITPAM failed. " + ex.getMessage());

}
```

Step 3 - Download and Run CA Remote Engineer

CA Remote Engineer collects the following product-specific critical diagnostic information and uploads it to CA Technologies:

- Log files
- Product configuration
- Hardware and software information
- A list of Microsoft installed products
- A list of CA installed products with an XML representation of the Windows registry

Note: The information in this topic is based on CA Remote Engineer Release 2.0 (the current release at publication time). If the version that you download is different, the steps can be different.

Follow these steps:

1. Download CA Remote Engineer from http://ca.com/support (http://www.ca.com/support) to the CA Service Catalog computer.
2. Unzip the utility.
3. Run the re.cmd file. This file is in the RemoteEngineer folder in the location where you unzipped the utility. This file opens a command-line utility. To use the UI-based alternative instead, run the RemoteEngineer.cmd file.
4. Follow the prompts and enter the requested information.

   Important! Specify *Service_Catalog* as the CA product name.

   For more information about the prompts, see the help file in the RemoteEngineer\help folder.

5. When prompted to verify the information that you entered, enter Yes or No.
   The utility proceeds as follows:

   - If you enter Yes, the utility collects the required information from your computer and zips it.
     Specify whether the utility must upload the zip file to CA Technologies through FTP. Alternatively, you can keep the zip file for reference or you can send to CA Technologies through another means. For example, email.

   - If you enter No, the utility aborts.

6. Close CA Remote Engineer.

Note: If you are using clustering, repeat the steps for all cluster nodes.

You have downloaded and run CA Remote Engineer.

Step 4 - JMX Client to Monitor Status

Configure the default Tomcat in CA Service Catalog to monitor the health of catalog instances with the JMX client. You can use JVM metrics to monitor the status information such as memory usage, CPU usage, and number of threads.

Note: This facility is not available if CA Service Catalog is deployed as web archive.

Follow these steps:

1. Enable the JMX remote monitoring without any security options. Use a free port of your choice.

2. Open the viewservice.conf wrapper configuration file from the *view**conf*\ location in an editor.

3. Uncomment the following three lines in the file for the JMX remote monitor.

   ```
   wrapper.java.additional.22=-Dcom.sun.management.jmxremote.port=9091
   wrapper.java.additional.23=-Dcom.sun.management.jmxremote.ssl=false
   wrapper.java.additional.24=-Dcom.sun.management.jmxremote.authenticate=false
   ```

4. Save and close the file.

Step 5 - Verify the Diagnostic Framework

The following results indicate a successful implementation of the diagnostic framework:

- The web service methods are called without any errors from the client.
- The web services run without errors.
- CA Remote Engineer collects product-specific data.
- The health of CA Service Catalog instances is monitored using the JMX client.

Deploy CA Service Catalog on a Custom Web Server

Deploying CA Service Catalog on a custom web server lets you use CA Service Catalog with another supported web server instead of the default Tomcat web server. Such a deployment also lets you use the same instance of the web server for multiple applications. For example, CA Service Catalog and CA RCM are installed on the same computer. You can use the same instance of the JBoss web server for CA Service Catalog and CA RCM. Such sharing helps your environment run more efficiently.

To deploy CA Service Catalog on the custom web server, follow this process:

- Step 1 - Verify the Prerequisites (see page 1501)
- Step 2 - Review the Limitations (see page 1502)
- Step 3 - Create the WAR File (see page 1502)
- Step 4 - Deploy the WAR File (see page 1503)
- Step 5 - Disable the Default Tomcat Instance (see page 1504)
- Step 6 - Verify the Deployment (see page 1504)

Step 1 - Verify the Prerequisites

Verify that you have met the following prerequisites, so that you can deploy the WAR file successfully:

- Install or upgrade the following applications on the same computer:
  - CA Service Catalog
    The applications with which you want to share the instance of the custom web server as CA Service Catalog, for example, CA RCM
  - The custom web server
    You can use one of the following options as your custom web server:
    - Tomcat 6 or 7
    - JBoss 5.1

    You can use either a new or existing installation of a supported web server, one of the following options:
    - A version that was supplied by installing another application. For example, CA RCM installs JBoss 5.1.
      In this case, this entire scenario applies, including the procedure to deploy the WAR file (see page).

- A stand-alone version that you installed manually. For example, you can download a supported web server from the Apache web site or the JBoss web site.
  In this case, this entire scenario applies, *except for* the procedure to deploy the WAR file. Instead, see your web server documentation for instructions to deploy the WAR file.

- Be an experienced administrator for the web server and database that you are using with CA Service Catalog.

Step 2 - Review the Limitations

Understand the following limitations:

- You *cannot* use the same custom web server for both CA Service Catalog and CA Process Automation.

- Stop, start, or restart the web server, to stop, start, or restart CA Service Catalog. You cannot stop, start, or restart CA Service Catalog by itself. However, you can individually restart other products that use the web server.
  For example, CA Service Catalog and CA RCM use the same web server. You can restart CA RCM alone, but you cannot restart CA Service Catalog alone. To restart CA Service Catalog, you restart the web server, which restarts *both* products.

- JMX Diagnosis is not available for war deployment.

Step 3 - Create the WAR File

Create the war file from CA Service Catalog.

Note: The war file that is generated from a computer must be deployed on the same computer. For example, in a clustered set-up, generate the war file on each node. Now deploy the war file on the nodes.

Follow these steps:

Click Start, Programs, CA, CA Service Catalog Command Prompt.

- (Optional) Run the following command if the custom web server is running on a port other than the port used for installation of CA Service Catalog (typically 8080).

  ```
  ant update-usm-host
  ```

  You are prompted to enter the new port number. Enter the port number of the custom web server.

- Run the following command at the command prompt:

  ```
  ant create-war
  ```

- Select one of the following options from the list:

- **Tomcat**
  Creates the war file for Tomcat 6 or 7.

- **JBoss**
  Creates the war file for JBoss 5.1

- **Other**
  Do not use this option as it is reserved for future use.
  For Tomcat, the usm.war file is generated in the USM_HOME\war folder.
  For JBoss, the usm.war folder is created.

- (Optional) Change the war file name to reflect the name of the catalog, business unit (tenant), or other meaningful entity:

  1. In Windows, manually rename the usm.war file, for example, to catalog.war or FinanceBU.war.

  2. Update the file name in the synchronization utility properties file: Specify the new name *without the .war extension* in the EIAMUser.Context=*filename* parameter in the syncuputil.properties file. This file resides in the USM_HOME folder.

  3. For example, if the new file name is FinanceBU.war, then the updated entry is EIAMUser.Context=FinanceBU.

  4. Update the file name in the administration configuration settings on the UI: Log in to CA Service Catalog as a Service Delivery administrator (for example, spadmin). Then select Administration, Configuration, Server Information, Context Path, and specify the new file name.
     The war file is created and available for deployment.

- If you are migrating or upgrading CA Service Catalog, follow these steps:

  1. Apply the patch on the installed CA Service Catalog before generating the war file.

  2. Deploy the WAR file on the same web server.

Step 4 - Deploy the WAR File

Deploy the war file so that you can use the custom web server for CA Service Catalog with other applications. Using the same web server for CA Service Catalog and other applications helps your system run more efficiently. This procedure uses CA RCM for illustration. Follow this procedure as a model for deploying your WAR file with other applications.

Follow these steps:

1. Copy the usm.war folder to the *RCM_HOME*\Server\eurekify-jboss\server\eurekify\deploy folder.
   RCM_HOME is the CA RCM installation folder; the default is C:\Program Files\CA\RCM.

2. Edit the *RCM_HOME*\Server\eurekify-jboss\bin\run.bat file, as follows:

   a. Locate the *set PATH=* statement.

b. At the end of this statement, add the path name of the database client, for example:

- The default path name for SQL 2008 R2 is C:\Program Files\Microsoft SQL Server\100\Tools\Binn.
- The default path name for Oracle 11g is C:\app\Administrator\product\11.2.0 \dbhome_1\BIN.

Troubleshooting

After you deploy the war file with CA RCM and you cannot start it, you see the following error message:

```
Provider org.apache.xalan.xsltc.trax.TransformerFactoryImpl not found" in eurekify.
log"
```

Note: The log files reside in this folder: C:\Program Files\CA\RCM\Server\eurekify-jboss\server\eurekify\log\eurekify.log.

If you are not able to start CA RCM, follow these steps:

1. If the xalan-x.x.x.jar and serilizer.jar files exist in the following folder, delete them.

   ```
   RCM_HOME\Server\eurekify-jboss\server\eurekify\deploy\eurekify.war\WEB-INF\lib
   ```

2. Copy the xalan-2.7.0.jar and serilizer.jar files from the following folder:

   ```
   RCM_HOME\Server\eurekify-jboss\server\eurekify\deploy\usm.war\WEB-INF\lib
   ```

   to the following folder:

   ```
   RCM_HOME\Server\eurekify-jboss\server\eurekify\deploy\eurekify.war\WEB-INF\lib
   ```

3. Restart the JBoss server.

Step 5 - Disable the Default Tomcat Instance

After you deploy the war file on the custom web server, stop the CA Service Catalog Windows service. Stopping the CA Service Catalog service disables the default Tomcat instance. Optionally, you can disable the service to prevent it from starting automatically.

Note: The CA Service Accounting service needs no modifications.

Step 6 - Verify the Deployment

After you deploy the custom web server, you can verify whether the deployment is successful.

Follow these steps:

1. Access the following catalog URL: http://*computer_name:port/context*

   - **Computer name**
     Defines the name of the computer on which CA Service Catalog is installed.

   - **Port**
     Defines the port number on which the web server is configured to run.

   - **Context**
     Defines the name of the war file that is created during deployment. The default is usm.war.

   If you renamed the war file, use the new name here.

2. Verify that you can access CA Service Catalog, for example, by creating, submitting, and acting on requests.
   You have verified the deployment.

Deploy and Undeploy Components from the Command Line

This article contains the following topics:

CA Service Catalog allows you to deploy and undeploy components from the command line.

Prerequisites

Fulfill the following prerequisites before deploying:

To deploy CA EEM:

The following columns must be filled in config.properties file.

- eem.configured = true
- eiam.backend =
- eiam.application =
- eiam.admin.username = EiamAdmin
- eiam.admin.password =

To deploy the MDB:

The following columns must be filled in config.properties file.

- mdb.configured = true
  Mandatory parameters for the command line interface.
- mdb.deploy.vendor =
- mdb.deploy.host =
- mdb.deploy.port =
- mdb.deploy.user =
- mdb.deploy.password =
- mdb.deploy.dbinstance =
  Mandatory parameter specific to Oracle
- mdb.deploy.connectionid =
  MDB Configuration
- mdb.deploy.dbname =
- mdb.deploy.mdbadminpwd =
- mdb.deploy.usmuser =
- mdb.deploy.usmpassword =

Note: For a SQL database, fill only the columns that are related to SQL.

To deploy a component:

- component.catalog = true
- component.accounting = true
- component.webserver = true
- application.service = true
- corporate.service = true
- facilities.service = true
- it.service = true
- network.service = true
- personnel.service = true
- project.service = true

- reservation.service =true

To run all the commands:

All the columns that are mentioned must be filled in config.properties. Note that the Oracle and SQL columns must not be filled at the same time. If the database is Oracle then only the Oracle columns must be filled. The same criteria holds true for SQL database.

Deploy Components

Deploy the CA Service Catalog components such as the MDB, CA EEM from the command line using the config.properties file. The config.properties file is an input file and must be located outside the USM_HOME. The file accepts passwords in plain text format only.

Note: You can also deploy the components from the CA Service Catalog User Interface.

Follow these steps:

1. Open the CA Service Catalog command prompt by clicking Start, Programs, CA, Service Catalog, CA Service Catalog Command Prompt.
2. Go to the Scripts path in the USM folder.
3. Enter one or more of the following commands:
   - To deploy MDB, enter the following command:

     ```
     Configurator.bat  - c mdb  - p "path to config.properties"
     ```

     For Example: C:\Program Files\ca\service catalog\scripts>Configurator.bat - c mdb - p "C:\config.properties"
   - To deploy CA EEM, enter the following command:

     ```
     Configurator.bat  - c eem  - p "path to config.properties"
     ```

     For Example: C:\Program Files\ca\service catalog\scripts>Configurator.bat - c eem - p "C:\config.properties"
   - To deploy component, enter the following command:

     ```
     Configurator.bat  - c component  - p "path to config.properties"
     ```

     For Example: C:\Program Files\ca\service catalog\scripts>Configurator.bat - c component - p "C:\config.properties"
   - To deploy all CA Service Catalog components, enter the following command:

```
Configurator.bat  - c all  - p "path to config.properties"
```

For Example: C:\Program Files\ca\service catalog\scripts>Configurator.bat - c all - p "C:\config.properties"

Important! Stop and start the tomcat service for the changes to take effect.

You have deployed the CA Service Catalog components using the command line.

Undeploy Components

CA Service Catalog allows you to undeploy the MDB, CA EEM, and other components individually from the command line. Undeploy these components in reverse order.

Follow these steps:

1. Open the CA Service Catalog command prompt by clicking Start, Programs, CA, Service Catalog, CA Service Catalog Command Prompt.
2. Go to the Scripts path in the USM folder.
3. Enter one or more of the following commands:
   - To undeploy all CA Service Catalog components, enter the following command:

     ```
     Configurator.bat  - u all  - p "path to config.properties"
     ```

     For Example: C:\Program Files\ca\service catalog\scripts>Configurator.bat - u all - p "C:\config.properties"
   - To undeploy component, enter the following command:

     ```
     Configurator.bat  - u component  - p "path to config.properties"
     ```

     For Example: C:\Program Files\ca\service catalog\scripts>Configurator.bat - u component - p "C:\config.properties"
   - To undeploy MDB, enter the following command:

     ```
     Configurator.bat  - u mdb  - p "path to config.properties"
     ```

     For Example: C:\Program Files\ca\service catalog\scripts>Configurator.bat - u mdb - p "C:\config.properties"
   - To undeploy CA EEM, enter the following command:

     ```
     Configurator.bat  - u eem  - p "path to config.properties"
     ```

For Example: C:\Program Files\ca\service catalog\scripts>Configurator.bat - u eem - p "C:\config.properties"

Important! Stop and start the tomcat service for the changes to take effect.

You have undeployed the CA Service Catalog components using the command line.

Perform Maintenance

You can perform the following maintenance tasks:

- CA Service Catalog files are updated during use. Backup such files regularly. For more information about file location on the CA Service Catalog component. You can perform maintenance by backing up files regularly that are updated when you use CA Service Catalog. You can change the name of of the host computer running CA EEM for security compliance. You can also change the names of the applications whose access control you manage through CA EEM. To change these names, you run the setup utility on every computer that has a CA Service Catalog component.
- You can also change the database settings like host name, port number, instance name, or service name. CA Service catalog components use the database settings for communication.
- You can also use the operating system (not the ant update-usm-host command) to change the host name. You can make use of the ant command to propagate this change for catalog systems.
- Run the setup utility to change the password of the database user, to comply with security, governance, or other requirements. CA Service Catalog components use the logon credentials (user name and password) of the database user to access the database.

Perform the following maintenance tasks:

- Files to Back Up Regularly (see page 1509)
- Update the CA EEM Host Name and Application Names (see page 1510)
- Update the Database Host, Password, Instance, Service Name, or Port (see page 1511)
- Update the Host Name and Port Number Using the ant Command (see page 1513)
- Update the Password of the Database User (see page 1514)

Files to Back Up Regularly

Several CA Service Catalog files are updated during use. Back up such files regularly.

The following table identifies the features that use the files on the Catalog Component server and their locations:

Feature	Folder
Request Attachments	USM_HOME\filestore\documents\requests
CA Service Catalog Images for services	USM_HOME\filestore\images\offerings

Feature	Folder
Documents	USM_HOME\filestore\documents
CA Service Catalog Forms	USM_HOME\filestore\forms
Data Objects and Data Views	USM_HOME\filestore\reporting
Offline Data Objects and Data View	USM_HOME\filestore\reporting\offline
Custom files for CA Service Catalog, including custom images, data fields for business units, accounts, and users. You can optionally store these files in a filestore.	USM_HOME\filestore\custom **Example:** Suppose you customized data fields for business units, accounts, and users. Sample folder name: USM_HOME\filestore\custom\locale\icusen (for English). Suppose you customized images for service option groups. Sample folder name: USM_HOME\filestore\custom\images\rateplans
Data Mediation	USM_HOME\filestore\DataMediation
CA Service Repository Agent files (also known as Data Mediation Data Repository Agent)	USM_HOME\repagent. This folder contains these sub folders: \conf, \log, and \data

Administrators who have installed CA Service Catalog on multiple computers must keep files synchronized on all servers. Otherwise, an error can occur.

The following table identifies the features that use files on multiple computers and the folders where those files are located:

Feature	Folder
Attachments	USM_HOME\view\documents
CA Service Catalog Images	USM_HOME\FileStore\images\offerings
Documents	USM_HOME\view\documents
CA Service Catalog Forms	USM_HOME\view\forms

Update the CA EEM Host Name and Application Names

To comply with security, governance, or other requirements, you can change the name of the host computer running CA EEM. You can also change the names of the applications whose access control you manage through CA EEM. To change these names, you run the setup utility on *every* computer that has a CA Service Catalog component. This utility updates these names globally to ensure that CA Service Catalog, CA EEM, and the integrated products run efficiently.

The *application names* are the CA EEM policies for managing user access control and other resources to these products. The application name *Service Delivery* in CA EEM refers to the policies governing user access control in CA Service Catalog. CA EEM includes a *Global* application name that you can apply in part or in whole to one or more products.

Follow these steps:

1. Enter the following URL in your browser for the CA Service Catalog installation that you want to update:

`http://hostname:portnumber/usm/config`

2. Enter the password to log in to the setup utility.
   The setup utility opens on the Database tab.

3. Click the Security tab, and specify new values for the settings that you want to change, as follows:

   - The host name of the CA EEM computer.
     If you change the host name, a “Backup and restore” option appears. To back up the CA EEM data on the current computer and restore it on the new computer, select this option. If you select the Backup and restore option, specify the password of the administrator on the old CA EEM computer.
   - The name of the CA EEM application instance.
   - The password of the CA EEM application instance.

4. Save your changes.

5. Restart the Windows services for Accounting Component and CA Service Catalog to make your updates take effect.

6. Make the same updates on all remaining CA Service Catalog computers in your environment.

7. Verify that CA Service Catalog is running correctly, as follows:

   a. Log in to CA Service Catalog.

   b. Perform administrative tasks. Create Services. Also, create and process requests.

The new or updated host name and application names are updated in the Windows registry.

Note: As a best practice, back up the Windows registry after you update the host name and application names. For more information, see your Windows documentation.

Update the Database Host, Password, Instance, Service Name, or Port

To comply with changes in your environment or for other reasons, you can change the following database settings: host name, port number, instance name, or service name. CA Service Catalog components use these settings to communicate with each other and the database.

Follow these steps:

1. Perform the following prerequisite tasks:

   a. To update the database host name, update the operating system computer name of the computer which has the database. For more information, see your operating system documentation.

b. Update the database settings in your DBMS software (Oracle or SQL Server). For more information, see your DBMS documentation.

c. Verify that the updated DBMS is accessible from every DBMS client on every CA Service Catalog computer. Use your DBMS client software (not CA Service Catalog) to perform this step.

2. Enter the following URL in your browser for the CA Service Catalog installation that you want to update:

   `http://hostname:portnumber/usm/config`

3. Enter the password to log in to the setup utility.
   The setup utility opens on the Database tab.

4. Enter the new password for the database user in the Application User Settings section only if *both* of the following conditions exist.

   - You are using SQL Server.
   - The database was backed up and restored on a new computer.

   Confirm the password and save your changes.

5. (Optional) When you are prompted for your password, specify your existing password to continue using it.

6. Specify new values for the settings that you want to change, as follows:
   SQL Server
   If applicable update the instance name for the MDB.
   Default: MSSQLSERVER
   Oracle
   If applicable, update the service name. Every Oracle database or service has a service name. The service name of an Oracle database is typically its global database name. Enter the service name of the Oracle database or other service that you want to access.

7. If applicable, update the port number.

8. Save your changes.

9. Restart the Windows services for CA Service Catalog to make your updates take effect.

10. Make the same updates on all remaining CA Service Catalog computers in your environment.

11. Verify that CA Service Catalog is running correctly, as follows:

    a. Log in to CA Service Catalog.

    b. Perform administrative tasks. Create services. Also, create and process requests.

Update the Host Name and Port Number Using the ant Command

If applicable, you use the operating system (not the ant update-usm-host command) to change the host name. Afterwards, you use the ant command to propagate that host name change throughout the catalog system. Use the ant command to both update the port number directly *and* propagate that change throughout the catalog system.

You perform these steps *only* on the computer whose host name or port number has changed. You do not perform these steps on *other* computers.

Follow these steps:

1. Stop the CA Service Catalog services on the computer being updated.

   Important! Stop these services on *all* CA Service Catalog computers in your environment *before* proceeding to the next step. Use the Windows Control Panel to stop the services.

2. Perform the following actions:

   a. Open the CA Service Catalog command prompt from the CA Service Catalog portion of the Windows Start menu.

   b. Enter the following command at the CA Service Catalog command prompt:

      ```
      ant update-usm-host
      ```

      Note: For a list of ant commands and their descriptions, enter ant -p.

      The utility displays the current settings for the host name and port number.

   c. Update each setting that you want to change, and record all updated settings for reference.

The command utility performs the following actions:

- Updates the host name and port number settings in your DBMS (Oracle or SQL Server) and in configuration files
- Records the actions that it performs in the maintenance.log file.
  This log file and the backed-up configuration files are stored in the USM_HOME\conf-backup*date-time* folder. The name of the *date-time* subfolder is based on when the ant update-usm-host command was run. Thus, this subfolder name is different on each computer in the environment. The utility writes the name of the subfolder to the screen as soon as the backup is completed.

3. Perform the following actions:

    a. View the maintenance.log file in the USM_HOME\conf-backup*date-time* folder for a record of the actions performed.

    b. Record the name of this folder for future reference.

4. Verify that you have finished updating the host name and port number on the current computer. Update the host name and port number on the next computer, if necessary.

5. Verify that you have updated the required settings on *all* CA Service Catalog computers.

6. Log in to CA Service Catalog.

7. Verify that CA Service Catalog is running correctly, as follows:

    a. Log in to CA Service Catalog.

    b. Perform administrative tasks. Create services. Create and process requests.

The new or updated host name and application names are updated in the Windows registry.

Update the Password of the Database User

You can run the setup utility to change the password of the database user, to comply with security, governance, or other requirements. CA Service Catalog components use the logon credentials (user name and password) of the database user to access the database. The setup utility updates these password references globally to help CA Service Catalog continue to run efficiently throughout your environment. You run the setup utility on *every* computer in your environment that has a CA Service Catalog component installed.

Follow these steps:

1. Start the setup utility by entering the following URL in your browser for the CA Service Catalog installation that you want to update: http://*hostname:portnumber*/usm/config.

2. Enter the password to log in to the setup utility.
   The setup utility opens on the Database tab.

3. Enter the new password for the database user in the Application User Settings section. Confirm the password and save your changes.

4. Restart the Windows services for CA Service Catalog to make your updates take effect.

5. Update the password on all remaining CA Service Catalog computers in your environment.

6. Verify that CA Service Catalog is running correctly, as follows:

    a. Log in to CA Service Catalog.

    b. Create services, create and process requests, and perform administrative tasks.

Configuring CA Asset Portfolio Management

This section contains the following articles:

Configurations

As an administrator, you can configure the user interface to simplify how users enter, manage, and search for data. You can also protect users from performing unauthorized tasks, ensure that you conform to your IT asset management practices. When you configure the user interface, you, and all users affected by your configuration changes, immediately see the changes. For example, you do not want anyone, except the asset manager, to see any information for sites and companies. Therefore, you hide the Site and Company tabs and specify that only users in the asset manager role can see those tabs.

When configuring the user interface, use the following types of configurations:

- **Global configuration**. Configure the product for all users, regardless of their role.
  A *global configuration* lets you modify the functionality of your product implementation. You focus on configuring the pages, objects, fields for your specific implementation. You need not worry about making configuration changes for all possible users and roles.
  For example, you do not want to use the contact management functionality. Therefore you define a global configuration on the Contact page, hide this functionality from all users, and save the global configuration. As a result, users do not see the Contact page, unless you define a local configuration to override the global configuration.
  A global configuration can apply to all asset families or legal templates or to a specific family or template. You can have only one global configuration that applies to all families or templates or that applies to a specific family or template.

  
  If you do not want to make any global user interface changes for your implementation, you do not have to define a global configuration. You can define a local configuration without defining a global configuration.

- **Local configuration**. Configure the product for specific users and roles.
  Use a *local configuration* to configure the user interface pages based on the requirements of the different users and roles.

  
  Local configuration changes override global configuration changes.

For example, you define a global configuration to hide the contact management functionality in your implementation. However, there are users in a specific role who must be able to see and update contact information. Therefore, you define a local configuration on the Contact page, make the contact information appear, and save the local configuration. When you assign the local configuration to the users in the role, they see the contact information.
A local configuration can apply to all asset families or legal templates or to a specific family or template. You can have multiple local configurations that apply to all families or templates or that apply to a specific family or template. You can assign to a role only one local configuration that applies to all families or templates or that applies to a specific family or template.

You cannot assign a global configuration to a role. By default, a global configuration is assigned to all roles when the users log in and the security permissions for the roles are determined. You can only assign a local configuration to a role.

A global configuration is always assigned to all roles, even when you assign the role to a local configuration. Any permission from the global configuration that a local configuration does not override is applied to the role. Global configurations are used to configure the product for every user (except for the system administrator role, *uapmadmin*). To configure the user interface on a more detailed level by role, add a local configuration. In this situation, all users in all roles will see the configured interface based on the global configuration changes, and users assigned to a local configuration will see the additional changes to the interface.

If a user is assigned to a local configuration, the local configuration is assigned to the role when the user logs in.

Page Configuration by Asset Families and Legal Templates

This article contains the following topics:

For most objects, you configure the user interface, save the configuration, and all users in the role that is assigned to the selected configuration see the page that way. No additional configuration options are available. For certain objects (assets, models, and legal documents) you can provide a more specific configuration by selecting a particular *asset family* or *legal template, or all asset families or legal templates*.

You can manage pages in the following ways:

- Configure the model or asset page by asset family (see page 1518).
- Configure the legal document page by legal template (see page 1519).

Example: Configure for a Hardware and Software Asset

- (Hardware Asset) Configure the page for assets by moving important fields (asset name, model name, quantity, serial number, operating system, purchase order number, and service status) to the top of the page and making the fields required. In addition, remove the Host Name field. When you save the configuration, select the asset family *Hardware*. As a result, when users assigned to the configuration enter a hardware asset, they see the page as you have configured it.

- (Software Asset) Configure the page for assets by moving important fields (asset name, model name, quantity, serial number, department, cost center, and purchase order number) to the top of the page and making the fields required. In addition, remove the Service Status and Service Status Date fields. When you save the configuration, select the asset family *Software*. As a result, when users assigned to the configuration enter a software asset, they see the page as you have configured it.

Example: Configure Across All Asset Families

Configure the page for assets in all asset families by making the Requisition ID and Purchase Order ID fields read only for all users except the asset fulfiller. The asset fulfiller can edit these two fields. To achieve this result, you create two configurations:

1. A global configuration that makes the Requisition ID and Purchase Order ID fields read only. Select Across all families for this configuration so that the fields are read only on the Asset page for all asset families. This global configuration applies to all users.

2. A local configuration that allows users to edit the Requisition ID and Purchase Order ID fields. Select Across all families for this configuration, also, so that the fields can be edited on the Asset page for all asset families. This local configuration is assigned to users in the asset fulfiller role.

As a result, users who are not asset fulfillers cannot edit the Requisition ID and Purchase Order ID fields on the Asset page for any asset family. However, users in the asset fulfiller role can edit the two fields on the Asset page for all asset families.

Example: Configure for a Confidentiality Agreement

Configure the page for legal documents by moving important fields (Document Identifier, Effective Date, Termination Date, and Negotiator) to the top of the page and making the fields required. In addition, remove the Status and Status Date fields. When you save the configuration, select the legal template *Confidentiality Agreement*. As a result, when users assigned to the configuration enter a confidentiality agreement, they see the page as you have configured it.

Custom Asset Families

You can extend the product by creating additional asset families (see page) to track products other than hardware and software. *Custom asset families* let you track information about almost any classification of asset in your IT environment. For example, you can create asset families for telecommunications, services. After you create a custom asset family, configure the page and save the configuration for the custom asset family. As a result, a user assigned to the configuration for the custom asset family sees the page as you configure.

Configure the Model and Asset Page by Asset Family

You can configure the Model or Asset page for a specific asset family (for example, hardware asset and software asset) or for all asset families. Users in the role assigned to the configuration see the page as you have configured it.

Follow these steps:

1. Click the Model or Asset tab.
2. On the left, click CONFIGURE: ON.
   The configuration of the page is enabled.
3. In the Configuration Information area of the page, select an asset family or select Across all families.

   If you are creating a global configuration and a global configuration already exists across all families, the Across all families field does not appear.

4. Specify the information for the new global or local configuration (see page 1515), or select an existing configuration that you want to change.

   Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles that are assigned to the selected configuration.

5. Complete any of the following steps:
   - Change a field label.
   - Move a field to a new location.
   - Make a field read-only, required, or optional.
   - Hide a field.
   - Make a previously hidden field appear.
   - Add a field.
6. Click Save Configuration.
   When you assign a configuration to a role, users in the role see the page as you have configured it.

Configure the Legal Document Page by Legal Template

You can configure the Legal Document page for a specific legal template or for all legal templates. Users in the role that is assigned to the configuration see the page as you have configured it.

Follow these steps:

1. Click the Legal Document page.
2. On the left, click CONFIGURE: ON.
   The configuration of the page is enabled.
3. In the Configuration Information area of the page, select a legal template or select Across all templates.

   If you are creating a global configuration and a global configuration already exists across all templates, the Across all templates field does not appear.

4. Specify the information for the new global or local configuration (see page 1515), or select an existing configuration that you want to change.

   Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles that are assigned to the selected configuration.

5. Complete any of the following steps:
   - Change a field label.
   - Move a field to a new location.
   - Make a field read-only, required, or optional.
   - Hide a field.
   - Make a previously hidden field appear.
   - Add a field.
6. Click Save Configuration.
   When you assign a configuration to a role, users in the role see the page as you have configured it.

How to Configure the User Interface

To configure the user interface, complete the following tasks:

- Protect the users from performing unauthorized tasks using object access configuration and tab and menu configuration.
- Make it easier for users to enter information for the objects they manage using field configuration.
- Validate and enforce the field format and data entry requirements using field data validation configuration (see page 1526).
- Protect the users from performing unauthorized tasks using hyperlink and button configuration.
- Extend the repository to store more data using extended field configuration (see page 1524).
- Extend the product and enhance how users enter information for the objects they manage using reference field configuration.
- Extend the product and track more information and detail about an object using hierarchy configuration (see page 1528).
- Make it easier for users to enter model, asset, and legal document information by family and legal template using page configuration (see page 1516).
- Make it easier for users to find the objects they manage in searches using search configuration.
- Make it easier for users to enter information for legal documents using legal template configuration (see page 1530).
- Alert users about upcoming events and verify that the appropriate tasks are performed in the correct order at the right time using event and notification configuration (see page 1522).
- Make it easier for users to select the correct items from lists using list management (see page 1532 .
- Extend the product and enhance how users manage object information using custom relationships (see page 1520).

Custom Relationships

Custom relationships are links between two related objects. The relationship describes and provides information about the interdependencies between the objects. Through a custom relationship, you can navigate from one object to the other object. You can locate, retrieve, and modify information about the objects.

Manage Custom Relationships

You can define and update custom relationships between two objects. In a custom relationship, one of the objects is a primary object and the other object is a secondary object.

You cannot delete a custom relationship that you define and save.

Follow these steps:

1. Define a custom relationship.
    a. Click the tab and optional subtab for the object for which you want to define a custom relationship.
    b. Select CONFIGURE: ON from the search results page.
    c. Select a global configuration across all families or templates or create and save a global configuration.

You cannot define a custom relationship for a local configuration.

    d. Click Add Custom Relationship.
    The Add Custom Relationship dialog opens.
    e. Specify a name for the primary object relationship and secondary object relationship.
    f. Select the secondary object.

For assets, models, and legal documents, select a family or template or select across all types.

    g. Click Save.
    The new custom relationships are displayed under the Custom Relationship menu for the primary and secondary objects.
    h. (Optional) Add simple or reference extended fields to the custom relationship.
2. Update a custom relationship.
    a. Click the tab and optional subtab for the object for which you want to update a custom relationship.
    b. Select CONFIGURE: ON from the search results page.
    c. Select a global configuration across all families or templates.
    d. Select the relationship under the Custom Relationship menu.

e. Modify the information for the custom relationship and click Save.

Event and Notification Configuration

This article contains the following topics:

An *event* represents an activity related to a field (default or extended) for an object. When you define an event, you specify the criteria that must be met before the event occurs. For example, you want to know when the data in a particular field changes. You can define an event that detects the data change. An event works in combination with a *notification*, which the workflow provider (for example, CA Process Automation) creates to alert your team members that an important event has occurred for a specific field or object. By using events and notifications, you alert people about upcoming events and help ensure that the appropriate tasks are performed in the correct order at the right time.

A notification is triggered when an event that you define occurs. For example, you define a date event on the Termination Date field for a legal document to notify the contract manager 15 days before a legal contract expires. The contract manager uses the 15 days to review and possibly negotiate a better contract. When the date arrives (that is, 15 days before the contract expires), the event occurs and the notification process is triggered through the workflow provider. The workflow provider constructs, issues, and manages the notification based on the configuration that you provided in the workflow provider and in CA APM.

The default notification method in CA APM supports email notifications using a workflow provider. You can send an email notification to any user or distribution list that is defined in your internal email system, even if the user is not a CA APM user. In addition, you can send an email to any external email address, if permitted by your email system.

You can also configure the notification process in the workflow provider to trigger any type of process. For example, you can set up the notification process to perform certain actions in another application when an event occurs in CA APM. For information about setting up different notification processes, see your workflow provider documentation.

You can define the following types of events to track and manage important changes to fields or objects:

- Date events. Monitor a date field for an object and have the workflow provider notify you that an important date is approaching or has passed.
- Change events. Monitor a field for an object and have the workflow provider notify you that the field value has changed.
- Watch events. Monitor a field for an object and have the workflow provider notify you about a potential obstruction to completing a task.

How to Configure Events and Notifications

Events work in combination with notifications, which the workflow provider (for example, CA Process Automation) creates, to communicate information to your team members about important events and activity. To configure events and notifications, complete the following steps:

1. Administrators grant permissions to users to manage events.

2. Users with the correct permissions open an existing configuration and define date events, change events, and watch events. For more information about defining events, see Events and Notifications (see page 2376).

3. Users, when defining an event, map all workflow provider process parameters to a CA APM object attribute. For more information, see Workflow Provider Process Parameters (see page 2376).

4. The workflow provider initiates the notification process.

5. Users View an Audit History of Events (see page 2340).

Grant Permissions to Manage Events

You can grant permissions to users so they can configure the user interface and can define an event.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure.

2. On the left, click CONFIGURE: ON.
   The configuration of the page is enabled.

3. In the Configuration Information area of the page, select an existing global or local configuration (see page 1515).

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles that are assigned to the selected configuration.

4. In the Permissions area of the page, move Manage Events to the Granted Permissions list.

5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.
   When you assign a configuration to a role, users in the role have permissions to define an event.

Extended Field Configuration

Contents

You can design your own fields (extended fields) and can add them to objects. Extended fields are additional fields to help you capture data in your repository critical to the asset management at your site. If you are not able to find an appropriate field in your repository to store key data, define an extended field for the data.

You can define extended fields for models, assets, legal documents, costs, payments, model parts and pricing, contacts, companies, organizations, locations, and sites. You can use extended fields when searching and for reports.

You can add an extended field that you created for an asset cost to a legal document cost. Under Legal Document, click Add Existing Fields on the Costs configuration page.

Extended fields are shared with the products integrating with CA APM (CA Service Desk Manager and CA Service Catalog). Any changes that are made to the extended field values in the integrating products are immediately reflected in CA APM. And, any changes you make to the extended field values in CA APM are reflected in the integrated products.

Define an Extended Field

You can define an extended field to help you capture all data in your repository that is critical to your asset management program. For example, when entering an asset for a blade server, there is no way to enter the chipset. Define an extended field that is named *chipset,* which adds the field to the Asset Details page. Users can enter the chipset information (for example, Intel 5520) with the other information such as the asset name, serial number, memory, processor, operating system.

Important!: These steps work only the first-time you complete the wizard and define the extended field for the object. Before you define the extended field, verify that you have the following information for reference: table name, label, format (character, boolean, currency, date, decimal, or integer), field name, attribute name, field size, and whether an entry for the extended field is required. After you complete the wizard, you can configure the extended field like any field.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure.

2. On the left, click CONFIGURE: ON.
   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global configuration (see page 1515), or select an existing global configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.
   For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object. Changes do not apply to the other parts of the object.

You can only define an extended field for a global configuration. You cannot define an extended field for a local configuration.

4. Click Save Configuration to create the global configuration.

5. Click Add Extension.
   A wizard appears.

6. To enter the information for the extended field, select the Simple Field option and follow the on-screen instructions.

To change the default object label for the extended field, change the label in the Object Label field. For example, change the default label *asset hardware Extension* to *Hardware Extension*.

7. Click Save Configuration.
   All users see the extended field on the page.

Note: After you add a field and define an extended field, and save the field to a local or global configuration, users can define an event for the field. For more information about managing events, see Event and Notification Configuration (see page 1522).

Grant Permissions to Define an Extension

You can grant permissions to users so an Add Extension link appears to define an extension.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure.

2. On the left, click CONFIGURE: ON.
   The configuration of the page is enabled.

3. In the Configuration Information area of the page, specify the information for the new global configuration (see page 1515). You can select an existing global configuration that you want to change.

   You can only define an extended field for a global configuration. You cannot define an extended field for a local configuration.

4. In the Permissions area of the page, move Extend Object to the Granted Permissions list.

5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.
   When you assign a configuration to a role, users in the role have permissions to define an extension.

Field Data Validation Configuration

You can create field data validation configurations to validate the data entry in fields. These field data validations ensure that users enter data in the correct format and enforce your organizational business rules.

The data validation affects new data that is added. Existing data records are validated only when you access the data record and you save the record.

For example, you want to ensure that users enter asset names using only alphanumeric characters (no special characters). Create a data validation for the Asset Name field on the New Asset or Asset Details page. Specify that the field allows only alphanumeric entries. Users receive an error message if the characters they use are not alphanumeric.

Add a Data Validation for a Text Field

You can validate the data entry in text fields (for example, contact name, email address, or telephone number) to enforce specific format requirements. You create the data validations for text fields by defining the regular expressions that apply to the different types of text fields.

A *regular expression* is a text string that describes a particular pattern or format. Regular expressions are used to validate text to ensure that the text matches a predefined format. For example, create a regular expression to specify the correct format for an email address, telephone number, or IP address.

Compose and test your regular expression before creating the text field data validation. You can find resources on the Web for creating, analyzing, and testing regular expressions.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.
   The configuration of the page is enabled.
3. In the Configuration Information area of the page, complete the following steps:
   a. Specify the information for the new global or local configuration, or select an existing configuration that you want to change.

      Permissions for data validation are allowed by default. You can deny data validation permissions for the current configuration. The users that are assigned to the configuration do not then see the Data Validation icon and cannot add data validations.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.
      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles that are assigned to the selected configuration.

4. Next to the text field that you want to validate, click the Data Validation icon.
5. Enter the regular expression that applies to the type of field (for example, telephone number, email address) and click OK.

Verify that you selected the correct regular expression for the field type and that you entered the regular expression accurately.

To modify or delete an existing data validation, complete one of the following steps:

- To modify the validation, edit the regular expression in the text entry field and click OK.
- To delete the validation, clear the regular expression in the text entry field and click OK.

6. Click Save Configuration.
   When you assign the configuration to a role, users in the role receive data validation messages if their text entries do not match the defined format.

Hierarchy Configuration

In the product, a *hierarchy* is a way to establish a logical relationship to an object field. You can define a hierarchy to extend the product and track more information and detail about an object. You can define a hierarchy for any object.

Example: Create a Hierarchy to Locate an Asset

In CA APM, when you enter an asset, use the Location Name field to enter generic asset information. Information can be the location of an asset (city and address). However, for a hardware asset family, you need a more detailed way to track the asset location. To locate an asset for maintenance and repair, find the specific office number, building number, floor number, and cubicle number. Define the following hierarchy:

```
Pittsburgh Office
   Building 3
    Fourth Floor
        Cubicle 49466
```

In the previous hierarchy, each field is related to the field above it. If you change the information for a parent field, the information for the child field is changed. However, changing a child field (Fourth Floor) does not change the parent field (Building 3).

By defining this hierarchy, you know and can track the exact location of the asset. CA APM manages the fields that you define in the hierarchy so they can be used in searches and reports.

Define a Hierarchy

You can define a hierarchy to extend the product and track more information and detail about an object. For example, define a location hierarchy for an asset to track the asset to a specific location. When asset location with an established hierarchy for the asset family is selected, a list appears inside the location section. Each location hierarchy extended field has one list. If the location selected has values for the hierarchy, the values are populated in the drop-down list.

Before you define a hierarchy, verify that you have the following reference information: table name, label, format, field name, attribute name, field size. Also verify, if an entry for the extended field in the hierarchy is required.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.
   The configuration of the page is enabled.
3. In the Configuration Information area of the page, complete the following steps:
   a. Specify the information for the new global configuration (see page 1515), or select an existing global configuration that you want to change.
   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Permission changes that you make apply only to that part of the object. For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object.

   You can only define a hierarchy for a global configuration. You cannot define a hierarchy for a local configuration.
4. (Optional) Click Save Configuration to create the global configuration.

5. Click Add Extension.
   A wizard appears.

6. To define the hierarchy, select the Hierarchy option and follow the on-screen instructions. The following fields require explanation:

   - **Object Label**
     Specify the default object label for the hierarchy. You can change this label to meet your requirements. For example, change the default label Asset Extensions to Asset.

   - **Object Table Name**
     Specify the database table name for the hierarchy.

   - **Object Tenancy**
     If multi-tenancy is enabled, specify how multi-tenancy works for the hierarchy by selecting one of the following options. The option that you select is applied to all levels in the hierarchy.

     - **Untenanted**
       Defines objects without a tenant attribute. All data in these objects is public, and any user can create and update untenanted public data.

     - **Tenant Required**
       Defines objects with a tenant attribute that cannot be null (enforced by CA APM, not the DBMS). All data in these objects is associated with individual tenants; there is no public data.

     - **Tenant Optional**
       Defines objects with a tenant attribute that can be null. You can either create these objects as tenanted or public. When you select a tenant in a tenant drop-down to create an object, the object becomes a tenanted object. However, when you select the Public Data option in a tenant drop-down, the object becomes a tenanted public object. A tenant drop-down does not appear for users assigned to a role that only exposes a single tenant when entering data.

   - **Begin with existing field**
     Select an existing field as the basis for fields in the first hierarchy level.

   - **Begin with a new field**
     Select to start the hierarchy with a new field you define. Define at least two levels for the hierarchy.

7. Click Save Configuration.
   All users see the hierarchy on the page.

Legal Template Configuration

This article contains the following topics:

A *legal template* provides the group of attributes that belong to a particular type of legal document. You typically set up and maintain legal templates, while users create legal document records based on the legal templates. When you create a legal document record, you first select a legal template on which to base the document. The legal document record inherits the attributes from the legal template.

Each legal template has *terms and conditions* that typically apply to the legal document type. For example, a legal template for an invoice includes information about the terms of payment.

You can use the product to define legal templates and change the attributes of a legal template. To change the terms and conditions assigned to a legal template, you can remove them or add new ones from the master list of terms and conditions.

A legal template cannot be deleted until all legal documents based on the template are deleted. In addition, you can search for legal documents by the legal template name, and you can use legal template names to select records to include in reports.

Define a Legal Template

You can define a legal template to group attributes that belong to a particular type of legal document. Administrators or users with appropriate privileges can define legal templates.

Follow these steps:

1. Click Directory, List Management.
2. On the left, expand Legal Document Lists and click Legal Template.
   The list of templates appears on the right.
3. Click New, enter a name for the template, and click Save.
   The new template appears in the list.
4. Click the Edit Record icon for the new template.
5. Click the View Assigned Ts & Cs hyperlink.
6. Click Select New and select the terms and conditions for the new template.
7. Click Save.
   Users can select the new template when they define legal documents.

Change the Terms and Conditions for a Legal Template

You can change the terms and conditions for a legal template. Administrators or users with appropriate privileges can change the terms and conditions.

Follow these steps:

1. Click Directory, List Management.
2. On the left, expand Legal Document Lists and click Legal Template.
   The list of templates appears on the right.

3. Click the Edit Record icon for the legal template.

4. Click the View Assigned Ts & Cs hyperlink.
   All terms and conditions for the legal template appear.

5. Select any of the following options:

   - Click Select New and select the terms and conditions for the template.

   - Click the Delete icon to remove the term and condition from the template.

6. Click Save.
   The updated terms and conditions are applied to the template.

List Management

This article contains the following topics:

You can define the items that appear in lists to help make it easier for users to select the correct information from lists for the objects they manage. For example, when defining a new contact, the user can specify a contact type. You define the items that appear in the contact type list. In addition, when defining a legal document, the user must specify a legal template. You define the items that appear in the legal template list.

You can manage items in the following lists and in the reference fields you define:

- Assets
- Companies
- Contacts
- Legal Documents
- Locations
- Models
- Organizations
- Searches
- Normalization

Define List Items

You can define, update, and delete list items to help make it easier for users to select the correct information from lists when managing objects. For example, you can change the name and description of a cost center to make it easier for users to select a cost center. You can also delete a general ledger code so that users cannot select that code when they define assets.

When you delete a list item, users cannot select the item when defining an object. Instead of deleting the list item, you can make the list item inactive. Then, if you need the list item in the future, you can make the item active again. You do not have to redefine the item.

By default, all the items in a list are displayed. However, if you have large number of list items, you can search for specific items. The search criteria depends on the properties of the list. For example, for **Cost Type** you can search the items based on **Value, Status**, and the **Description** of the cost type.

Note: This feature will only be available if you apply a patch for CA Service Management Release 14.1.01. Find the patch and the download details from CA Support Online.

Follow these steps:

1. Click Directory, List Management.
2. On the left, select the list that you want to manage.
3. Click New.
4. Enter the information for the list item.

   When multi-tenancy is enabled, select the tenant for the list item.

5. Click Save.

Define List Management Access

As an Administrator, you can define who accesses List Management. You can also determine the list items that different users can access. For example, a Contract Manager requires information related to legal document lists, company lists, and contact lists but not Asset lists. So, as an Administrator, you configure the access rights to Contract Manager role accordingly.

> **Note:** This feature will only be available if you apply a patch for CA Service Management Release 14.1.01. Find the patch and the download details from CA Support Online.

Follow these steps:

1. Click Administration, User/Role Management.
2. Click the role for which you want to configure List Management access.
3. To configure which list items the role access, select the appropriate check box.
   For example, to restrict asset list access to a Contract Manager, ensure clear the Asset Lists Access check box.
4. To enable or disable List Management, select or clear List Management Access.
5. Save the configuration changes.

Define the Class and Subclass Lists for an Asset Family

You can define the class and subclass lists for an asset family to help make it easier for users to select the correct information when defining models and assets. For example, you can define the class "printer" and the subclass "laser". Then when users create or search for printer assets, this additional information helps them to define or identify the correct assets.

Follow these steps:

1. Click Directory, List Management.
2. On the left, click Asset Lists, Asset Family.
3. Complete the following steps to define the class list:
   a. Click the Edit Record icon next to the asset family for which you want to define the class.
   b. Click the Class List hyperlink.
   c. Define the class record for the asset family.
   d. Click Save.
4. Complete the following steps to define the subclass list:
   a. Click the Edit Record icon next to the class record for which you want to define the subclass.
   b. Click the Subclass List hyperlink.
   c. Define the subclass record for the asset family.
   d. Click Save.

Define Legal Document Terms and Conditions

You can define the terms and conditions that apply to legal document lists. Users can then apply the correct terms and conditions when they define legal templates or legal documents.

Follow these steps:

1. Click Directory, List Management.
2. On the left, expand Legal Document Lists and select Terms and Conditions.
3. Click New.
4. Enter the information for the new list item.

   To make the new item apply to date-specific terms and conditions lists only, select the Date Specific Key check box.

5. Click Save.

Exclude an Asset Family

You can exclude an asset family so that it is not available for users. If you exclude an asset family, a user who creates or modifies a model cannot select that asset family. Also, the excluded asset family is not available for managing filters, data imports, or configurations. For example, if CA APM is integrated with CA Service Desk Manager, the asset families from CA Service Desk Manager are also available to CA APM users. If you do not require the CA Service Desk Manager asset families, you can exclude them so that they are not available to users.

If a model was already associated with an asset family before you excluded the family, you can still access and edit that model. You can also still use that model to create assets. However, you cannot change the asset family for that model to another excluded asset family.

You can change the asset family for a model only if the model does not have associated assets.

Follow these steps:

1. Click Directory, List Management.
2. On the left, select Asset Family under Asset Lists or Model Lists.
3. Click the Edit Record icon for the family that you want to exclude.
4. Clear the Is ITAM check box and click the Complete Record Edit icon.

> Do not select the Inactive check box. This action makes the asset family inactive for all products that are integrated with the CA MDB.

5. Click Save.

This feature will only be available if you apply a patch for CA Service Management Release 14.1.01. Find the patch and the download details from CA Support Online.

Manage Buttons

You can configure the button access to help prevent users from performing unauthorized tasks. You can configure buttons in the following ways:

- Hide a button when you do not want users to be able to see and use the New menu option and the Save, Copy, and Delete buttons. For example, you do not want a user to be able to copy or delete an asset. Therefore, you hide the Copy and Delete buttons on the Asset page.
- Make a previously hidden button appear when users must be able to see and use the New menu option and the Save, Copy, and Delete buttons. For example, you hid the Copy button for the Asset page, but the button appears. Therefore, you make the Copy button appear.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

   In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.
   For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

> Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

2. In the Permissions area of the page, complete the following steps in the Granted and Denied Permissions lists:

- To hide the New option and Save button, move Create to the Denied Permissions list.
- To hide the Copy button, move Copy to the Denied Permissions list.
- To hide the Delete button, move Delete to the Denied Permissions list.
- To make the New option and Save button appear, move Create to the Granted Permissions list.
- To make the Copy button appear, move Copy to the Granted Permissions list.
- To make the Delete button appear, move Delete to the Granted Permissions list.

3. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

4. Click Save Configuration.

Manage Fields

This article contains the following topics:

You can change the display and attributes of field information on the page to meet your asset management practices and help make it easier for users to enter information for the objects they manage. In the product, these fields are referred to as *configured fields*.

You can manage fields in the following ways:

- Change a field label to help make the field more familiar to users and conform to your IT asset management practices.
- Move a field to a new location to help make it easier for users to find the field on the page.
- Hide a field from display when users should not be able to view a particular field on the page.
- Make a field appear when users must be able to see a field that you previously hid. For example, you previously hid the Capacity field. Users must be able to see that field because it is required. Add the field back so users can enter a value when defining an asset.

- Make a field read-only, required, or optional (see page 1540).
- Add a field (see page 1539).
- Manage field permissions (see page 1541).

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure.

   On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

   In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.
   For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

2. To change a field label, complete the following steps:

   a. Click the field label and enter the new label.

   b. Click Save Configuration.
   When you assign a configuration to a role, users in the role see the new field label.

3. To move a filed to a new location, complete the following steps:

   a. Drag-and-drop the field to a new location in the current section.

   You cannot move a field from one section of the page to another. For example, you cannot move a field from the Additional Information section to the Basic Information section.

b. Click Save Configuration.
When you assign a configuration to a role, users in the role see the fields in the new location.

4. To hide a field, complete the following steps:

a. Next to the field, click the Remove Field icon.

b. Click Save Configuration.
When you assign a configuration to a role, users in the role do not see the field. If an event is defined for the hidden field, users still receive notifications. However, any mapped attribute that is not accessible in the workflow process associated with the event is not sent as part of the notification.

5. To make a previously hidden field appear, complete the following steps:

a. Click Expose Hidden Fields.

b. To add the field to the page, follow the on-screen instructions.

c. Click Save Configuration.
When you assign a configuration to a role, users in the role see the field on the page.

After you make a previously-hidden field appear, users can define an event for the field. You do not have to save the configuration because the field has already been added to the configuration. For more information about managing events, see Events and Notifications (see page 2376).

Add a Field

You can add a field to the page when users must be able to see a field that exists in the repository but is not part of a global configuration, or any field that has been removed and you have denied access. For example, you previously removed an extended field that is named chipset from the Asset Details page. Users must be able to see and enter a value for this field, so you add the field back onto the page. In addition, if you previously added an extension but did not save the global configuration, use these steps to add the extended field to the page.

When you add a field to an object having multiple asset families (Assets and Models) and legal templates (Legal Documents), the field is added to all families and templates for the object, regardless of the family or template to which you added the field. For example, you add a field for the Hardware asset family. The field is added to all other asset families, including Computer, Other, Projects, Service, and Software.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure.

2. On the left, click CONFIGURE: ON.
   The configuration to the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global configuration (see page 1515), or select an existing global configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make apply only to that part of the object. For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object.

You can only add a field for a global configuration. You cannot add a field for a local configuration.

4. Click Save Configuration to create the global configuration.

5. Click Add Existing Fields.
   A wizard appears.

6. To add to the page, select the fields.

For extended fields, a link appears that matches the object label that is specified when defining an extended field. To add to the page, click the link and select the extended fields.

7. Click Save Configuration.
   All users see the field on the page.

Note: After you add a field and define an extended field, and save the field to a local or global configuration, users can define an event for the field. For more information about managing events, see Event and Notification Configuration (see page 1522).

Make a Field Read-Only, Required, or Optional

A *required field* is a field that must contain a value to save the record. When you configure a field or create an extended field, you can make the field read-only, required, or optional. Making a field that is required is useful for fields that contain key pieces of data.

When making a new required field, saved records may not have data in the field. When you save the record in the future, you must enter data into the new required field. You must also enter data when a pre-existing record is updated by an application you write using the web services. Your client application must verify that the required field contains data, or provides data for the field. If not, the record will not be updated.

We recommend that before you make a field required, you populate the field for all existing records. You can search to locate all occurrences of blank values in the field by searching for NULL or space (clear the value field).

To make a field read-only, required, or optional

1. Click the tab and optional subtab for the object that you want to configure. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

   In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.
   For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

2. Next to the field, click the appropriate icon to make the field read-only, required, or optional.

3. Click Save Configuration.
   When you assign a configuration to a role, users in the role see the fields as read-only, required, or optional.

Manage Field Permissions

You can grant permissions to users so they can configure the user interface to change a field label, move a field, make a field required, and hide a field.

You can also grant permissions to users so they can configure the user interface and can perform mass changes on a field. You can perform mass changes on fields that are associated with the following objects:

- Asset
- Model
- Legal document
- Organization
- Contact
- Company
- Location
- Site

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.
   The configuration of the page is enabled.
3. In the Configuration Information area of the page, specify the information for the new global or local configuration (see page 1515), or select an existing configuration that you want to change.

   Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. In the Permissions area of the page, do one the following:
   - To grant permissions to change a field label, move Modify Labels to the Granted Permissions list.
   - To grant permissions to move a field, move Order Fields to the Granted Permissions list.
   - To grant permissions to make a field required, move Requiredto the Granted Permissions list.
   - To grant permissions to hide a field, move Secure (Read-Only and Access)to the Granted Permissions list.

- To grant permissions to perform mass changes on a field, move Mass Changeto the Granted Permissions list.

5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.
   When you assign a configuration to a role, users in the role have permissions to perform the respective configuration.

View Field Information

You can view the information about any field, including extended fields, to see database-related field attributes. For any field, you can view the object label, database table name, database field name, attribute name, data type, description, and size. Use this information in the following ways:

- You want to view CA APM data outside of the product using an external reporting solution and must understand database-level information. For example, you want to know the database table name, field name, attribute name, data type, description, or field size for a particular default field or user-defined extended field.

- You have changed a field label or moved a field to a new location on the page. Use the field information to understand how the field is represented in the database. This field information can be helpful when you work with Technical Support to understand any specific configuration changes you have made to the product.

Follow these steps:

1. Click the tab and optional subtab for an object.

2. On the left, click CONFIGURE: ON.
   The configuration of the object is enabled.

3. Next to the field, click the View Details icon.
   The field information appears.

Manage Hyperlinks

You can configure hyperlink access to help prevent users from performing unauthorized tasks and only see the information appropriate for their particular job function. You can configure hyperlinks in the following ways:

- Hide a hyperlink when users should not be able to see a particular hyperlink. For example, you do not want a user to be able to see the audit history for an object. Therefore, you hide the View Audit History hyperlink.

- Make a previously hidden hyperlink appear when users must be able to see a hyperlink that you previous hid. For example, you hid the View Audit History hyperlink, but the hyperlink should now appear. Therefore, you make the View Audit History hyperlink appear.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

   In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.
   For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

2. To hide a hyperlink, complete the following steps:

   a. Next to the hyperlink, click the Access Granted icon.
   The Access Denied icon appears for the hyperlink.

   b. Click Save Configuration.
   When you assign a configuration to a role, users in the role do not see the hyperlink.

3. To make a previously hidden hyperlink appear, complete the following steps:

   a. If the hyperlink is already hidden, click the Access Denied icon next to the hyperlink.
   The Access Granted icon appears for the hyperlink.

   b. Click Save Configuration.
   When you assign a configuration to a role, users in the role can see and use the hyperlink.

Manage Menu Options

You can configure the tab and menu access to:

- Help protect the integrity of the data for your objects.
- Prevent the users from performing unauthorized tasks such as adding or deleting object information.
- Support separation of duties so users only see the information appropriate for their particular job function.

For assets, models, and legal documents, you provide a specific configuration by specifying the *asset family* and *legal template*.

You can configure the menu access in the following ways:

- Hide a menu option when users should not be able to see all, or a particular menu option.
  For example, you do not want a user to be able to view model dependencies. Therefore, you hide the Dependencies menu option.
- Make a menu option appear when users should be able to see all, or a particular menu option.
  For example, you want a user to be able to view model dependencies. Therefore, you make the Dependencies menu option appear.
- Make a menu option read-only when users should be able to see, but not use a particular menu option.
  For example, you do not want a user to change any notes for a model. Therefore, you make the Notes menu option read-only.
- Make a menu option accessible when users should be able to see, and use a particular menu option.
  For example, you want a user to be able to change the generic configuration for a model. Therefore, you make the Model Configuration menu option accessible.

Combine the tab and menu configuration and field configuration to enforce more granular levels of access.

Follow these steps:

1. Click the tab and optional subtab for the object access that you want to configure. On the left, click **CONFIGURE: ON**.

   The configuration of the object access is enabled.

   In the Configuration Information area of the page, specify the information for the new global or local configuration, or select an existing configuration that you want to change.

Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

2. To hide a menu option, complete the following steps:

    a. On the menu or menu option, click the Access Granted icon.
    The Access Denied icon appears for the menu or menu option.

    b. Click Save Configuration.
    When you assign a configuration to a role, users in the role cannot see the menu option.

3. To make a menu option appear, complete the following steps:

    a. If the menu or menu option is already hidden, click the Access Denied icon on the menu or menu option.
    The Access Granted icon appears for the menu or menu option.

    b. Click Save Configuration.
    When you assign a configuration to a role, users in the role can see and use the menu option.

4. To make a menu option read-only, complete the following steps:

    a. On the menu or menu option, click the Editable icon.
    The Read Only icon appears for the menu option.

    b. Click Save Configuration.
    When you assign a configuration to a role, users in the role can see, but not use, the menu option.

5. To me a menu option accessible, complete the following steps:

    a. If the menu or menu option is already read-only, click the Read Only icon on the menu or menu option.
    The Editable icon appears for the menu option.

    b. Click Save Configuration.
    When you assign a configuration to a role, users in the role can see, and can use the menu option.

Manage Object Access

You can configure object access to help protect the integrity of the data, prevent users from performing unauthorized tasks, and provide users with only the information appropriate for their job functions. You can configure object access in the following ways:

- Hide an object to prevent users from seeing a particular area of the page for the object.
  For example, you do not want a user to be able to see pricing information for models. Therefore, you hide the Parts and Pricing area of the Models page.

- Make an object appear when users should be able to see a particular object.
  For example, you want a user to be able to see pricing information for models. Therefore, you make the Parts and Pricing area of the Models page appear.

- Make an object read-only when users should be able to see, but not change the information about a particular object.
  For example, you want a user to be able to see, but not change, pricing information for models. Therefore, you make the Parts and Pricing area of the Models page read-only.

- Make an object accessible when users should be able to see and change the information about a particular object.
  For example, you want a user to be able to see, and edit, pricing information for models. Therefore, you make the Parts and Pricing area of the Models page accessible.

- Grant permission to users to secure objects.

Combine object access and field configuration to enforce more granular levels of access.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

   In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.
   For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

2. To hide an object, complete the following steps:

   a. On the right, next to the title for the area of the page (for example, Models page, Parts and Pricing) click the Access Granted icon.
   The Access Denied icon appears for the object.

b. Click Save Configuration.
When you assign a configuration to a role, users in the role cannot see the object information.

3. To make an object appear, complete the following steps:

   a. If access is already denied for the object, click the Access Denied icon on the right, next to the title for the area of the page (for example, Models page, Parts and Pricing).
   The Access Granted icon appears for the object.

   b. Click Save Configuration.
   When you assign a configuration to a role, users in the role can see the object information.

4. To make an object read-only, complete the following steps:

   a. On the right, next to the title for the area of the page (for example, Models page, Parts and Pricing) click the Editable icon.
   The Read Only icon appears for the object.

   b. Click Save Configuration.
   When you assign a configuration to a role, users in the role can see, but not change the object information.

5. To make an object accessible, complete the following steps:

   a. If the object is already read-only, click the Read Only icon on the right, next to the title for the area of the page (for example, Models page, Parts and Pricing).
   The Editable icon appears for the object.

   b. Click Save Configuration.
   When you assign a configuration to a role, users in the role can access the object information.

Grant Permissions to Secure Objects

You can grant permissions to users so they can configure the user interface and hide objects, make objects appear, make objects read-only, and make objects accessible.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure.

2. On the left, click CONFIGURE: ON to enable the configuration of the page.

3. In the Configuration Information area of the page, specify the information for the new global or local configuration (see page 1515), or select an existing configuration that you want to change.

Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. In the Permissions area of the page, move Secure (Read-Only And Access)to the Granted Permissions list.

5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.
   When you assign a configuration to a role, users in the role have permissions to hide objects, make objects appear, make objects read-only, and make objects accessible.

Manage Tabs

You can configure tab access to help protect the integrity of the data for your objects, prevent users from performing unauthorized tasks such as adding or deleting object information, and to support separation of duties so users only see the information appropriate for their particular job function.

For assets, models, and legal documents, you provide a specific configuration by specifying the *asset family* (assets and models) and *legal template* (legal documents).

You can configure tab access in the following ways:

- Hide a tab when users should not be able to see a particular tab.
  For example, you do not want a user to be able to see any information for legal documents. Therefore, you hide the Legal Document tab.

- Make a tab appear when users should be able to see a particular tab.
  For example, you want a user to be able to see all information for legal documents. Therefore, you make the Legal Document tab appear.

- Make a tab read-only when users should be able to see, but not change the information on a particular tab.
  For example, you want a user to be able to see, but not change, the information for a model. Therefore, you make the Model tab read-only.

- Make a tab accessible when users should be able to view and change the information on a tab. For example, you want a user to be able to see, and edit, all information for a model. Therefore, you make the Model tab accessible.

Follow these steps:

1. Click the tab and optional subtab for the object access that you want to configure. On the left, click **CONFIGURE: ON**.

   The configuration of the object access is enabled.

   In the Configuration Information area of the page, specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   > Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

2. To hide a tab, complete the following steps:

   a. On the tab, click the Access Granted icon.
   The Access Denied icon appears for the tab.

   b. Click Save Configuration.
   When you assign a configuration to a role, users in the role cannot see the tab.

3. To make a tab appear, complete the following steps:

   a. If the tab is already hidden, click the Access Denied icon on the tab.
   The Access Granted icon appears for the tab.

   b. Click Save Configuration.
   When you assign a configuration to a role, users in the role can see the tab.

4. To make a tab read-only, complete the following steps:

   a. On the tab, click the Editable icon.
   The Read Only icon appears for the tab.

   b. Click Save Configuration.
   When you assign a configuration to a role, users in the role cannot change the information on the tab.

5. To make a tab accessible, complete the following steps:

   a. If the tab is already read-only, click the Read Only icon on the tab.
   The Editable icon appears for the tab.

b. Click Save Configuration.
When you assign a configuration to a role, users in the role can access the information on the tab.

Reference Field Configuration

This article contains the following topics:

You can define your own *reference fields* and add them to objects to extend the product and enhance how users enter information for the objects that they manage. When you define a reference field, you can reference an existing object, or define a new object.

- Define a reference field (see page 1551) to an *existing object* to standardize on a common set of values that the user can select when defining an object. For example, when defining an asset, you want users to select the specific terms and conditions for an asset and select an approved general ledger code. In this example, you define two reference fields to standardize the terms and conditions and general ledger codes the user can select when defining the asset.

- Define a reference field (see page 1551) to a *new object* to establish a relationship between people, companies, assets, and so forth. For example, when defining and managing vendors, you want the user to assign a service rating to each vendor and select a quality rating (one through five stars). In this example, you define one reference field to record the quality rating when defining and managing vendors.

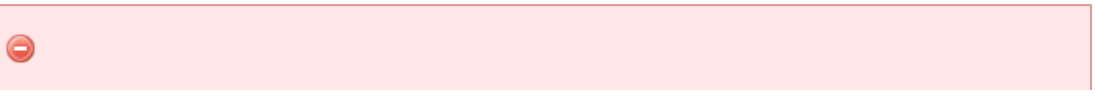
You can define reference fields for models, assets, legal documents, costs, payments, model parts and pricing, contacts, companies, organizations, locations, and sites.

After you define a reference field, you can configure the reference field (see page 1554) by completing the following tasks:

- Add a field to the reference field criteria and results
- Remove a field from the reference field lookup criteria and results
- Make a previously-hidden reference field appear
- Move a reference field to a new location

Define a Reference Field

You can define your own *reference fields* and add them to objects to extend the product and enhance how users enter information for the objects they manage. When you define a reference field, you can reference an existing object, or define a new object. For example, when defining an asset, you want users to select the specific terms and conditions for an asset and select an approved general ledger code. In this example, you define a reference field to an existing object and standardize the terms and conditions and general ledger codes the user can select when defining the asset.



Important!: These steps work only the first-time you complete the wizard and define the reference field. Before you define the reference field, verify that you have the following information for reference: table name, label, format (character, boolean, currency, date, decimal, or integer), field name, attribute name, field size, and whether an entry for the field is required. After you complete the wizard, you can configure the reference field by adding and removing fields, making a previously-hidden reference field appear, and moving a reference field to a new location.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure.

2. On the left, click CONFIGURE: ON.
   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global configuration (see page 1515), or select an existing global configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.
   For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   You can only define a reference field for a global configuration. You cannot define a reference field for a local configuration.

4. (Optional) Click Save Configuration to create the global configuration.

5. Click Add Extension.
   A wizard appears.

6. Select the Reference Field option and follow the on-screen instructions to enter the information for the reference field. The following fields require explanation:

   - **Object Label**
     Displays the default reference field object label to appear when you add a field to the reference field criteria and results, and make a previously-hidden reference field appear. You can change this label to meet your requirements. For example, change the default label Location Extensions to Location.

   - **Label**
     Enter the label for the reference field that you want to appear in list management.

- **Service provider eligible**
  Determines if field values from the service provider are included in the reference field. When you select this check box, public data and service provider objects are included in the reference field.

- **Based on current object**
  Select an existing object on which to base the reference field you are defining.

  
  When you select this option, the reference field for the object already exists and the multi-tenancy options for the object are applied.

- **Object table name**
  Specify the database table name for the reference field.

- **Object Tenancy**
  If multi-tenancy is enabled, specify how multi-tenancy works for the reference field by selecting one of the following options:

  - **Untenanted**
    Defines objects without a tenant attribute. All data in these objects is public, and any user can create and update untenanted public data.

  - **Tenant Required**
    Defines objects with a tenant attribute that cannot be null (enforced by CA APM, not the DBMS). All data in these objects is associated with individual tenants; there is no public data.

  - **Tenant Optional**
    Defines objects with a tenant attribute that can be null. You can either create these objects as tenanted or public. When you select a tenant in a tenant drop-down to create an object, the object becomes a tenanted object. However, when you select the Public Data option in a tenant drop-down, the object becomes a tenanted public object. Users assigned to a role that only exposes a single tenant will not see a tenant drop-down when entering data.

  
  When multi-tenancy is disabled, you do not see the Object Tenancy drop-down for the reference field. However, the product applies the Tenant Optional setting to the reference field. The product works this way so that if you enable multi-tenancy, the Tenant Optional setting is applied to the reference field.

7. Click Save Configuration.
   All users see the reference field on the page. When you define a reference field based on a new object, the reference field appears as a list item that can be managed using list management (see page 1532).

Manage Reference Fields

After you define a reference field, you can configure the field in the following ways:

- Add additional fields to extend the information that appears in your reference field criteria and results. For example, when users add an asset, they can search by model name and description to find the model describing the asset. You can configure the model reference field and add the Asset Family, Class, and Company Name fields to the reference field criteria and results to make it easier for users to find the model when defining the asset.

- Remove a field when you do not want a particular field included in the reference field criteria and results. For example, you previously configured the model reference field by adding the Asset Family, Class, Company Name, and GL Code fields. To protect users from viewing sensitive information, you remove the GL Code field from the model reference field.

- Make a reference field appear when users must be able to see a reference field that you previously hid. For example, you previously configured the model reference field by removing the Inactive field. Add the field back to the model reference field so users can find and not select inactive models when adding an asset.

- Move a reference field to a new location to help make it easier for users to find the reference field. For example, you configure the model reference field and add the Asset Family, Class, and Company Name fields to the reference field criteria and results to make it easier for users to find the model when defining an asset. You move the Company Name field to the top of the model reference field so users can find models in a particular company.

You can complete the tasks only when your assigned role has permissions to configure the object.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure.

2. On the left, click CONFIGURE: ON.
   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   - Specify the information for the new global or local configuration, or select an existing configuration that you want to change.
     (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.
     For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

Important!: Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. Click Save Configuration.

5. Next to the field, click the Lookup Field icon.
   A list of fields in the reference field criteria and results appears.

6. To add a field to the reference field criteria and results, complete the following steps:

   a. (Global configurations only) Click Add Fields.

   b. Select the fields to add to the reference field criteria, results, or both.

   c. Click Save.

   d. Click Save Configuration.
      The field appears in the reference field criteria and results.

7. To remove a field from the reference field criteria and results, complete the following steps:

   a. Click the Mark for Deletion icon next to the field you want to remove from the reference field criteria and results.

   b. Click Save.

   c. Click Save Configuration.
      The field does not appear in the reference field criteria and results.

8. To make a previously-hidden reference field appear, complete the following steps:

   a. Click Expose Hidden Fields.

   b. Select the fields to add to the reference field criteria, results, or both.

   c. Click Save.

   d. Click Save Configuration.
      When you assign a configuration to a role, users in the role see the field in the reference field criteria and results.

9. To move a reference field to a new location, complete the following steps:

   a. Drag-and-drop the reference field to a new location in the reference field criteria and results.

   b. Click Save.

   c. Click Save Configuration.
      When you assign a configuration to a role, users in the role see the fields in the new location.

Search Configuration

This article contains the following topics:

You can configure searches to simplify how users search for information in the repository and export the results. To configure searches, complete the following tasks:

- Set a search result limit.
- Make it easier to search by assigning a default search for a role.
- Make it easier to specify search criteria by completing the following tasks:
  - Adding fields
  - Removing fields
  - Moving fields
  - Changing the field name
  - Replacing fields
- Make it easier to find information in the search results by completing the following tasks:
  - Managing Columns in Search Results (see page 1562).
  - Adding sort fields
  - Preventing duplicate records from appearing
  - Preventing the ability to open records
- Make it easier to search by allowing users to save searches.

- Make it easier to use search results in spreadsheets by allowing users to export search results.
- Delete a search that you do not need.

Set a Search Result Limit

When you search for an object and the results are difficult to manage because too many object records appear, you can set a limit. For example, when you search for assets, over 2,000 assets appear in the search results. The results are difficult to navigate, you cannot find the assets you want, and the performance is negatively impacted. Therefore, you set a maximum of 50 object records to return.

Follow these steps:

1. Click the tab and optional subtab for the search that you want to configure.

   On the left, click Manage Searches.
   A list of saved searches displays. Click a search in the list.

2. In the Additional Settings, Maximum Search Results Returning area, specify the total number of objects to appear.

   For performance reasons, we recommend that you set this value to less than 500.

3. Click Go.
   The limited search results appear and help you see the impact on the results before you save the limit. All future search results are limited to the specified number or percentage.

Assign a Default Search for a Role

You can assign a default search for a role so that all users in the role have the same default search when they click a tab or subtab. For example, all users responsible for reviewing and negotiating contracts, agreements, and services belong to the Contract and Vendor Management role. To simplify the search setup for users so they do not have to specify a default search for themselves, you configure the default legal document search. You assign the configured legal document search as the default for all users in the Contract and Vendor Management role. When users in this role click the Legal Document tab, they see the configured legal document search as their default, rather than the default legal document search provided by the product.

Consider the following information when assigning a default search for a role:

If you do not assign a default search for a role, the default search for the object appears when users in the role click the tab or subtab.

- You can assign multiple default searches for a role. However, you can only assign one default search for a particular object type (for example, model, asset, legal document, and so forth) to a role.

- When a user saves a search as their default, that search is the default for the user, even when you assign a different search as the default for the role. For example, a user in the Asset Technician role sets their default search as the asset search provided by the product. You configure the default asset search by adding a field to the search criteria and removing a field from the search results. You then assign the configured asset search as the default search for the Asset Technician role, to which the user belongs. The default asset search is the default for the user, even when you have assigned the configured asset search as the default for the role.

- A search must be available to a role before you can assign the search as the default for the role. For example, you create a legal document search. To make the search available to the Contract and Vendor Management role, assign the Contract and Vendor Management role to the search. You can then assign the legal document search as the default for the Contract and Vendor Management role.

  
  For more information about assigning a role to a search, see Search Security.

Follow these steps:

1. Click Administration, User/Role Management.
2. On the left, expand the Role Management menu.
3. Click Role Search.
4. Search for and select a role.
   The role details appear.
5. In the Default Searches area of the page, click Select New.
6. Select the default search for the role.
   The default search is added to the Default Searches list.
7. Click Save.
   The search is saved as the default for all users in the role.

Add a Field

CA APM lets you extend the information that appears in your search criteria and results by adding additional fields. For example, you can add the DNS Name field to the asset search. You can add fields to a new and saved search. You cannot add fields to the default searches provided by the product.

Follow these steps:

1. Click the tab and optional sub tab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches displays.
3. Click a search in the list.

4. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.

5. Click Add Fields.
   The Add Fields dialog appears.

6. Select the fields to add to the search criteria, results, or both.

7. At the top of the page, click CONFIGURE SEARCH: OFF.
   The configuration of the search is complete.

8. Click Save.
   The field appears in the search criteria and results.

Remove a Field

CA APM lets you remove a field when you do not want a particular field included in the search criteria. For example, you can remove the DNS Name field from the asset search.

Follow these steps:

1. Click the tab and optional sub tab for the object that you want to find.

2. On the left, click Manage Searches.
   A list of saved searches appears.

3. Click a search in the list.

4. Complete the following steps:

   a. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.

   a. Click the appropriate icon next to the field in the search criteria.

   b. At the top of the page, click CONFIGURE SEARCH: OFF.

   The configuration of the search is complete.

5. (Optional). Complete the following steps:

   a. In the search criteria area of the page, click Advanced.

   b. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.

   a. Click the Mark for Deletion icon next to the field you want to remove from the search criteria.

   b. At the top of the page, click CONFIGURE SEARCH: OFF.

The configuration of the search is complete.

6. Click Save.
   The field is removed from the page and does not appear in the search criteria.

Move a Field

CA APM lets you move a field in the search criteria to a new location to help make it easier for you to enter your search criteria. For example, you can move the Bar Code Number field so that the field appears before the Serial Number field.

Follow these steps:

1. Click the tab and optional sub tab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches displays.
3. Click a search in the list.
4. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.
   Drag-and-drop the field to a new location in the search criteria.
5. At the top of the page, click CONFIGURE SEARCH: OFF.
   The configuration of the search is complete.
6. Click Save.
   The new location of the field is saved.

Change the Field Name

CA APM lets you change the label for a field to help make the field name more familiar in your search criteria. For example, you can change the label *Asset Quantity* to *Quantity*.

Follow these steps:

1. Click the tab and optional sub tab for the object that you want to find.
2. On the left, click Manage Searches.
   A list of saved searches appears.
3. Click a search in the list.
4. Complete the following steps:

   a. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.

   a. In the search criteria, click the field label and enter the new label.

b. At the top of the page, click CONFIGURE SEARCH: OFF.

The configuration of the search is complete.

5. (Optional). Complete the following steps:

   a. In the search criteria area of the page, click Advanced.

   b. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.

   a. Click the Edit Record icon next to the field for which you want to change the label.

   b. Enter the new field label.

   c. Click the Complete Record Edit icon.

   d. At the top of the page, click CONFIGURE SEARCH: OFF.

   The configuration of the search is complete.

6. Click Save.
   The new field label appears in the search criteria.

Replace a Field

CA APM lets you replace an existing field in your *advanced* search criteria with a different field. For example, when searching for companies, you can replace the field *Company ID* with *Company Name*.

You can replace fields only in a custom search that you created. You cannot replace fields in the product default search.

Follow these steps:

1. Click the tab and optional sub tab for the object that you want to find.

2. On the left, click Manage Searches.
   A list of saved searches appears.

3. Click a search in the list.

4. Complete the following steps:

   a. In the search criteria area of the page, click Advanced.

   b. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.

a. Click the Search icon next to the field that you want to replace with a different field.
The Add Fields dialog appears.

b. Select the replacement field and click OK.

c. At the top of the page, click CONFIGURE SEARCH: OFF.

The configuration of the search is complete.

5. Click Save.
The existing field is replaced in the search criteria.

Manage Columns in Search Results

You can configure search results columns in the following ways:

- Add a new column to the search results to help make it easier for you to find the information you need in search result lists. For example, you have several people in your enterprise with the name John Smith. Their first and last names are the same, but their additional contact information (email address, supervisor, department, and so forth) is different.
You can add columns to a new and saved search. You cannot add columns to the default searches provided by the product.

- Move a column to a new location to help make it easier for you to find the information you need in the search results. For example, you can move the Asset ID column so that the column appears before the Asset Name column.

- Change the label for a column heading to help make the label more familiar in your search results. For example, you can change the label *Asset Quantity* to *Quantity*.

- Remove a column when you do not want a particular column included in the search results. For example, you can remove the Mac Address column from the search results.

Follow these steps:

1. Click the tab and optional sub tab for the object that you want to find.

2. On the left, click Manage Searches.

   A list of saved searches displays.

3. Click a search in the list. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.

4. To add a column to the search results, complete the following steps:

   a. Click Add Fields.

   b. Select the fields to add to the search results.

   c. At the top of the page, click CONFIGURE SEARCH: OFF.

d. Click Save.
The column is added to the search results.

5. To move a column to a new location, complete the following steps:

   a. In the search results list, drag-and-drop the column to a new location.

   b. At the top of the page, click CONFIGURE SEARCH: OFF.

   c. Click Save.
   The new location of the column is saved.

6. To change a column heading label, complete the following steps:

   a. In the search results, select the column heading and enter the new label.

   b. At the top of the page, click CONFIGURE SEARCH: OFF.

   c. Click Save.
   The new column label appears in the search results.

7. To remove a column, complete the following steps:

   a. In the search results, click the appropriate icon next to the column.

   b. At the top of the page, click CONFIGURE SEARCH: OFF.

   c. Click Save.
   The column is removed from the page and the search results.

Add a Sorting Field

CA APM lets you add sorting fields to the search results and extend the default sort of a single column using either ascending or descending order. For example, you currently sort assets by asset name. You can add asset family to the sorting so that you can sort on both asset name and asset family.

Follow these steps:

1. Click the tab and optional sub tab for the object that you want to find.

   a. On the left, click Manage Searches.

   b. A list of saved searches displays.

   c. Click a search in the list.

   d. At the top of the page, click CONFIGURE SEARCH: ON.

   e. The configuration of the search is enabled.

2. Click a search in the list.

3. In the Additional Settings, Search Result Sorting area, add the additional field for sorting.

4. Click Go.
   The results appear with the extended sorting and help you see the impact on the results before you save the sorting. The new field is added and you can use the field to sort the search results.

Prevent Duplicate Object Records

CA APM lets you prevent duplicate object records from appearing in the search results. For example, you have several people in your enterprise with the name John Smith. Their first and last names are the same, but their additional contact information (email address, supervisor, department, and so forth) is different.

You have a saved contact search in which only the first and last name of the contact appears in the results. When you search using the saved contact search and specify *John* as the first name and *Smith* as the last name, two instances of John Smith appear in the search results. When you prevent duplicate records from appearing, only one instance of John Smith appears.

Follow these steps:

1. Click the tab and optional sub tab for the object that you want to find.

   a. On the left, click Manage Searches.

   b. A list of saved searches displays.

   c. Click a search in the list.

   d. At the top of the page, click CONFIGURE SEARCH: ON.

   e. The configuration of the search is enabled.

2. Click the search for which you want to prevent duplicate records from appearing.

3. In the Additional Settings, Unique Search Characteristics area, select the Make Results Unique check box.

4. Click Go.
   The results appear without the duplicate records and help you see the impact on the results before you save your settings. The DISTINCT argument is added to the SQL statement, preventing duplicate records from appearing in the search results.

Prevent Opening Records

CA APM lets you disable the ability to open individual records from the search results. For example, you do not want users to open and display contact information from the contact search results.

Follow these steps:

1. Click the tab and optional sub tab for the object that you want to find.

   a. On the left, click Manage Searches.

b. A list of saved searches displays.

c. Click a search in the list.

d. At the top of the page, click CONFIGURE SEARCH: ON.

e. The configuration of the search is enabled.

2. Click a search in the list.

3. In the Additional Settings, Unique Search Characteristics area, clear the Allow Selection of Results check box.

4. Click Save.
A hyperlink does not appear in the search results to open the object.

Allow Users to Save Searches

You can grant permissions to users so a Save button appears to save searches.

Follow these steps:

1. Click the tab and optional sub tab for the object you want to configure.

2. On the left, click CONFIGURE: ON.
The configuration of the page is enabled.

3. In the Configuration Information area of the page, specify the information for the new global or local configuration (see page 1515), or select an existing configuration that you want to change.

Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. In the Permissions area of the page, complete the following steps in the Granted and Denied Permissions lists:

When you grant any combination of the following permissions, the user can save searches.

a. To allow only the current user who is logged in to save a search, move Save Search to User to the Granted Permissions list.

b. To allow the current user who is logged in and specific configurations to save a search, move Save Search to Configuration to the Granted Permissions list. The search is available to the current user and all users that you select for the configuration.

c. To allow the current user who is logged in and specific roles to save a search, move Save Search to Role to the Granted Permissions list. The search is available to the current user and all users in the roles you select.

5. Click Save Configuration.
   The configuration is saved. Verify that you correctly assign a configuration to a role.

Allow Users to Export Search Results

You can grant permissions to users so they can save exported search results.

Follow these steps:

1. Click the tab and optional subtab for the object you want to configure.

2. On the left, click CONFIGURE: ON.
   The configuration of the page is enabled.

3. In the Configuration Information area of the page, specify the information for the new global or local configuration (see page 1515), or select an existing configuration that you want to change.

   Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. In the Permissions area of the page, complete the following steps in the Granted and Denied Permissions lists:

   When you grant any combination of the following permissions, the user can save exported search results.

   a. To allow only the current user who is logged in to save the exported search results, move Export for User to the Granted Permissions list.

      When this is the only permission granted to a user, the user cannot select the Export to All Configurations assigned on Search and Export to All Roles assigned on Search check boxes when scheduling search requests. For information about scheduling search requests, see Search Results Export

(see page 2439). An email is sent to the current user only. The email includes a link to the CSV file or specifies the name of the database view, depending on the type of export.

b. To allow the current user who is logged in and specific configurations to save the exported search results, move Export for Configuration to the Granted Permissions list. The export is available to the current user and all users in the selected configurations assigned to the search used by the export.

When this permission is granted to a user, the user can select the Export to All Configurations assigned on Search check box when scheduling search requests. For information about scheduling search requests, see Search Results Export (see page 2439). An email is sent to all users in the selected configurations. The email includes a link to the CSV file or specifies the name of the database view, depending on the type of export.

c. To allow the current user who is logged in and specific roles to save the exported search results, move Export for Role to the Granted Permissions list. The export is available to the current user and all users in the selected roles assigned to the search used by the export.

When this permission is granted to a user, the user can select the Export to All Roles assigned on Search check box when scheduling search requests. For information about scheduling search requests, see Search Results Export (see page 2439). An email is sent to all users in the selected roles. The email includes a link to the CSV file or specifies the name of the database view, depending on the type of export.

5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.
   The configuration is saved. Verify that you can correctly assign a configuration to a role.

Delete Saved Searches

As an Administrator, you can delete user-defined searches if they are not in use for long time.

Note: You cannot delete searches that are out-of-box.

Follow these steps:

1. Click the tab and optional sub tab for the object that you want to find.
2. On the left, click Manage Searches.
3. Under Search Results, select the user-defined search you want delete.
4. Click Delete.

Administering CA Asset Portfolio Management

This section contains the following articles:

Administration

The overall administration of CA APM involves setting up security, configuring the user interface, managing hardware reconciliation, and optionally changing configuration settings for product components. The product administration is flexible and you can complete the following administration tasks in any order that you want.

After you complete the following tasks, provide the CA APM URL and login credentials to all users so that they can log in to the product.

- **Security**
  You define security to control user access to the product and features. For example, you can provide one user with access to models and assets, and another user with access to legal documents.

  
  For more information, see Security (see page 1570).

- **User Interface Configuration**
  You configure the user interface to simplify how users enter, manage, and search for data. In addition, you secure and protect users from performing unauthorized tasks and ensure that you conform to your IT asset management practices. For example, you can globally hide the Contact page from all CA APM users. However, there are some users who must be able to see and update contact information. Therefore, you make the Contact page appear for those users. User interface configuration is flexible, and you can configure almost all aspects of the user interface.

  
  For more information, see How to Configure the User Interface (see page 1520).

- **Hardware Reconciliation**
  You use hardware reconciliation to match *discovered assets* to their corresponding *owned assets* from different logical repositories and manage your assets. You can identify unauthorized, missing, under-utilized, and over-utilized assets, which helps you to optimize your hardware asset base.

  
  For more information, see Hardware Reconciliation (see page 2404).

- **Product Components**
  You can change the product component configurations that were set up during the product installation. For example, you can change the listening port for Oracle. You can also add components to additional servers to maintain product performance and enable product scalability. For example, you can add a Hardware Reconciliation Engine on an additional server. The configuration is flexible, and you can change many component settings.

  
  For more information, see Configure a Product Component (see page 1586) and Add Component Servers (see page 1568).

Log In to CA APM

After the product is installed, your implementer verifies that all services are started and starts the web interface to verify that CA APM is ready to use. The implementer provides you with the URL and credentials to log in to the product. You can then prepare the product for users to manage assets.

By default, the login credentials (username and password) for the default System Administrator user are uapmadmin. You can change the password to meet your requirements by changing the settings for the CA EEM component.

The default password can also be changed during the installation process.

Maintaining Security

This article contains the following topics:

Security

Before you allow user access to CA APM, set up security to control access to the product, protect your repository from unauthorized or inaccurate changes, and make necessary data available to users. For example, you can provide one user with access to models and assets, and another user with access to legal documents.

Setting up security involves the following tasks:

1. Users (see page 1571). Define the users who can access the product.

2. User Roles (see page 1574). Define groups of users who perform similar tasks.
3. Authentication (see page 1581). Define how users are authenticated when they log in.
4. Searches (see page 1583). Define which users can use searches.
5. Configuration. Protect users from performing unauthorized tasks.

One or more system administrators perform these security tasks in CA APM. A system administrator with the user ID *uapmadmin* acts as a global system administrator, with complete control over all security aspects of the product.

You enforce security across the enterprise by using the web interface. Minimal database skills are required to perform these tasks.

Users

You establish user security when you add new users to the product and assign a user ID and password. If a user does not have a valid user ID and password, they cannot log in. For each person, a user record is established, and the record is associated with a contact in the ca_contact table.

You can add users to the product in the following ways:

1. Import them.
2. Manually define them.

When manually defining users, you can immediately authorize them to use the product. However, when you import users, import them first, and then you can authorize them.

When you define a user manually, a corresponding CA EEM user is also created. CA EEM verifies the user name and password when the user logs in to CA APM.

After you define all CA APM users, assign each user to a *user role* and assign the entire role access rights to determine what they see and can access when they log in.

Best Practices (Users and Roles)

Use the following best practices to effectively manage users and roles:

- A user must have a valid user ID and password, and be authorized, to log in.
- Remove a user from a role before assigning a new role to the user.

  The product does not allow you to assign a user to more than one role.

- Verify that there are no users assigned to a role before deleting the role.

- Delete users before deleting a role.

Import and Synchronize Users

Important! Verify that the user completing this task belongs to a role in which user management access is enabled.

You can import a list of users from an external user store such as an active directory through CA EEM, and synchronize them to be saved as contacts in CA APM. Importing users helps you to save time when defining your users, and helps ensure the accuracy of the user information. After you import and save the users, authorize them to access the product.

Follow these steps:

1. Click Administration, User/Role Management.
2. On the left, expand the User Management menu.
3. Click LDAP Data Import and Sync.
4. If multi-tenancy is enabled, select a tenant from the drop-down list.
5. Click Start LDAP Data Import and Sync.
   The import process begins and users are imported from the external store. If multi-tenancy is enabled, users are imported for the selected tenant as contacts into the ca_contact table. You can then authorize the imported users to access the product.

The LDAP Data Import and Sync works for user names that begin with a letter or number. User names that begin with a special character are not imported.

Define a User

Important! Verify that the user completing this task belongs to a role in which user management access is enabled.

You define all users of CA APM and provide them with access to the product. After you define a user, assign a role to the user.

Follow these steps:

1. Click Administration, User/Role Management.
2. On the left, expand the User Management menu.

3. Click New User.
4. Enter the information for the new user and the contact-related information.
5. (Optional) Specify if you want to authorize the user to access to the product.
6. Click Save.
   The user is defined.

Authorize a User

Important! Verify that the user completing this task belongs to a role in which user management access is enabled.

You can authorize a user so they can log in and use the product. Before you can authorize a user, save the user as a contact.

Follow these steps:

1. Click Administration, User/Role Management.
2. On the left, expand the User Management menu.
3. Click Authorize Users.
4. Search to find the list of available users.
5. Select the user you want to authorize and click OK.
   The user appears in the Authorized Users list.
6. Click the Edit icon next to the user name.
7. (Optional) Select a contact to assign a user with contact details.

   If you do not select a contact, a new contact is created for the user.

8. (Optional) Select a role to assign to the user.
9. Click Authorize.
   The selected user is authorized to log in to the product.

Deny a User Access

> **Important!** Verify that the user completing this task belongs to a role in which user management access is enabled.

You can deny a user access and prevent them from logging in to the product. For example, you hire a new asset technician and want to prevent them from using the product until they have received proper training. When you deny a user access, the contact information for the user is not deleted from the product.

Follow these steps:

1. Click Administration, User/Role Management.
2. On the left, expand the User Management menu.
3. Click Authorize Users.
4. Select the user for which you want to deny access from the Authorized Users list.
5. Click De-Authorize.
   The user is prevented from logging in to the product.

User Roles

A *user role* is the primary record that controls security and user interface navigation in the product. Each role defines a focused view of the product by exposing only the functionality necessary for users to perform the tasks that are assigned to their business roles. The default role for a user and the associated user interface configuration determine the data and functions that are available to the user. A user can belong to only a single role.

Define user roles to apply functional and field-level repository access rights. You determine and assign the level of access that is required for each role. Group the users with the same job function and assign them the corresponding role. Role assignment prevents the users from performing unauthorized tasks, such as adding or deleting data. For example, users in an Administrator role need full access to all records, while users in an Asset Technician role need limited access to fewer records.

> The product contains predefined System Administrator and user roles that you can use as the basis for user management.

You can perform several tasks to set up and manage user roles:

- Define a role.
- Assign a role to a user.

- Remove a user from a role.
- Update a role.
- Delete a role.
- Assign a configuration to a role.

Predefined Roles

The product provides a System Administrator role, which has complete control and access to all objects and tenant data. This role is associated with the System Administrator contact and cannot be deleted. A user in this role can define, update, and delete objects, in addition to defining and updating more roles to meet your business requirements. You cannot assign a configuration to the System Administrator role.

The product also provides the following predefined user roles to help you manage users:

- CA APM Asset Technician - Provides access to the data and functions that are required for working with asset information only.
- CA APM Contract Manager - Provides access to the data and functions that are required for working with legal documents and the contract management process only.
- CA APM Default User - Provides read-only access to a limited view of the product. This role can view most of the data in the product. However, this role cannot modify the product data.
- CA APM Fulfiller - Provides access to the data and functions that are required for asset fulfillment tasks only.
- CA APM Receiving - Provides access to the data and functions that are required for updating assets that are received from a fulfillment process only.

Each predefined user role has associated configurations, which provide access to the data that is required to complete the particular function. You can modify the configurations that are associated with each predefined role. The predefined roles are available only after a new installation.

Define a User Role

Important! Verify that the user completing this task belongs to a role in which role management access is enabled.

You can define customized user roles to meet your site-specific business requirements. For example, you can define one role with access to reconciliation management, and another with access to asset fulfillment.

Follow these steps:

1. Click Administration, User/Role Management.

2. On the left, expand the Role Management menu.

3. Click New Role.

4. Enter the information for the role.

   - **User Management Access**
     Select this check box so a user assigned to the role can access the user management functionality (Administration, User/Role Management, User Management). The User/Role Management subtab is available only when the role has access to the user management functionality, the role management functionality, or both.

   - **Role Management Access**
     Select this check box so a user assigned to the role can access the role management functionality (Administration, User/Role Management, Role Management). The User/Role Management subtab is available only when the role has access to the user management functionality, the role management functionality, or both.

   - **System Configuration Access**
     Select this check box so a user assigned to the role can access the system configuration functionality (Administration, System Configuration).

   - **Web Services Access**
     Select this check box so a user assigned to the role can access the CA APM web services documentation and WSDL (Administration, Web Services). If this check box is not selected and a user in the role attempts to access the web services from an external client application, the user receives a login error.

   - **Filter Management Access**
     Select this check box so a user assigned to the role can access the filter management functionality (Administration, Filter Management).

   - **Other Information Configuration Access**
     Select this check box so a user assigned to the role can access the Other Information Configuration functionality. This function allows the user to access additional related information for selected objects. The user can access this additional information by selecting menu items under Relationships on the left side of the page.

   - **Data Importer User Access**
     Select this check box so a user assigned to the role can access the Data Importer functionality (Administration, Data Importer) with user permissions. Users can create imports and can modify or delete their own imports. Users can also view any import that was created by another user.

   - **Data Importer Admin Access**
     Select this check box so a user assigned to the role can access the Data Importer functionality (Administration, Data Importer) with administrator permissions. Administrators can create imports and can modify or delete any import that was created by any user.

   - **Reconciliation Management Access**
     Select this check box so a user assigned to the role can access the reconciliation rules management functionality (Administration, Reconciliation Management).

- **Asset Fulfillment Access**
  Select this check box so a CA Service Catalog user assigned to the role can perform asset fulfillment using CA Service Catalog.

- **Tenancy Admin Access**
  Select this check box so a user assigned to the role can access the multi-tenancy administration functionality to enable multi-tenancy, define tenants, define subtenants, and define tenant groups (Administration, Tenancy Management).

- **Normalization Access**
  Select this check box so a user assigned to the role can access the normalization rules management functionality (Directory, List Management, Normalization).

- **Mass Change Utilities Access**
  Select this check box so a user assigned to the role can access the Mass Change Utilities functionality. This function allows the user to change the asset family for a model and also to change the model for an asset.

5. (Optional) Specify the read/write permissions for tenants. Multi-tenancy expands the purpose of the role to control the tenant or tenant group that a user within the role can access. When multi-tenancy is enabled, the Tenant Information section includes Tenant Access Read and Tenant Access Write drop-down lists.

   The Tenant Information section is visible only when multi-tenancy is enabled. For information about how to enable multi-tenancy, see Implementing Multi-Tenancy (see page 1606). In addition, users associated with a tenant other than the service provider can only create or update objects associated with their own tenant. Only users associated with the service provider are permitted to create or update objects belonging to tenants other than their own.

   - **All Tenants**
     Contains no tenant restrictions. A user in a role with this access can view any object in the database (including public objects). In addition, a user associated with the service provider can update or create objects associated with any tenant. When a service provider user with this access creates an object, the product requires the user to select the tenant of the new object.

   - **Contact's Tenant**
     (Default value) Associates the role with the tenant of the contact. The product restricts a user in a role with this access to viewing, creating, and updating only those objects associated with their own tenant (and to view public objects). When a user with this access creates an object, the user cannot select a tenant. The tenant is automatically set to the tenant for the contact.

   - **Contact's Tenant Group**
     Associates the role with the tenant group of the contact. The product restricts a user in a role with this access to viewing, creating, and updating only those objects associated with the tenants in their tenant group (and to view public objects). When a user with this access creates an object, the user can select any tenant belonging to the tenant group.

- **Single Tenant**
  Associates the role with a named tenant. When you select this option, select a specific tenant in either the Tenant Write or Tenant Read field. The product restricts a user in a role with this access to viewing, creating, and updating only those objects associated with the tenant you select (and to viewing public objects). When a user with this access creates an object, the user cannot select a tenant. The tenant is automatically set to the tenant you select.

  Note: Only a service provider user can create or update data for a tenant other than their own. A tenant user in a role with single tenant access to another tenant is restricted to read access.

- **Tenant Group**
  Associates the role with a named tenant group. When you select this option, select a specific tenant group in either the Tenant Group Write or Tenant Group Read field. The product restricts a user in a role with this access to viewing only those objects that belong to any tenant in the tenant group. In addition, a user associated with the service provider can update or create objects associated with any tenant in the group. When a service provider user with this access creates an object, the product requires the user to select the tenant for the new object.

- **Update Public (check box)**
  Available only when you select All Tenants. Select this check box to authorize a user in the role to create or delete tenanted public data.

6. Click Save.
   The role is defined and you can assign users to the role.

Assign a Role to a User

Important! Verify that the user completing this task belongs to a role in which role management access is enabled. In addition, if you do not assign a role to a user, the Administration tab is hidden from the user.

You can assign a role to a user to define a focused view of the product and determine what they see when they log in. For example, assign an administrator to the system configuration role. You can assign a user to only a single role. Save a user as a contact before you assign the user to a role.

Note: Remove a user from their previous role before assigning a new role to the user.

Follow these steps:

1. Click Administration, User/Role Management.

2. On the left, expand the Role Management menu.
3. Click Role Search.
4. In the Role Contact area of the page, click Assign Contact.
   All users not assigned to a role appear.
5. Select the user for which you want to assign the role.
6. Click OK.
7. Click Save.
   The role is assigned to the user.

Remove a User from a Role

Important! Verify that the user completing this task belongs to a role in which role management access is enabled.

You can restrict the access rights for a user by removing them from a role. For example, an administrator is transferred to a different department and you remove them from the system configuration role. Remove a user from a role before assigning them to another role, or if they are no longer a part of your site or organization.

Follow these steps:

1. Click Administration, User/Role Management.
2. On the left, expand the Role Management menu.
3. Click Role Search.
4. Click the delete icon next to the user you want to remove from the role.
5. Click Save.
   The user is removed from the role.

Update a User Role

Important! Verify that the user completing this task belongs to a role in which role management access is enabled.

At any time, you can update a user role to change what the user sees when they log in to the product. For example, the users in a particular role no longer perform tenancy management functions. In this situation, remove the tenancy management access for the role.

Important! You can delete a role that is no longer active in your site or organization, or when the role functions are no longer required. You cannot delete the predefined System Administrator role (see page 1575).

Follow these steps:

1. Click Administration, User/Role Management.
2. On the left, expand the Role Management menu.
3. Click Role Search.
4. Search for and select a role.
5. To update the user role, change the information for the role and click Save.
   The role is updated.
6. To delete the user role, click Delete.
   The role is deleted.

Assign a Configuration to a Role

Important! Verify that the user completing this task belongs to a role in which role management access is enabled.

You can configure the user interface to simplify how users enter, manage, and search for data. When you assign a configuration to a role, you help ensure that any user assigned to the role sees the product as you have configured it for them.

Example: Assign a configuration to an asset manager

In this example, an asset manager must quickly view, and monitor the most important information that has been entered into the product for an asset. This information is used for reporting, cost analysis, and inventory control. The administrator configures the search results to display the asset name, model name, quantity, serial number, operating system, purchase order number, and cost center. The administrator saves the configuration and assigns it to the asset manager role. When an asset manager logs in to the product, the configuration for the asset manager role is selected and appears.

For more information about configurations, see How to Configure the User Interface (see page 1520).

Follow these steps:

1. Click Administration, User/Role Management.
2. On the left, expand the Role Management menu.
3. Click Role Search.
4. Search for and select a role.
5. Click Role Configuration.
6. Click Select New.
   The list of saved configurations appears.
7. Select the configuration you want to assign to the role.
8. Click OK.
9. Click Save.
   The configuration is assigned to the role. Any user assigned to the role sees the configuration when they log in to the product.

Authentication

Authentication is the process of obtaining identification credentials from a user such as name and password to validate their credentials to verify that the user exists. If the credentials are valid, the user is authenticated. After a user is authenticated, the authorization process determines whether the user can log in to the product.

Note: CA APM uses CA EEM to process user authentication.

The following types of authentication are supported:

- Form Authentication. A user is prompted for a user name and password to log in to the product.

  Form authentication is the default authentication type.

- Windows Integrated Authentication. A user already logged in to the Windows domain can access the product without having to provide additional login credentials.

You can provide additional security by defining tab and menu configuration in the product to restrict the pages and tabs that a user can access.

Configure Form Authentication

Verify that the user completing this task belongs to a role in which system configuration access is enabled.

You can configure form authentication so a user is prompted for a user name and password when logging in.

Follow these steps:

1. Click Administration, System Configuration.
2. On the left, click EEM.
3. Select Form from the Authentication Type drop-down list.
4. Click Save.
   Form authentication is enabled.

Configure Windows Integrated Authentication

Verify that the user completing this task belongs to a role in which system configuration access is enabled.

You can configure Windows integrated authentication and reference the CA EEM server to the active directory used for authentication. With Windows integrated authentication enabled, a user already logged in to the Windows domain can access the product without having to provide any additional login credentials.

You can also configure Windows integrated authentication with CA EEM and CA SiteMinder. CA SiteMinder uses the active directory for authentication. For information about this configuration, see the CA EEM product documentation.

For Windows integrated authentication to work, the CA EEM server, the Active Directory, and the client computer making the authentication request must belong to the same domain.

In addition, when you create and authorize a user in the CA EEM local store with a user name that exists in the Active Directory, the corresponding Active Directory user is automatically authorized.

Follow these steps:

1. On the computer where CA EEM is installed, configure the CA EEM server to reference your Active Directory or LDAP system.

For information about performing these functions, see the CA EEM product documentation.

2. In CA APM, click Administration, System Configuration.
3. On the left, click EEM.
4. Select Windows Integrated from the Authentication Type drop-down list.
5. Click Save.
   Windows integrated authentication is enabled.

Single Sign-On

Single sign-on is an authentication process where the user can enter one user ID and password and access a number of resources within the organization. Single sign-on eliminates the need to enter additional authentication credentials when switching from one solution to another.

Single sign-on lets users log in to the product automatically using Windows login information. After you add the user ID to any role, the product verifies the login credentials and displays the appropriate home page to the user.

For single sign-on to work correctly, configure Windows user accounts as domain user accounts, and not as the local user accounts.

Search Security

Default searches let you find objects in the repository. For example, use the default searches to find assets, models, contacts, and so forth. The security for the default searches makes them available to all users and configurations. You can use these searches to create additional searches.

In contrast, you can apply security to the searches that you create to limit who can use the search. When you save a configured search, you can select specific user roles and configurations (restricted to administrators). By default, the security for the searches you create makes them available to all users and configurations. By applying unique security to your searches, you help ensure that certain users cannot view sensitive information that a search returns.

Consider the following information when applying security to searches:

- You can access all searches (default and user-defined searches) so that you can configure and troubleshoot searches for users.
- You can access all scheduled searches and exports so that you can configure and troubleshoot scheduled searches and exports for users.

- All users that are assigned to a role and configuration can access the default searches and the user-defined searches that are assigned to the role and configuration. However, the search results that users see for the default searches do not display information and fields that you hide and secure.

- When a default and user-defined search becomes invalid because of configuration changes, you may not need the search. You can delete any default and user-defined search in CA APM.

Troubleshooting Search Security

Troubleshooting tips related to search security help you when working with configured searches.

- Role Cannot Be Assigned to a Configured Search (see page 1584)

- Configuration Cannot Be Assigned to a Configured Search (see page 1584)

Role Cannot Be Assigned to a Configured Search

Valid on all supported operating environments.

Symptom:

When attempting to provide a role with access to a configured search, I receive an error similar to one of the following errors:

You cannot assign role <role name> to the search because the role cannot access the following field (s): <field name> on Asset Type <asset family>

You cannot assign role <role name> to the search because the role cannot access the Asset Type <asset family>

You cannot assign role <role name> to the search because the configuration cannot access the following field(s): <field name>, <field name>

Solution:

Use any of the following solutions to resolve this error:

1. Update the configuration and provide the role or user with access to the search.

2. Update the configuration and remove the hidden field from the search.

3. Do not allow the role to access the search.

4. Remove the configuration from the role.

Configuration Cannot Be Assigned to a Configured Search

Valid on all supported operating environments.

Symptom:

When attempting to provide a global or local configuration with access to a configured search, I receive an error similar to one of the following errors:

You cannot assign configuration <configuration name> to the search because the configuration cannot access the following field(s): <field name> on Asset Type <asset family>

You cannot assign configuration <configuration name> to the search because the configuration cannot access the Asset Type <asset family>

You cannot assign configuration <configuration name> to the search because the configuration cannot access the following field(s): <field name>, <field name>

Solution:

Use any of the following solutions to resolve this error:

1. Update the configuration and make the hidden field available to the search.
2. Update the configuration and remove the hidden field from the search.
3. Do not allow the configuration to access the search.

Managing Product Components

This article contains the following topics:

- Modify the Debugging Level for Component Service Log Files (see page 1605)

Product Components

After you install CA APM, you can manually configure many of the product components. In addition, you can add components to additional servers to maintain optimum performance and enable scalability. For example, you can add a Hardware Reconciliation Engine or an additional component server. The configuration is flexible, and you can change many component settings.

For a description of each product component, see the Step 9: Configure Product Components (see page 319).

Configure a Product Component

Verify that the user completing this task belongs to a role in which system configuration access is enabled.

You can change the component configurations that were set up during the product installation. For example, you can change the name of the SMTP server that is used to send email.

Follow these steps:

1. Click Administration, System Configuration.
2. On the left, select the product component.
3. Enter the new configuration settings for the component:
   - Database
     - Oracle (see page 1587)
     - SQL Server (see page 1589)
   - Web Server (see page 1590)
   - Application Server (see page 1592)
   - Hardware Reconciliation Engine (see page 1593)
   - CA EEM (see page 1594)
   - Export Service (see page 1595)
   - Data Importer (see page 1596)

- Data Importer Engine (see page 1596)
- LDAP Data Import and Sync Service (see page 1597)
- CORA (see page 1597)
- Storage Manager Service (see page 1598)
- Event Service (see page 1598)
- Common Asset Viewer (see page 1600)
- WCF Service (see page 1601)
- SAM - Import Driver (see page 1601)
- Software Asset Management (see page 1602)

4. Click Save.
   The configuration settings are saved.

Oracle Database Configuration Settings

After you install the product, if you are using Oracle as the database for the CA MDB, you can change the settings for the Oracle database server.

The following fields require explanation:

- **DBA User Name**
  The user name for connecting to the target database. The user name must be for a privileged user.
  Default: sys

- **Listen Port**
  The database connection port.
  Default: 1521

- **Oracle Service Name**
  The service name for the target database.
  Default: orcl

- **Oracle Net Service Name**
  The net service name for the target database.
  Default: orcl

- **Tablespace Path**
  The location of the Oracle tablespaces.
  Default: c:\oracle\product\10.2.0\oradata\orcl

- **Data Tablespace Name**
  The name of the data tablespace.
  Default: MDB_DATA

- **Data Tablespace Size**
  The amount of disk space to be allocated for the data tablespace.
  Default: 400 MB

- **Index Tablespace Name**
  The name of the index tablespace.
  Default: MDB_INDEX

- **Index Tablespace Size**
  The amount of disk space to be allocated for the index tablespace.
  Default: 100 MB

- **mdbadmin Password**
  The password that is associated with the mdbadmin user. If a new CA MDB is being created, this is the password that is assigned to the mdbadmin user.

- **Command Timeout**
  The maximum amount of time that the application waits for a response from the database.

- **Stored Procedure Command Timeout**
  The maximum amount of time that the application waits for a response from the database stored procedures.

- **Max Connection Pool Size**
  The maximum number of requests that the database can process simultaneously.

- **Enable CORA Connection Pooling**
  Placeholder for the flag that enables CORA connection pooling. Currently, CORA does not support connection pooling.

- **CORA Connection Pool Lifetime**
  Placeholder for the lifetime of the CORA connection pool. Currently, CORA does not support connection pooling.

- **CORA Connection Pool Size**
  Placeholder for the size of the CORA connection pool. Currently, CORA does not support connection pooling.

- **Last Run Date Option**
  Determines if the imported data should update the existing CA APM data. CA APM receives discovered hardware data imports and uses the data to match ownership and discovery data. CA APM determines if the imported data is more current than the existing data by comparing their inventory dates. Then CA APM decides whether the imported data should update the existing CA APM data.

  Default: 2
  See the following table for a description of all valid options.

Option	Definition
1	Always update the existing CA APM data with the imported data.
2	

Option	Definition
	(Default) Update the existing CA APM data only if the inventory date of the imported asset is more current than the inventory date of the existing asset. If the imported asset does not have an inventory date, an error occurs and the imported asset data does not update the existing CA APM data.
3	Update the existing CA APM data only if the inventory date of the imported asset is more current than the inventory date of the existing asset. If the imported asset does not have an inventory date, update the existing CA APM data with the imported data.

SQL Server Database Configuration Settings

After you install the product, if you are using SQL Server as the database for the CA MDB, you can change the settings for the SQL Server database server.

The following fields require explanation:

- **SQL Server Login**
  The user name for connecting to the target database. The user name must have sysadmin role privileges assigned in SQL Server.
  Default: sa

- **SQL Server TCP/IP Port**
  The database connection port.
  Default: 1433

- **Command Timeout**
  The maximum amount of time that the product waits for a response from the database.

- **Stored Procedure Command Timeout**
  The maximum amount of time that the product waits for a response from the database stored procedures.

- **Max Connection Pool Size**
  The maximum number of requests that the database can process simultaneously.

- **Enable CORA Connection Pooling**
  Placeholder for the flag that enables CORA connection pooling. Currently, CORA does not support connection pooling.

- **CORA Connection Pool Lifetime**
  Placeholder for the lifetime of the CORA connection pool. Currently, CORA does not support connection pooling.

- **CORA Connection Pool Size**
  Placeholder for the size of the CORA connection pool. Currently, CORA does not support connection pooling.

- **SQL Server Host Name**
  The host name of the server that is used for SQL Server.

- **Last Run Date Option**
  Determines if the imported data should update the existing CA APM data. CA APM receives discovered hardware data imports and uses the data to match ownership and discovery data. CA APM determines if the imported data is more current than the existing data by comparing their inventory dates. Then CA APM decides whether the imported data should update the existing CA APM data.

  Default: 2
  See the following table for a description of all valid options.

Option	Definition
1	Always update the existing CA APM data with the imported data.
2	(Default) Update the existing CA APM data only if the inventory date of the imported asset is more current than the inventory date of the existing asset. If the imported asset does not have an inventory date, an error occurs and the imported asset data does not update the existing CA APM data.
3	Update the existing CA APM data only if the inventory date of the imported asset is more current than the inventory date of the existing asset. If the imported asset does not have an inventory date, update the existing CA APM data with the imported data.

Web Server Configuration Settings

After you install the product, you can change the settings for the web server.

The following fields require explanation:

- **Web Server or Load Balancer IP/Host**

  The CA APM installation, by default, sets this field to the web server host name.

  - In a single web server environment, you can enter the web server host name, or the web server IP address.
  - In a multiple web server environment, you can enter either the web server host name, or the IP address of the Load Balancer.

  Note: The web server can be registered with a different name in the Domain Name System (DNS) than what is registered as the web server host name. In this situation, specify the different name in this field.

- **Authentication Timeout**
  Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the product and must log in again.
  Default: 3600000 (6 minutes)

- **State Data**
  The temporary view data that is stored at the server side for each user until the user logs off. This data can be stored either in the database or on the web server file system. The value of State Data can be SERVER (FileSystem) or DATABASE.

- **Cache Timeout**
  The elapsed time-out period for cached files to be deleted from the store.
  When a user logs in, along with view data, documents are stored in system memory (Cache). If the user is not referring to these documents, the documents become stale. After some time, these documents are deleted. The time limit is the Cache Timeout.

- **Auto complete Result Count**
  The number of values to display in the Auto Complete drop-down lists. In fields with lists, the user can start to type a value and the product provides a list of matching values. The user can then select a value from this Auto Complete list.

  Note: If you set a low number for this parameter, the Auto Complete list may not be useful since the user will have to type most of the value before finding it in the list. If you set a high number for this parameter, the list could perform slowly.

- **Homepage**
  The default CA APM home page that is opened after the user logs in.

- **SM Web Service Protocol**
  The protocol that is used to access the Storage Manager Service.
  The Storage Manager Service provides file storage facility to other product components. When the other components want to interact with the Storage Manager Service, the components use this protocol.

- **SM Web Service Port**
  The port on which the Storage Manager Service is running.
  This port is the HTTP port on which the Storage Manager Service is hosted. The default port is 80. If the Storage Manager Service is configured to host on a different port, that port number is shown.

- **EEM Backend**
  The name of the server where CA EEM is installed. This value is populated during installation.

- **Reporting Web Service Server**
  The CA Business Intelligence server name and port. This value is populated during installation.

- **Reporting Timeout**
  The time-out in seconds for a connection to the CA Business Intelligence (reporting) web service.

- **Reporting Name**
  The name of the CA Business Intelligence (reporting) engine. This name is always "Allegheny Reporting Engine".

- **Reporting User**
  The CA Business Intelligence (reporting) user with administrative privileges.

- **Reporting Password**
  The password for the Reporting User.

- **External AuthHeader**
  This header works with the External setting of Authentication Type on the CA EEM configuration. The external authentication mechanism sets information in the HTTP header for the CA APM web pages to receive. One piece of information is the User Id. The External AuthHeader is the name of the variable external authentication that sets the User Id value. The External AuthHeader setting must match the configured setting in the external authentication for which the User Id is provided.

- **From Address**
  The From email address for the notifications that are sent from the Event Service.

- **To List**
  The list of recipients who receive the email notifications about issues from the Event Service.

- **Cc List**
  The list of recipients in the Cc list who receive the email notifications about issues from the Event Service.

- **Bcc List**
  The list of recipients in the Bcc list who receive the email notifications about issues from the Event Service.

- **Email Subject**
  The subject line in the email notification about issues that the Event Service sends to the recipients in the To List, Cc List, and Bcc List.

Note: If you change the setting on Administration, System Configuration, Web Server for the Web Server Protocol or the Web Server or Load Balancer IP/Host, you must restart the Windows service for CA Asset Portfolio Management - Export Service.

Application Server Configuration Settings

After you install the product, you can change the settings for the application server.

The following fields require explanation:

- **Application Server or Load Balancer IP/Host**

  The CA APM installation, by default, sets this field to the application server host name.

  - In a single application server environment, you can enter the application server host name, or the application server IP address.

  - In a multiple application server environment, you can enter either the application server host name, or the IP address of the Load Balancer.

The application server can be registered with a different name in the Domain Name System (DNS) than what is registered as the application server host name. In this situation, specify the different name in this field.

- **Authentication Timeout**
  Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the product and must log in again.
  Default: 3600000 (6 minutes)

- **EEM Backend**
  The name of the server where CA EEM is installed. This value is populated during installation.

- **USM Web Service URL**
  The URL for the USM web service. This value is used when the product is integrated with CA Service Catalog or CA Service Desk Manager.

If you change the setting on Administration, System Configuration, Application Server for the Web Service Protocol or the Application Server or Load Balancer IP/Host, you must restart the following Windows services:

- CA Asset Portfolio Management - Export Service
- CA Asset Portfolio Management - Event Service
- CA Asset Portfolio Management - HW Reconciliation Engine
- CA Asset Portfolio Management - LDAP Import Service

Hardware Reconciliation Engine Configuration Settings

After you install the product, you can change the settings for the Hardware Reconciliation Engine.

The following fields require explanation:

- **Message Queue Retention**
  Number of days that records remain in the message queue before the Hardware Reconciliation Engine purges them.
  Default: 7

- **Refresh Lock Record Count**
  Engine performance tuning setting that works with the Lock Stale Interval setting. The number of records that the Hardware Reconciliation Engine adds or updates before refreshing the lock on the reconciliation rule record. If the lock refresh does not happen within the number of seconds specified in the Lock Stale Interval setting, the reconciliation rule record is available to another Hardware Reconciliation Engine.
  Default: 100

- **Lock Stale Interval**
  Engine performance tuning setting that works with the Refresh Lock Record Count setting. If the lock refresh does not happen on the reconciliation rule, the amount of time, in seconds, after which a reconciliation rule record is available to another Hardware Reconciliation Engine.
  Default: 600

- **Web Service Authentication Timeout**
  Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the service and must log in again.
  Default: 3600000 (6 minutes)

- **Processing Mode**
  Specifies whether the Hardware Reconciliation Engine processes continuously. The product supports the following option:

  - **0**
    Process in continuous reconciliation mode.

- **Engine Snooze Time**
  Amount of time, in milliseconds, that the Hardware Reconciliation Engine waits between processing cycles.
  Default: 300000 (5 minutes)

- **Connection Retry Time**
  Amount of time, in milliseconds, that the Hardware Reconciliation Engine waits between attempts to connect to the database.
  Default: 60000 (1 minute)

- **Engine Debug Level**
  Debug level for the message queue. The levels are Fatal, Error, Warning, Info, and Debug.
  Default: Fatal

- **Web Service Batch Size**
  Number of records that are sent to the web service at one time for update processing.
  Default: 50

- **Pending Modification Retention**
  Number of days that pending modification requests remain in the queue before the Hardware Reconciliation Engine purges them. This setting affects any tenant that is processed by the Hardware Reconciliation Engine.
  Default: 7

CA EEM Configuration Settings

After you install the product, you can change the settings for CA EEM.

The following fields require explanation:

- **Authentication Type**
  Type of authentication allowed:

  - **Form**. A user is prompted for a user name and password to log in to the product.

- **Windows Integrated**. A user who is already logged in to the Windows domain can access the product without having to provide additional login credentials.

- **External**. A user is authenticated by an external access management system, for example, CA SiteMinder.

Default: Form

- **uapmadmin Password**
  Password for the uapmadmin user to access the web and application servers.

Export Service Configuration Settings

After you install the product, you can change the settings for the Export Service.

The following fields require explanation:

- **On Demand Request Period**
  Amount of time, in milliseconds, that the Export Service waits between On Demand Request processing cycles.
  Default: 5000 (5 seconds)

- **On Demand Maximum Threads**
  Number of On Demand Request processing threads.
  Default: 2

- **Scheduled Requests Period**
  Frequency, in milliseconds, of Scheduled Requests processing cycles.
  Default: 7200000 (2 hours)

- **SMTP Server**
  Email server name.

- **Authentication Timeout**
  Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the product and must log in again.
  Default: 360000 (6 minutes)

- **Purge Start Time**
  Time of day, in 24-hour format (Universal Time) when the purge thread starts.
  Default: 5 (5:00 a.m. Universal Time)

- **Search Batch Size**
  Maximum number of data records returned for each search in a single export request. Changing the default value may affect performance. For example, a lower value may increase the number of web service calls that are needed to retrieve all the data, and a higher value may require a longer period of time to gather all the records.
  Default: 2000

- **SM Web Service Protocol**
  The protocol that is used to access the Storage Manager Service.

- **SM Web Service Port**
  The port on which the Storage Manager Service is running.

- **Export Service Email Address**
  The email address that is used by the Export Service for notifications.

Data Importer Configuration Settings

After you install the product, you can change the settings for the Data Importer.

The following fields require explanation:

- **Authentication Timeout**
  Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the component and must log in again.
  Default: 3600000 (6 minutes)

- **Maximum Batch Record Size**
  Maximum number of records in a Data Importer batch.
  Default: 50

Data Importer Engine Configuration Settings

After you install the product, you can change the settings for the Data Importer Engine.

The following fields require explanation:

- **SMTP Server Value**
  The email server name.

- **Scheduled Requests Period**
  The amount of time that the Data Importer Engine waits before checking for pending scheduled import requests. This value applies to scheduled data imports only.
  Default: 60000 (60 seconds)

- **On Demand Request Period**
  The amount of time that the Data Importer Engine waits before checking for pending on demand import requests. This value applies to on demand data imports only.
  Default: 60000 (60 seconds)

- **Max Batch Record Size**
  Maximum number of records in a Data Importer Engine batch.
  Default: 100

- **Max Job Threads**
  The maximum number of Data Importer Engine threads that can be running simultaneously for one import job.
  Default: 5

- **Max Import Threads**
  The maximum number of Data Importer Engine threads that can be running simultaneously for all import jobs.
  Default: 5

LDAP Data Import and Sync Service Configuration Settings

After you install the product, you can change the settings for the LDAP Data Import and Sync Service.

The following fields require explanation:

- **DB Check Time**
  Amount of time, in milliseconds, that the service checks the status (active or sleep mode). If the status is active, the service starts importing data.

- **EEM Backend**
  The name of the server where CA EEM is installed. This value is populated during installation.

CORA Configuration Settings

After you install the product, you can change the settings for CORA (CA APM Registration Service).

The following fields require explanation:

Note: Changes to the Common parameters affect the Web Server, WCF Service, Hardware Reconciliation, and Application Server components. Changes to the Registration Service parameters affect the Registration Service component.

- **(Common) Enable CORA**
  Enables Common Object Registration API features for the Web Server, WCF Service, Hardware Reconciliation, and Application Server components.
  Default: False

- **(Common) Enable CORA ID Generation**
  Allows the CORA tables to get the next CORA ID for a new record for the Web Server, WCF Service, Hardware Reconciliation, and Application Server components.
  Default: True

- **(Registration Service) Enable CORA**
  Enables the Common Object Registration API features using the Registration Service for all CA APM components.
  Default: True

- **(Registration Service) Enable CORA ID Generation**
  Allows the CORA tables to get the next CORA ID for a new record using the Registration Service for all CA APM components.
  Default: False

Storage Manager Service Configuration Settings

After you install the product, you can change the settings for the Storage Manager Service.

The following fields require explanation:

- **Purge Start Time**
  Time of day, in 24-hour format, when the Storage Manager Service starts to delete unused files.

- **Authentication Timeout**
  Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the service and must log in again.
  Default: 3600000 (6 minutes)

Event Service Configuration Settings

After you install the product, you can change the settings for the Event Service.

The following fields require explanation:

- **Provider URL**
  The URL for accessing the workflow provider (for example, CA Process Automation).
  Example: The following URL is the default CA Process Automation workflow web services URL:

  ```
  http://<wf_hostname>:<wf_tomcat_port>/itpam/soap
  ```

- **Provider Authentication Type**
  The type of authentication (user or CA EEM) to be used with the Event Service.
  Default: User (CA EEM authentication is not currently supported for the Event Service.)

- **Provider User Name**
  The user ID for logging in to the workflow provider.

- **Provider Password**
  The user password for logging in to the workflow provider.

- **Provider Process Path**
  The path for accessing the start request forms for the workflow provider. These forms must be available for the CA APM integration with the workflow provider. For more information, see your workflow provider documentation.
  Default:/

- **Number of Events to be Processed**
  The maximum number of events to be processed in one Web Service call.
  Default: 2000

- **Time of the day for Event purge (in hours, GMT)**
  The time of day, in 24-hour format (GMT), when CA APM starts to purge event definitions that are marked for deletion.
  Default: 5 (5:00 a.m. GMT)

- **CMDB Audit Share Required**
  The indicator that enables audit sharing with the CMDB.
  The CMDB common database tables can be used by multiple applications. For example, the ca_contact table is used by CA APM, CA Service Catalog, and CA Service Desk Manager when they are integrated. An audit table maintains the changes that are made to these common tables. When there is a change to any of the CMDB objects in CA APM and this value is set to true, the change audit is posted to the CMDB audit table.

- **From Address**
  The From email address for the notifications that are sent from the Event Service.

- **To List**
  The list of recipients who receive the email notifications about issues from the Event Service.

- **Cc List**
  The list of recipients in the Cc list who receive the email notifications about issues from the Event Service.

- **Bcc List**
  The list of recipients in the Bcc list who receive the email notifications about issues from the Event Service.

- **Email Subject**
  The subject line in the email notification about issues that the Event Service sends to the recipients in the To List, Cc List, and Bcc List.

- **Interval between Event Occurrence check (in milliseconds)**
  The amount of time, in milliseconds, that CA APM waits between database checks for field changes related to defined events.
  If SAM capabilities are enabled, verify that this parameter is set to 30000. If SAM capabilities are not enabled, verify that this value matches the setting in the Event Service configuration file.
  Default (without CA SAM implementation): 3600000 (1 hour)
  Default (with CA SAM implementation): 30000 (30 seconds)

- **Interval between triggering events check (in milliseconds)**
  Amount of time, in milliseconds, that CA APM waits between database checks for triggered events that need to be sent to the workflow provider.
  If SAM capabilities are enabled, verify that this parameter is set to 60000. If SAM capabilities are not enabled, verify that this value matches the setting in the Event Service configuration file.
  Default (without CA SAM implementation): 3600000 (1 hour)
  Default (with CA SAM implementation): 60000 (60 seconds)

- **Interval between triggered events status update (in milliseconds)**
  The amount of time, in milliseconds, that CA APM waits between updates to the status of triggered events that were sent to the workflow provider.
  If SAM capabilities are enabled, verify that this parameter is set to 60000. If SAM capabilities are not enabled, verify that this value matches the setting in the Event Service configuration file.
  Default (without CA SAM implementation): 3600000 (1 hour)
  Default (with CA SAM implementation): 60000 (60 seconds)

- **Interval between asset contact update (in milliseconds)**
  The amount of time, in milliseconds, that CA APM waits between updates to asset contacts in the CA CMDB.
  Default: 43200000 (12 hours)

- **CA SAM Status Update Frequency**
  The frequency for updating the status of CA SAM import jobs in the MDB (in milliseconds).
  Default: 120000 (120 seconds)

- **On Demand Max Threads**
  The maximum number of threads for processing the data synchronization between CA APM and CA SAM. The default (zero) indicates that the system creates the required number of threads, depending on the system hardware configuration. Any value other than the default value uses the same number of threads, regardless of the system configuration.
  Default: 0

- **CA SAM Events Notification Email**
  The CA APM administrator email address for receiving notifications about the CA SAM data synchronization.

- **Authorization Token**
  The token that establishes communication between the CA APM Event Service and the CA SAM Import and Export Service. This value must match the CA SAM Import and Export Service configuration setting.

  If you change this value, you must update the value of the Authorization Token for the CA SAM Import and Export Service on the CA SAM server to match this value.

For more information about events and notifications, see Events and Notifications (see page 2376).

Common Asset Viewer

After you install the product, you can change the settings for the Common Asset Viewer.

The Tomcat port number for CA APM defaults to 9080. If another product that is integrated with CA APM uses this port number, change the port number in CA APM so that you do not have a conflict.

The following fields require explanation:

- **Tomcat Port**
  Port that should be used for the Apache Tomcat server that is processing the Common Asset Viewer.
  Default: 9080

  You must first update the port in the Apache Tomcat configuration file before you change the setting in the product. For information about updating the Apache Tomcat configuration file, see Update the Apache Tomcat Configuration File (see page 314).

WCF Service Configuration Settings

After you install the product, you can change the settings for the Windows Communications Foundation (WCF) Service component.

The following fields require explanation:

- **WCF Service Load Balancer IP/Host**

  The CA APM installation, by default, sets this field to the WCF Service server host name.

  - In a single WCF Service server environment, you can enter the WCF Service server host name, or the WCF Service server IP address.
  - In a multiple WCF Service server environment, you can enter either the WCF Service server host name, or the IP address of the Load Balancer.

  Note: The WCF Service server can be registered with a different name in the Domain Name System (DNS) than what is registered as the WCF Service server host name. In this situation, specify the different name in this field.

- **Authentication Timeout (in milliseconds)**
  Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the service and must log in again.
  Default: 3600000 (6 minutes)

- **Operation Threshold**
  The maximum number of records that can be sent by or returned to the client or server. When you call the Search method from a WCF client program, this value represents the maximum number of records that can be returned to you. If you call the Create method, this value represents the maximum number of records that you can send at one time.

- **EEM Backend**
  The name of the server where CA EEM is installed. This value is populated during installation.

SAM - Import Driver Configuration Settings

After you install the product, you can change the settings for the CA SAM Import Driver.

The following fields require explanation:

- **Server**
  The name of the server where the CA SAM Import Driver component is installed.
- **Username**
  The user name that is required for adding, changing, or deleting records with the Data Importer.
- **ITAM Root Path**
  The path to the root location where the product is installed.
- **File Path**
  The path to the root location where CA SAM export files are imported.
  Example:*[ITAM Root Path]*\ITAM\Import Driver\Input
- **Data Importer Executable Path**
  The path to the Data Importer executable file (ITAM Data Importer.exe).
  Example:*[ITAM Root Path]*\ITAM\Data Importer\ITAM Data Importer.exe
- **CA SAM Server Name**
  The name of the server where CA SAM is installed.

Software Asset Management Configuration Settings

After you install the product, you can configure the settings for software asset management. After you configure these settings, restart the Apache Tomcat Common Asset Viewer service.

Also restart the Apache Tomcat Common Asset Viewer service if you change the entries in any of the following fields at a later time:

- CA SAM Web Service WSDL URL
- CA SAM Web Service Login
- CA SAM Web Service Password

The following fields require explanation:

- **CA SAM Web Client URL**

  Specifies the URL for the CA SAM home page.

  Note: You can copy the web client URL from the CA SAM home page after you log in.

  CA SAM Import Export Webservice URL

  Specifies the URL for the CA SAM web service. Use the following format:

```
http://[CA SAM System Name]:[Port Number]/SAMImportExportService/Service.svc
```

- Replace [CA SAM System Name] with the name of the CA SAM server.
- Replace [Port Number] with the port number where the CA SAM Import and Export Service is hosted.

Enable SAM Capabilities

Specifies that software asset management capabilities are enabled. If you previously had CA SCM fields on the CA APM user interface, they are removed after you select this check box.

CA SAM Web Service WSDL URL

The URL for the CA SAM Web Service Definition Language (WSDL). This URL is used to access the CA SAM web service. Use the following format:

```
http://[CA SAM System Name]:[Port Number]/prod/soap/dyn_server.php
```

- Replace [CA SAM System Name] with the name of the CA SAM server.
- Replace [Port Number] with the port number where the CA SAM Web Service is hosted.

CA SAM Web Service Login

Login name for the CA SAM web service.

Note: Verify that this login name and the CA SAM Web Service Password match the login name and password in the config_soap.inc file. This file is found in the following CA SAM installation folder path:

```
app\includes\prod\st\config_soap.inc
```

Important! The default content of the config_soap.inc file is commented. Remove the comment delimiters (/* */) and configure the login name and password.

CA SAM Web Service Password

Login password for the CA SAM web service.

CA SAM SSO Encryption Algorithm

Specifies the encryption algorithm to be used for single sign-on access to CA SAM from the CA IT Asset Manager common home page.

This entry must match the entry in CA SAM System Configuration for the security_auth_token_cipher field.

Note: For more information about CA SAM single sign-on, see the description of single sign-on in the *CA Software Asset Manager Administration Manual.*

CA SAM SSO Authentication Mechanism

Specifies the mechanism to be used for logging in to CA SAM.

This entry must match the entry in CA SAM System Configuration for the security_auth_method field.

Note: We recommend that you select auth_token_password for this mechanism. The auth_token mechanism disables the login for other CA SAM users.

CA SAM SSO Field to Authenticate User

Specifies the type of unique identifier (import ID or email address) that is used to authenticate the user.

This entry must match the entry in CA SAM System Configuration for the security_auth_token_user_identifier field.

CA SAM SSO Secret Key

Specifies the key that CA APM and CA SAM share and that is used to encrypt and decrypt the user authentication. This key ensures that CA APM users who do not have the proper authentication cannot access CA SAM.

This entry must match the entry in CA SAM System Configuration for the security_auth_token_key field.

Enable SSO from CA Asset Portfolio Management to CA Service Desk Manager

CA Service Management allows you to enable SSO from CA Asset Portfolio Management (CA APM) to CA Service Desk Manager. For more information, see Enable Single Sign-On (SSO) from CA Asset Portfolio Management to CA Service Desk Manager (see page 3251).

Add Component Servers

Verify that the user completing this task belongs to a role in which system configuration access is enabled.

After the product is installed, you can add components to additional servers to maintain optimum performance and enable scalability as your enterprise grows. You can install the following components on one or more servers:

- Web server
- Application server
- Hardware Reconciliation Engine
- Data Importer
- WCF
- Data Importer Engine

Follow these steps:

1. Click Administration, System Configuration.
2. On the left, select the product component.
3. Specify the required server connection information in the Add Component to Server section, including the administrator username and password for the server.
4. Click Add.
   The server is added to the Component Server List.
5. Enter the configuration settings for the new component server:
   - Web Server
   - Application Server
   - Hardware Engine
   - Data Importer
6. Click Save.

Install CA APM on the server you just added. For information about installing, see Implementing CA IT Asset Manager (see page 301).

Modify the Debugging Level for Component Service Log Files

The product components have corresponding Windows services. These services create log files that allow you to verify the service status and review error details. The amount of detail information in a log file depends on the specified debugging level. The default debugging level for the service log files is Fatal. You can change the default level for the Windows services by editing the log configuration file for each component.

Follow these steps:

1. Navigate to a component folder on the application server where CA APM is installed.
   Example:

   ```
   [ITAM Root Path]\ITAM\Hardware Engine
   ```

2. Open the logging.config file in a text editor (for example, Notepad).
3. Locate the debugging level value statements.
4. Edit the statements to include your debugging levels.

   The log configuration files contain comments that explain the different debugging level values.

5. Save the log configuration file.

Implementing Multi-Tenancy

This article contains the following topics:

Multi-Tenancy

Multi-tenancy is the ability for multiple independent tenants (and their users) to share a single implementation of CA APM. Tenants only interact with each other in defined ways, as specified by their roles and tenant hierarchies. Typically, unless granted access by a role or tenant hierarchy, each tenant views the CA APM implementation as solely for its own use and cannot update or view the data for another tenant.

Multi-tenancy allows tenants to share hardware and application support resources, which reduces the cost of both, while gaining many benefits of an independent implementation.

Multi-tenancy is installed automatically during the CA APM installation. After you have installed CA APM, follow the steps in this section to implement multi-tenancy.

If you integrated CA Software Asset Management (CA SAM), you can also implement CA APM multi-tenancy with CA SAM. For more information, see How to Implement Multi-tenancy with CA SAM (see page 390).

Service Provider

The *service provider* is the primary tenant (owner) in a CA APM multi-tenancy implementation. The first tenant added to a CA APM implementation is always the service provider tenant. The service provider tenant cannot have a parent tenant.

CA APM associates the privileged user (typically, uapmadmin) with the service provider tenant.

Only the service provider tenant can perform any of the following CA APM tasks:

- Define, edit, or delete tenants.
- Allow tenants to have subtenants.
- Update tenanted public data.

The CA APM administrator can grant tenant users access to data other than their own. In addition, a user role can specify separate read and write access to certain tenant groups for users within that role.

How Multi-Tenancy Works

When you enable multi-tenancy, you can grant each contact access to all tenants (public), a single tenant, or a tenant group (user-defined or product-maintained). The role for a contact controls access, which specifies read and write access independently.

If multi-tenancy is enabled, most CA APM objects include a tenant attribute that specifies the tenant that owns the object. Objects are categorized into three groups, depending on their tenant attribute and how the object is used:

- **Untenanted**

Defines objects without a tenant attribute. All data in these objects is public, and any user can create and update untenanted public data.

Tenant Required

Defines objects with a tenant attribute that cannot be null (enforced by CA APM, not the DBMS). All data in these objects is associated with individual tenants; there is no public data.

Tenant Optional

Defines objects with a tenant attribute that can be null. You can either create these objects as tenanted or public. When you select a tenant in a tenant drop-down to create an object, the object becomes a tenanted object. However, when you select the Public Data option in a tenant drop-down, the object becomes a tenanted public object. Users assigned to a role that only exposes a single tenant do not see a tenant drop-down when entering data.

When a user queries the database, the product restricts the results to objects belonging to tenants that the user is authorized to access. As a result, you never see data in tenant required tables except for the data that belongs to tenants that you are permitted to access. If the data is tenanted public data, you can see the data in tenant optional tables because the data is also public data.

When a tenant user asks to create or update a database object, the product verifies that the object belongs to a tenant that the current role for the user can update. The product also verifies that all references from the object to other objects are to public (untenanted) objects, to objects from the same tenant, or to objects from tenants in the tenant hierarchy above the tenant for the object. That is, a tenanted object is allowed to reference objects belonging to its parent tenant, to the parent of the parent, and so on.

If a user who creates an object has update access to multiple tenants, the user must specify the tenant explicitly, either directly or indirectly.

The referenced objects restriction has one exception. Certain references are permitted to reference objects that belong to tenants in the tenant hierarchy of their containing object. These references are designated as SERVICE_PROVIDER_ELIGIBLE in the CA APM object schema. The SERVICE_PROVIDER_ELIGIBLE setting makes a difference only if the service provider tenant is not in the tenant hierarchy above the tenant for the object; if the service provider tenant is in the hierarchy, tenant validation rules permit service provider references.

A service provider user asking to create or update an object is subject to the same restrictions as tenant users, except that service provider users can be authorized to create or update tenanted public objects. The defined role of the service provider user controls this authorization. A service provider user with authorization to multiple tenants who is creating a tenanted object must specify the tenant directly or indirectly.

User Interface Impact

Implementing multi-tenancy changes the user interface, depending on the authorization and tenant access associated with the role for the user.

Tenant Users

A tenant user who is restricted to a single tenant and who is not an administrator has the following user interface changes:

- Any user belonging to more than one tenant can select a tenant in a drop-down list when entering information and when generating a report.

  If you do not want a user to select a tenant when generating a report, you can remove the tenant drop-down list from the report. For more information about removing the tenant drop-down list, see Remove the Tenant Drop-Down List (see page 2430).

- Any user having read access to more than one tenant has a Tenant Name column in search results.

How to Implement Multi-Tenancy

Multi-tenancy is the ability for multiple independent tenants (and their users) to share a single implementation of CA APM. Tenants only interact with each other in defined ways, as specified by their roles and tenant hierarchies. Typically, unless granted access by a role or hierarchy, each tenant views the CA APM implementation as solely for its own use and cannot update or view data for another tenant.

To implement multi-tenancy in CA APM, complete the following steps:

1. Verify that the CA CASM service is started.
2. Verify that the user implementing multi-tenancy is assigned to a role in which multi-tenancy administration access is enabled.
3. Enable multi-tenancy.
4. Define tenants, subtenants, and tenant groups.
5. Restart the CA APM web server and application server.
6. Log in to the product using the privileged username (typically *uapmadmin*) and complete the following steps:
   a. Define user roles with tenant access.
   b. Define contacts, or import and synchronize users.
   c. Authorize users to use the product.
   d. Assign contacts to user roles.
7. Log in to the product using the privileged username and verify that the multi-tenancy restrictions are enforced.

Enable Multi-Tenancy

Enable multi-tenancy so multiple independent tenants (and their users) can share a single implementation of CA APM. Before you enable multi-tenancy, define tenants, subtenants, tenant groups, and create user roles and assign users to roles. As soon as you enable multi-tenancy, multi-tenancy enforcement is enabled. Multi-tenancy enforcement means that when an object is tenant-required, you cannot save a record without meeting the tenant restrictions.

To enable multi-tenancy

1. Click Administration, Tenancy Management.
   The Multi-Tenancy Administration page appears.
2. Click Edit.
3. In the Status drop-down list, select one of the following options:
   - **off**
     Disables multi-tenancy.
   - **on**
     Enables multi-tenancy.
4. In the Maximum Tenant Depth field, specify the maximum depth allowed for a tenant hierarchy.
5. Click Save.
   Multi-tenancy is enabled.
6. Restart the web server and application server.

Tenant, Subtenant, and Tenant Group Administration

Define the tenants, tenant groups, and subtenants to share a single implementation of CA APM. Multi-tenancy allows tenants to share hardware and application support resources, which reduces the cost of both, while gaining many benefits of an independent implementation.

Define a Tenant

You can define as many tenants as required to manage multiple separate enterprises that provide support to clients. Define a tenant before an instance of a tenant-required object can be updated.

The first created tenant, the service provider, is the primary tenant (owner) in a CA APM multi-tenancy implementation. The service provider tenant cannot have a parent tenant. After you define the service provider tenant, log out of the product and log in again as a member of the service provider. We recommend that you log in as the privileged user (uapmadmin), because this user automatically belongs to the service provider tenant.

To define a tenant

1. Click Administration, Tenancy Management.
   The Multi-Tenancy Administration page appears.

2. On the left, click Tenant.

   The Tenants page appears.

3. Click Create Tenant.
   The Create New Tenant page appears.

4. Enter the tenant information. The following fields require explanation:

   - **Tenant Number**
     (Information Only) Displays the tenant number. CA APM does not use this field.

   - **Record Status**
     Sets the tenant to active or inactive. After you define the service provider tenant, this option is read-only for the tenant.

   - **Terms of Usage**
     (Information Only) Displays the terms of usage statement for the tenant. CA APM does not use this field.

   - **Parent Tenant**
     Specifies another tenant above this tenant, making this tenant a *subtenant* in a tenant hierarchy.

   - **Subtenants Allowed**
     Allows this tenant to have subtenants. The tenant cannot modify the setting.

   - **Tenant Depth**
     (Information Only) Indicates the tenant depth of this tenant.

   - **Logo**
     (Information Only) Displays the URL for an image file that contains the logo for the tenant, which can be any web image type. CA APM does not use this field.

   - **Contact**
     Displays the Contact lookup page.

   - **Location**
     Displays the Location lookup page.

5. Click Save.
   The tenant is defined.

Update a Tenant

When necessary, you can update the information for an existing tenant.

To update a tenant

1. Click Administration, Tenancy Management.
   The Multi-Tenancy Administration page appears.

2. On the left, click Tenant.
   The Tenants page appears.

3. Search to find the tenant that you want to update.
   All tenants matching the search criteria appear in the Tenant List.

4. Click the tenant that you want to update.
   The tenant information appears.

5. Click Edit.

6. Enter the new information for the tenant.

7. Click Save.
   The tenant is updated.

Make a Tenant Active

When users must see and enter information for a particular tenant that is inactive, you can make the tenant active. For example, the service provider did not receive payment for services provided to a particular tenant. Based on the service agreement, the service provider makes the tenant inactive and stops offering services until payment is made. After the tenant provides payment for the services, the service provider makes the tenant active.

To make a tenant active

1. Click Administration, Tenancy Management.
   The Multi-Tenancy Administration page appears.

2. On the left, click Tenant.
   The Tenants page appears.

3. Search to find the tenant that you want to make active.
   All tenants matching the search criteria appear in the Tenant List.

4. Click the tenant that you want to make active.
   The tenant information appears.

5. Click Edit.

6. In the Record Status drop-down list, select Active.

7. Click Save.
   The tenant is active.

How to Initialize a New Tenant

As the service provider, you can define a standard set of data for a new tenant, such as cost centers, cost types, and departments. For information about how to import data for tenants, see Import Data (see page 1622).

Define a Tenant Group

You can define a tenant group to classify, manage, and control access to tenants. For example, you can assign asset managers to a tenant group containing tenants belonging to a particular geographic location.

To define a tenant group

1. Click Administration, Tenancy Management.
   The Multi-Tenancy Administration page appears.

2. On the left, click Tenant Group.
   The Tenant Groups page appears.

3. Click Create Tenant Group.
   The New Tenant Group Detail page appears.

4. Enter the tenant group information.

5. Click Save.
   The tenant group is defined.

6. Click Assign Tenants.
   The Tenant Search page appears.

7. Search and select the tenant that you want to add to the group.
   The tenant is added to the group.

Update a Tenant Group

You can update a tenant group to manage the group members and detail information.

To update a tenant group

1. Click Administration, Tenancy Management.
   The Multi-Tenancy Administration page appears.

2. On the left, click Tenant Group.
   The Tenant Groups page appears.

3. Search to find the tenant group that you want to update.
   All tenant groups matching the search criteria appear in the Tenant Group List.

4. Click the tenant group in the list.
   The Tenant Group Detail page appears.

5. Click Edit.

6. Enter the new information for the tenant group.

7. (Optional) Click Assign Tenants to add a tenant to the group.

   Adding or removing a tenant also adds or removes the subtenants of that tenant.

8. Click Save.
   The tenant group is updated.

Tenant Hierarchies

A *tenant hierarchy* is a structured tenant group that is system-created or modified when you assign a parent tenant to a tenant. The tenant becomes a subtenant of the parent and higher tenants (if any) in that hierarchy.

The service provider can create multiple unrelated hierarchies, or none. Even in a system with tenant hierarchies, you can define standalone tenants.

CA APM supports a tenant hierarchy of unlimited depth. However, the service provider can specify a limit on the total number of tenants and the depth of tenant hierarchies (default is four levels). The service provider also determines whether individual tenants can have subtenants.

Note: Although not required, the service provider can participate in tenant hierarchies. The service provider cannot have a parent tenant.

Define a Subtenant

Subtenancy allows you to define and modify tenant hierarchies for organizational and data-sharing purposes. To place a tenant into a tenant hierarchy, you specify a parent tenant for the tenant.

To define a subtenant

1. Click Administration, Tenancy Management.
   The Multi-Tenancy Administration page appears.

2. On the left, click Tenant.
   The Tenants page appears.

3. Click Create Tenant.
   The Create New Tenant page appears.

4. Enter the subtenant information. The following fields require explanation:

- **Parent Tenant**
  Specifies another tenant above this tenant, making this tenant a *subtenant* in a tenant hierarchy.

The Parent Tenant drop-down only displays tenants that are allowed to have subtenants.

5. Click Save.
   The tenant is a subtenant of the parent tenant.
   Note: When a tenant becomes a subtenant, the tenant belongs to the subtenant group of the parent tenant, in addition to its other subtenants (if any), and so on. The parent tenant joins the supertenant group of its new subtenant, in addition to its other supertenants (if any), and so on. Each joins the related tenants group of the other.

Update a Subtenant

When necessary, you can update the information for an existing subtenant.

To update a subtenant

1. Click Administration, Tenancy Management.
   The Multi-Tenancy Administration page appears.
2. On the left, click Tenant.
   The Tenants page appears.
3. Search to find the tenant that you want to update.
   All tenants matching the search criteria appear in the Tenant List.
4. Click the tenant in the list. The subtenant name appears in the Name column of the Tenant List.
   The tenant information appears.
5. Click Edit.
6. Enter the new information for the subtenant.
7. Click Save.
   The subtenant is updated.

Product-Maintained Tenant Groups

The product generates and maintains the following tenant groups automatically for each tenant in a tenant hierarchy (*tenant* is the tenant name):

- *tenant*_subtenants (tenant, its *child* tenants, and their lower subtenants)
- *tenant*_supertenants (tenant, parent tenant and its higher supertenants)

- *tenant*_relatedtenants (entire single hierarchy)

System-maintained groups can be used like user-defined tenant groups. However, only the name and description can be modified.

How to Secure CA APM Data with Filters

You can set up CA APM data security by creating data filters. You use the data filters to limit the data that users and user roles can view, create, or modify. Users can view, create, or modify only the data that the filter specifies. You can create filters for any of the primary objects:

- Asset
- Model
- Legal Document
- Contact
- Company
- Location
- Organization
- Site

You cannot create a filter for a secondary object that is included in List Management. For example, you can filter assets (primary object) based on the cost center (secondary object) so that you only see assets that belong to a specific cost center. However, all cost centers are still accessible. To restrict access to cost centers (or other secondary objects), assign the user to a configuration that does not allow access to these objects.

As a system administrator, you define filters that limit data access in the following ways:

- Limit data based on the current user (contact).
  For example, define a filter that limits assets by the cost center of the contact. If you apply the filter to all users, the assets dynamically filter based on each user cost center. If the contact cost center is changed, the product filters the assets for the new cost center automatically.

- Limit data based on fixed values.
  For example, allow a user to view assets in the Development cost center. Development is a fixed value. If the cost center changes, the cost center is not automatically changed in the filter.

The data that matches the filter criteria is accessible to filter users.

Note: You can also set up CA APM security by configuring the user interface. Through this configuration, you can control user access to the different functions in CA APM.

In this scenario, the system administrator defines the filters. However, the administrator can grant filter management permissions to any CA APM user role.

To filter CA APM data, perform these steps:

1. Review the Prerequisites (see page 1617).
2. Define and Apply a Filter (see page 1617).
3. Verify the Filter (see page 1620).

Example: Filter Asset Data by Cost Center

Sam, the CA APM system administrator at Document Management Company, wants to ensure that organizational data security requirements are met. Sam wants to limit user access to the company asset records so that users see only their own cost center data. Sam creates a filter for Asset (All Families) and assigns the filter to particular users. Sam verifies that the filter works to ensure the organizational data security.

Review the Prerequisites

To ensure that you can successfully filter data, verify that you have completed the following prerequisites:

1. Identify the product data that you want to limit by user or role.
2. Identify the users and roles that have limited data access.

Define and Apply a Filter

Define a filter and assign the filter to a role, a user, or a combination of roles and users. The product displays only the data that the user is authorized to access.

Follow these steps:

1. Click Administration, Filter Management.
2. On the left, click New Filter.
3. In the Filter Information area, enter the required and optional (if needed) information. The following fields require explanation:

   - **Object**
     Specifies the object data that you want to filter. The object that you select determines the fields that you can use as criteria in the Filter Criteria area.

If you select Model or Asset, select a family, also. If you select Legal Document, select a template, also. The filter is applied to objects that belong to the family or template that you select. For example, a filter for the hardware asset object does not apply to any other asset family.

You cannot change the object or the object family or template after you specify filter criteria or after you save the filter. Delete the filter criteria to change the object.

- **Family or Legal Template**
  Specifies the family for the Model or Asset object or specifies the template for the Legal Document object.

4. In the Filter Security area, enter information for role or user security.

   If you save your filter without selecting a user or role in the Filter Security area, your filter is not applied to any users.

5. In the Filter Criteria area, click Add Fields.

6. Select a field from the dialog and click OK.
   The criterion is shown in the Filter Criteria list.

7. Click the Edit Record icon next to the criterion you added.

8. Enter information to define the filter criterion for a selected field. The following fields require explanation:

   - **Left Parenthesis**
     Specifies the first criterion in a group of criteria. You can define groups of criteria to control the logic of the filter.

     If you select Left Parenthesis to define the first criterion in a group, select Right Parenthesis for the last criterion in the group.

     For example, you can filter for assets with the asset name OE001 or with both the asset family Computer and the asset name Dell. In this example, the group consists of two criteria. The Left Parenthesis is selected for the first criterion, which states that the asset family is Computer. The Right Parenthesis is selected for the second criterion, which states that the asset name is Dell.

   - **Field Name**
     Specifies the field data that is filtered.

- **Operator**
  Specifies the filter operator to use to filter object data. For all operators except Has Value and Has No Value, enter a value in the Value field.
  For example, you can filter assets in which the asset name is not equal to OE001 and the asset family is equal to Computer.

  If you specify an Operator and Value, the filter limits data based on a fixed value for the Field Name. In this type of filter, the Use Contact's Value field is not applicable.

- **Use Contact's Value**
  Specifies that the filter uses the Field Name value that is associated with the current user. For example, if you select this check box and you select cost center for Field Name, the users can access product data for their cost centers only. If you apply the filter to all users in the product, the data dynamically filters based on each user cost center. If the cost center changes, the product filters the data for the new cost center automatically.

  If you select this check box, the filter limits data based on the Field Name value that is associated with the current user. In this type of filter, the Operator and Value fields are not applicable.

- **Right Parenthesis**
  Specifies the last criterion in a group of criteria. You can define groups of criteria to control the logic of the filter.

  If you select Right Parenthesis to define the last criterion in a group, select Left Parenthesis for the first criterion in the group.

  For example, you can filter for assets with the asset name OE001 or with both the asset family Computer and the asset name Dell. In this example, the group consists of two criteria. The Left Parenthesis is selected for the first criterion, which states that the asset family is Computer. The Right Parenthesis is selected for the second criterion, which states that the asset name is Dell.

- **Connector**
  Specifies the connector between a set of two criteria:

  - And - Filters the data if the current criterion and the next criterion in the list are valid.
  - Or - Filters the data if either the current criterion or the next criterion in the list is valid.

  For example, you can filter for assets with an asset family of Computer and an asset name of Dell.

- **Value**
  Specifies the field value that you want to filter. If you specify a value, select an Operator in the Operator field. If a Search icon appears next to this field, you can also select a value by clicking the Search icon.
  For example, you can filter an asset with an asset name of OE001.

  If you specify an Operator and Value, the filter limits data based on a fixed value for the Field Name. In this type of filter, the Use Contact's Value field is not applicable.

9. Click the Complete Record Edit icon.
10. (Optional) Click Add Fields to define more filter criteria.
11. Click Save after you have completed all filter criteria.
    The filter is defined and applied to users and roles. The data that matches the filter criteria is accessible to filter users.

Example: Filter Asset Data by User Cost Center

As the system administrator, Sam defines a filter that restricts users to the asset data for their own cost centers. To define this filter, Sam makes the following selections:

1. In the Filter Information area, Sam selects Asset in the Object field and (All Families) in the Family field.
2. In the Filter Security area, Sam selects the users who are associated with the filter.
3. In the Filter Criteria area, Sam creates a criterion by performing these steps:
   a. Sam selects Cost Center in the Field Name field.
   b. Sam selects the Use Contact's Value check box.
4. Sam saves the filter.

Verify the Filter

Verify that your filter works to ensure the security of your organizational data.

Follow these steps:

1. Log in to the product as a user who was assigned to the filter.
2. View some of the data that the filter allows for the user.

3. Attempt to view some of the data that the filter does not allow for the user.
   For example, log in as another user who has access to data that is not allowed for the filter user. Copy the URL for a page that displays some data that the filter user cannot access. Paste the URL in the browser of the filter user.
   An error message appears.

4. Attempt to modify some of the data that the filter does not allow for the user.
   For example, identify a text entry field on a page. Enter data that the user cannot access (such as a specific company name that the filter does not allow) and click Save.
   An error message appears.

Example: Verify that the Data Filter Limits Asset Data

Sam created a filter for Asset (All Families) data and assigned the filter to a particular user. With the filter, the user can access only the assets that are in the user cost center. Sam then performs these steps to verify that the filter works:

1. Logs in as the assigned user and validates that assets are available on the Asset Search page.

2. Logs in as a second user with access to assets that are outside of the first user cost center.

3. Views an asset that is outside of the first user cost center and copies the URL of the asset.

4. Logs in as the first user (who was assigned the filter) and pastes the copied asset URL in the browser.
   An error message states that the asset does not exist.

How to Delete Unused Files from CA APM

The files that you use while working with the product are stored on the CA APM application server where the Storage Manager Service is installed. These files include attachment files and Data Importer source data files and legacy map files.

When you delete an attachment, you delete only the reference to the attachment in the object record. If the deleted attachment is a file, the file remains in the file system on the CA APM application server. In similar fashion, when you delete an import that uses a specific data file, you do not delete the data file from the CA APM server.

If a specific attachment file, import data file, or legacy map file is no longer needed, you can delete the file from the CA APM server. Before you delete the file, verify that the file does not have any associations.

To delete unused files, perform these steps:

1. Review the Prerequisites (see page 1622).

2. Query the CA MDB (see page 1622).

3. Locate and Delete the Unused Files (see page 1622).

Review the Prerequisites

To ensure that you can successfully delete the unused files, identify the names of the unused files that you want to delete.

Query the CA MDB

If a specific attachment file, import data file, or legacy map file is no longer needed, you can delete the file from the CA APM application server. Before you delete the file, verify that the file does not have any associations in CA APM (for example, a file attached to a legal document or an import data file associated with a data import).

Follow these steps:

1. Access the CA MDB that is associated with your CA APM installation.

2. Query the al_file_storage table to search for the file name and the associated tenant if applicable. The following statement is an example query:

   ```
   select COUNT(0) from al_file_storage where attachment_url = 'filename.txt'
   ```

   If no records are returned, no records are associated with the specified file name. You can delete the file.

Locate and Delete the Unused Files

After you verify that the files do not have any associations in CA APM, you can locate and delete the files.

Follow these steps:

1. On the CA APM application server where the Storage Manager Service is installed, navigate to one of the following locations, depending on whether you are using multi-tenancy:

   ```
   [ITAM Root Path]/Storage/Common Store/Attachments
   [ITAM Root Path]/Storage/Tenant_Name/Attachments
   [ITAM Root Path]/Storage/Common Store/Import
   [ITAM Root Path]/Storage/Tenant_Name/Import
   ```

2. Locate and delete the unused files.

Import Data

This section contains the following articles:

How to Delete Data with the Data Importer

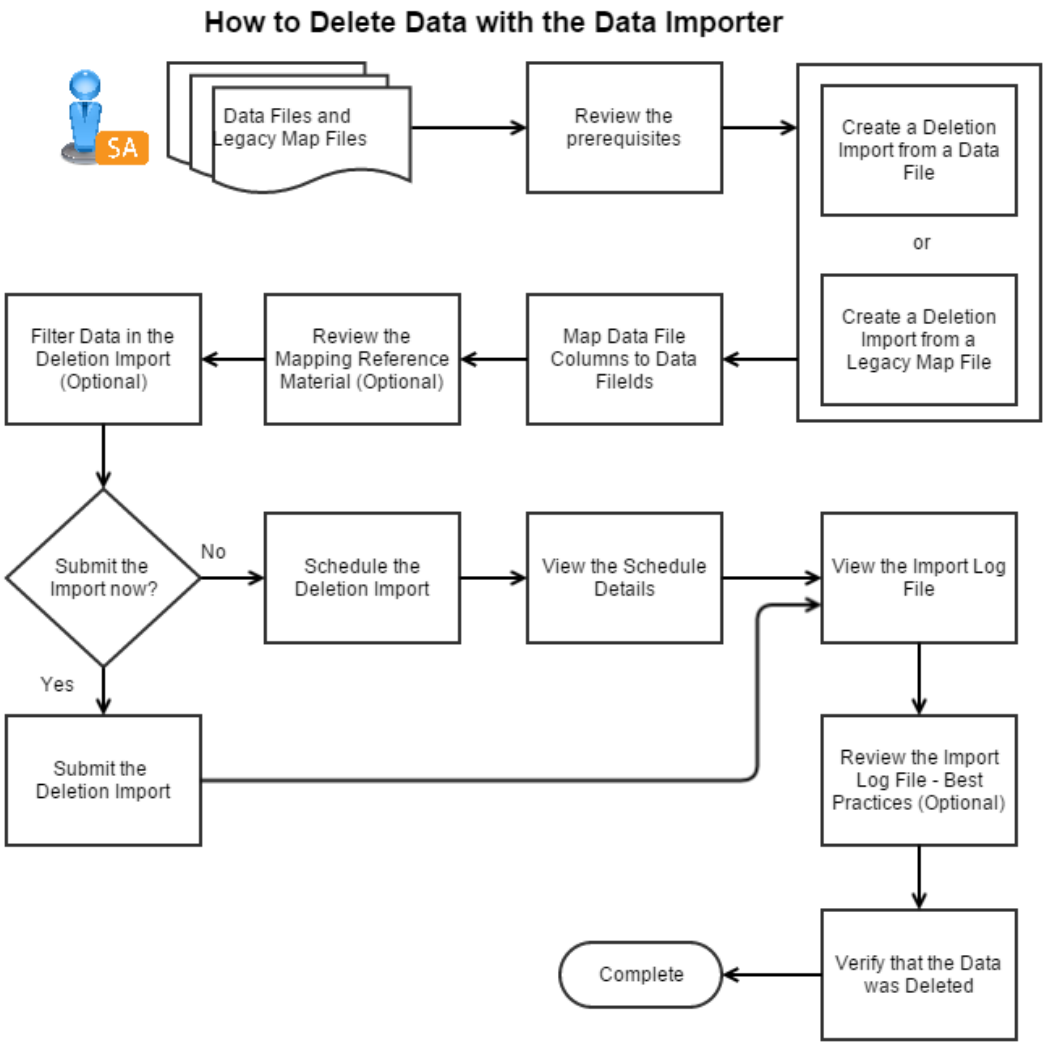
When data is no longer valid for your implementation, delete the data from CA APM using the Data Importer. In most situations, however, it is considered good IT asset management practice to keep the data in the repository with a status of inactive. This method allows you to access the data for historical and audit purposes. However, in some cases, the data was created by mistake. In these cases, you want to delete the data.

In this scenario, the system administrator performs the data deletion. However, the administrator can grant Data Importer User Access or Data Importer Admin Access to any CA APM user role. User access allows users to create imports, modify or delete their own imports, and view any import that was created by another user. Admin access allows users to create imports and modify or delete any import that was created by any user.

You can delete primary objects and can remove the relationships to their secondary objects. For example, you delete an asset (primary object) and you remove its relationship to a legal document (secondary object).

When you delete a primary object and its relationship to a secondary object, the secondary object is not deleted. The primary object is deleted, and the relationship between the primary and secondary object is removed. For example, if you delete an asset and its associated legal document relationship, the asset is deleted but the legal document is not deleted. Only the relationship between the asset and the legal document is removed.

The following diagram illustrates how a system administrator deletes data.



To delete CA APM data, perform these steps:

1. Review the Prerequisites. (see page 1625)
2. Create a Deletion Import from a Data File (see page 1626) or Create a Deletion Import from a Legacy Map File (see page 1629).
3. Map Data File Columns to Data Fields. (see page 1631)
4. Review the Mapping Reference Material. (see page 1650)
   - Primary and Secondary Lookup Combinations (see page 1650)
   - Hard-Coded Values (see page 1652)
   - Multiple Values for a Single Field (see page 1653)
5. Filter Data in the Deletion Import (see page 1635).

6. Submit the Deletion Import (see page 1636) or Schedule the Deletion Import (see page 1637).
7. View the Schedule Details (see page 1656).
8. View the Import Log File. (see page 1657)
9. Review the Import Log File - Best Practices (see page 1657).
10. Verify that the Data was Deleted (see page 1640).

Example: Delete Laptops

Miriam, the CA APM system administrator at Document Management Company, wants to delete several laptops that have been retired and recycled. Miriam also wants to delete the associations with legal documents that were made for these laptops. Miriam has a data file that identifies the laptop names, the manufacturers, and the model names. Using the Data Importer and the source data file, Miriam creates a deletion import. After Miriam runs the import, she views the import statistics, import log file, and user interface to verify the deletions.

Review the Prerequisites

To ensure that you can successfully delete the data, verify that you have completed the following tasks:

- Prepare a source data file in delimited text format (for example, tab or comma) containing the data that you want to delete.
  We recommend that you include the main destination object in the name of the source data file. This file naming convention helps you locate your data files when you create your import.

  A value of NULL in your source data file clears the corresponding destination field value. An empty field in your source data file leaves the corresponding destination field value unchanged.

  If a data value in your source data file contains the selected delimiter, you must use double quotation marks around the data value. For example, you select a comma as the delimiter to import companies. You want to include the data value Document Management Company, Inc. in your source data file. Specify this data value with double quotation marks: "Document Management Company, Inc".

- (Optional) Copy your source data files from your local server to one of the following locations. You can access these locations on the CA APM application server where the Storage Manager Service is installed. The location depends on whether you are using multi-tenancy.

  ```
  [ITAM Root Path]\Storage\Common Store\Import

  [ITAM Root Path]\Storage\Tenant_Name\Import
  ```

If you copy the data file before you create an import, you can then specify the file name when you create the import. If you do not copy the data file first, you can upload the file from your local server when you create the import.

- (Optional) Copy your legacy map files from a previous product release (if you have these files) from your local server to one of the following locations. You can access these locations on the CA APM application server where the Storage Manager Service is installed. The location depends on whether you are using multi-tenancy.

```
[ITAM Root Path]\Storage\Common Store\Import

[ITAM Root Path]\Storage\Tenant_Name\Import
```

Create a Deletion Import from a Data File

You can delete data using a source data file (delimited text file) that contains the data that you want to delete. You select the file, configure the import parameters, and specify the delimiter (for example, a comma) that separates the data in the file.

You can also create a deletion import using a legacy map file from a previous product release. For more information, see creating a deletion import from a legacy map file (see page 1629).

Follow these steps:

1. Log in to CA APM as the administrator.

   In this scenario, the system administrator performs the deletion import. However, the administrator can grant Data Importer User Access or Data Importer Admin Access to any CA APM user role. User access allows users to create imports, modify or delete their own imports, and view any import that was created by another user. Admin access allows users to create imports and modify or delete any import that was created by any user.

2. Click Administration, Data Importer.

3. Click New Import.

4. Enter the required information in the Basic Information area and supply optional information as needed. The following fields require explanation:

   - **Data File**
     Specifies the source data file.
     If this file is available on the CA APM application server, search for the data file and select the file. If this file is not available on the application server, upload the file.

   - **Upload File**
     Browse on your local server for a source data file or a legacy map file that you want to use to create mappings. This file is uploaded to the CA APM application server.

Note: The file size is limited by the product environmental settings. For more information, contact your administrator.

- **Main Destination Object**
  Specifies the main object for the deletion import.
  Asset and Model objects are listed with their corresponding families. You can also specify All Families. Legal Document objects are listed according to legal template. You can also specify All Templates. The objects include all objects that can be imported or deleted.

  For assets or models that include multiple asset family types or legal documents that include multiple legal templates, use the following selections for this field. Specify the particular family or template for each record in your source data file.

  - For an asset, select Asset (All Families).
  - For a model, select Model (All Families).
  - For a legal document, select Legal Document (All Templates).

  Ensure that you select the correct main destination object. You cannot change the main destination object after you save or copy an import.

- **First Row Has Column Names**
  Specifies whether the first row in the source data file contains the column names. If the first row does not contain the column names, the names display as generic names, such as Field 1 and Field 2.

- **Tenant**
  Specifies the tenant that applies to the import (if you are using multi-tenancy).
  You can select a tenant only when multi-tenancy is enabled in CA APM and you are authorized to access different tenants. If you have access to public data and you have multiple tenants, you can select all tenants.
  If you specify all tenants, your source data file must have a tenant name column that you map to the Tenant Name field.

  If you specify one tenant, verify that all data in your source data file belongs to your selected tenant. If you have data for more than one tenant, data for all tenants is applied to the selected tenant.

- **Data Delimiter**
  Specifies the delimiter (for example, comma or tab) that you used in the source data file.

If a data value in your source data file contains the selected delimiter, you must use double quotation marks around the data value. For example, you select a comma as the delimiter to import companies. You want to include the data value Document Management Company, Inc. in your source data file. Specify this data value with double quotation marks: "Document Management Company, Inc".

- **Data File Locale**
  Specifies the locale for the source data file. This setting determines the date and time format.

5. Enter the required information in the Advanced Settings area and supply optional information as needed.
   The following fields require explanation:

   - **Maximum Error Threshold (in %)**
     Defines the number of errors after which the import stops. The threshold is based on the percentage of records processed. We recommend a minimum threshold of 15 percent.

     The Data Importer processes the number of records that are specified on Administration, System Configuration, Data Importer (Maximum Batch Record Size field) before calculating if the error threshold has been reached.

   - **Primary Lookup Object Processing Type**
     Specifies the type of import activity. Select one of the following options:

     - **Delete Primary Objects and Associated Relationships**
       Select this option to delete primary objects and the relationships to their associated secondary objects. For example, you delete a company (primary object) and you remove the relationship to an associated asset allocation (secondary object).
       When you select this option, verify that your mapping rules specify the primary objects only. Do not include any mapping rules for secondary objects.
       Note: The secondary object that is associated with a primary object is not deleted. The relationship between the primary object and the secondary object is removed. For example, you have a primary object Company1 with an associated acquired company Company2 (secondary object). When you delete Company1, the relationship to Company2 is removed. The secondary object Company2 is not deleted.

     - **Delete Relationships Only**
       Select this option to remove the relationships between secondary objects and their primary objects. When you select this option, verify that your mapping rules specify the primary and secondary objects only. You include a mapping rule for a secondary object; however, do not select the Primary Lookup check box for this rule.
       Note: A secondary object that is associated with a primary object is not deleted. The relationship between the primary and secondary object is removed.

   - **Normalization Behavior**
     Specifies whether to normalize the data or write an error message in the log file without normalizing the data.

This field appears only if you have defined normalization rules.

- **Error on Normalization**
  Writes an error message to the Data Importer log file when data that can be normalized is found in the data that you are deleting. The data involved is not deleted. The log file error message includes the details about the data.
  For example, your data includes the company name Microsoft. The company normalization rules that you created identify Microsoft as a collected (nonauthoritative) value and specify Microsoft Corporation as the normalized (authoritative) value. If you select this option when deleting your data, the object with the company name Microsoft is not deleted and an error message is written to the log file.

- **Apply Normalization without Error**
  Uses the normalization rules to normalize the data that you are deleting. If data that can be normalized is found, the data is normalized and deleted. No error message about the data is written to the log file.
  For example, your data includes the company name Microsoft. The company normalization rules you created identify Microsoft as a collected (nonauthoritative) value and specify Microsoft Corporation as the normalized (authoritative) value. If you select this option when deleting your data, the object with company name Microsoft is normalized. In this example, the company name is changed to Microsoft Corporation and the associated object is deleted.

6. Click Save.
   The deletion import is saved. The Mapping, Exclusion Filter, and Schedule areas of the page are now available for your input.

Example: Create a Deletion Import from a Data File

Miriam, the CA APM system administrator, performs the following actions to create the deletion import:

1. Navigates to Administration, Data Importer and clicks New Import.

2. Enters Hardware Deletions.csv in the Data File field.
   This CSV file is the source data file that contains the laptop deletions.

3. Selects Asset (Hardware) for the Main Destination Object and comma for the Data Delimiter.

4. Selects Delete Primary Objects and Associated Relationships in the Primary Lookup Object Processing Type field and clicks Save.

Create a Deletion Import from a Legacy Map File

You can create a deletion import using a legacy map file from a previous CA APM release. The map file defines the corresponding data file and the import parameter settings.

Note: We recommend that you copy your legacy map files and corresponding data files to the CA APM application server before you create the deletion imports. However, if necessary, you can use the optional steps to upload a legacy map file.

You can also create a deletion import using a data file only. For more information, see creating a deletion import from a data file (see page 1626).

Follow these steps:

1. Click Administration, Data Importer, New Import.
2. Click Search and Load Map to select a legacy map file that is already available on the CA APM application server.

   The corresponding data file must also be available on the CA APM application server.

   If the legacy map file is not available on the CA APM application server, upload the file using the Upload File field.
3. (Optional) Upload a legacy map file that is not available on the CA APM application server using the following steps:

   a. In the Upload File field, browse on your local server and select a legacy map file.
   The legacy map file is uploaded and is displayed in the Upload File field.

   b. Click Search and Load Map and select the legacy map file that you uploaded.
   The legacy map file is displayed in the Legacy Map File field.
   The Basic Information is loaded.

   Note: If you receive a warning about the source data file, upload the data file using the Upload File field.
4. Specify the Advanced Settings and click Save.
   The Exclusion Filter and Mapping data mapping are loaded. The Mapping, Exclusion Filter, and Schedule areas of the page are now available for your input. The Mapping and Exclusion Filter areas display the data from the legacy map file.

   Note: For information about specifying the Advanced Settings, see creating a deletion import from a data file (see page 1626).

Map Data File Columns to Data Fields

You can map the columns in your source data file to product fields. You perform column mapping to specify which data is deleted. You can select most objects and associated fields as destination fields during column mapping.

> If you created your deletion import from a legacy map file, the column mapping exists. You can edit the existing mapping rules if you want to change the values. You can also add new mapping rules.

When you log in, the user role that your administrator assigned to you determines the objects and fields that you can see and use. If your role specifies that you do not have permissions for an object field, the field is not available for a mapping. You can only create a mapping and import or delete data for the objects and fields for which you have permissions.

Follow these steps:

1. On the Administration tab, Data Importer page, in the Mapping area for a selected deletion import, click New or click Load Source Fields.
   - New allows you to select the source fields individually from the source data file.
   - Load Source Fields adds all source fields from the source data file.

   > If you have existing mappings, Load Source Fields allows you to replace those mappings with the source fields in the source data file. This option also allows you to add the source fields from the source data file that you do not already have in your mappings.

   a. If you clicked Load Source Fields, click the Edit Record icon next to a field.

2. Click the Select icon next to Source Field (if this field is empty), select a column from your data source, and click OK.
   If this field already contains a source field (because you loaded all source fields), you can skip this step.

3. Click the Select icon next to Destination Field, select a Destination Field for the selected Source Field, and click OK.
   The destination fields that appear are based on your selected main destination object.

   >

> The destination fields display in hierarchical order. For example, the fields that are listed under Asset Type Hierarchy are Asset Family, Class, and Subclass. The order of the fields represents the field hierarchy. Follow the field hierarchy when you specify mapping rules. For example, for Asset Type Hierarchy, specify a rule for Class before you specify Subclass.

4. Select the Primary Lookup and Secondary Lookup check boxes as required.

    a. Select a Primary Lookup check box for each destination field that you want to use to find the primary object. Use the following guidelines when selecting this check box:

    - Select at least one Primary Lookup check box in the column mapping for an import.
    - Do not select this check box if the Destination Field is Note Text (under the Note object). The database data type for the Note Text field does not allow it to function as a lookup field.

    b. Select a Secondary Lookup check box for each destination field that you want to use to find the secondary object. Use the following guidelines when selecting this check box:

    - Do not select this check box if the destination field is not one of your lookup fields for the secondary object.
    - Do not select this check box if the Destination Field is Note Text (under the Note object). The database data type for the Note Text field does not allow it to function as a lookup field.

5. Click the Complete Record Edit icon.

6. (Optional) Click New again, or click the Edit Record icon next to another source field, to specify more mapping rules.

> ⚠ To delete a specific mapping rule from the list of mapped columns, click the Delete icon next to the mapping rule. The column mapping rule is removed from the list.

7. Click Save.
   Your column mapping is saved.

Example: Map Data File Columns to Data Fields

Miriam performs the following steps to map the columns in the source data file to the CA APM data fields:

1. Clicks New in the Mapping area of the Import Details page.

2. Selects %Hardware Name% in the Source Field by clicking the Select icon next to Source Field and selecting this item from the dialog.
   The items that are listed in the dialog are the columns from the source data file.

3. Selects Asset Name in the Destination Field by clicking the Select icon next to Destination Field and selecting this object from the dialog.

4. Selects the Primary Lookup check box.

5. Clicks the Complete Record Edit icon and clicks Save.

Review the Mapping Reference Material

Reference the following information when setting up the column mapping for importing or deleting data.

Primary and Secondary Lookup Combinations

The fields that you select as the primary and secondary lookup in your column mapping are used to search for data in the product database.

- **Simple mapping**
  In simple mapping, you specify only the primary lookup. For example, you are importing or deleting a set of company records from a text file into the product database. You specify the Company Name as the primary lookup. If a company with a particular name does not exist in the database when you are importing data, a record is created for the company. The following table shows an example of the lookup for a simple mapping.

Source Field	Destination Field	Primary Lookup	Secondary Lookup
%Company Name%	Company.Company Name	Yes	No

- **Reference field mapping**
  In reference field mapping, you specify primary and secondary lookup values. To search for a unique object, specify more than one primary lookup. For example, to search for a company, you can specify Company Name, Parent Company, and Company Type as primary lookup values. In this example, the Data Importer searches for a company with the specified name, the specified parent company, and of the specified company type. If the object does not exist and you are importing data, the record is created (depending on the insert or update option you selected in Advanced Settings). The following table shows an example of the lookup for reference field mapping.

Source Field	Destination Field	Primary Lookup	Secondary Lookup
%Company Name%	Company.Company Name	Yes	No
%Parent Company%	Company.Parent Company.Company Name	Yes	Yes
%Company Type%	Company.Company Type.Value	Yes	Yes

This mapping has both the Primary Lookup and the Secondary Lookup check boxes selected for Parent Company and Company Type. The Data Importer uses the Company Name to look up the parent company and uses the Parent Company to look up the company name.

- **Secondary object mapping**
  If a mapping rule maps to a secondary object property, the primary lookup values establish a relationship between a secondary object and the reference fields. The following table shows examples of the lookup for a secondary object mapping.

Source Field	Destination Field	Primary Lookup	Secondary Lookup
%Comment%	Legal Document.Legal Party.Comment	No	Yes
%Legal Document ID%	Legal Document.Document Identifier	Yes	No
%Company Name%	Legal Document.Legal Party.Legal Party. Company Name	Yes	Yes
%Legal Template%	Legal Document.Legal Template.Template	Yes	Yes

In the first mapping rule, Legal Document is the primary object, and Legal Party is the secondary object. Comment is a property of Legal Party.

In the third mapping rule, Legal Document is the primary object, and Legal Party is the secondary object. In addition, Legal Party has a reference field in the Company table. The Secondary Lookup check box indicates that the Company Name is used to look up the Company object. The Primary Lookup check box indicates that the Company object is used to look up the Legal Party object.

Hard-Coded Values

In the column mapping, the percent signs that appear before and after column names identify the names as column headers in your source data file. You can also specify a hard-coded value in the Source Field that you want to apply to all records in your source data file. You can then map the hard-coded value to a Destination Field. The hard-coded values do not display with percent signs to distinguish these values from the source data file column names.

1. Source data file column header
2. Hard-coded value

You can define a hard-coded value in the Source Field to expand your source data and to ensure that you include all required fields. Hard-coded values typically do not begin and end with a percent sign (%). If you have hard-coded values with percent signs, the values cannot match the field names in your source data file.

Example: Use hard-coded values for asset family

In this example, the assets in your source data file do not contain asset family, which is required when creating an asset. You can add a hard-coded value to your mapping. If all of your assets are hardware, you can enter Hardware in the Source Field. You can map this value to the Asset Family field. If your assets belong to different families, add a column to your source data file with the corresponding asset families before importing or deleting data.

The following information illustrates the difference between values from your source data file and values that are added through hard-coded values:

- You have an Asset Family column in your source data file. The selection in the Source Field is %asset family%.
- You do not have an Asset Family column in your source data file. However, all of your assets are hardware assets. You specify a hard-coded value of Hardware in the Source Field.

You can also use the Main Destination Object to specify that all records in your source data file belong to a particular family or template. For example, the Asset (Hardware) selection for Main Destination Object specifies that all source records belong to the hardware asset family.

Multiple Values for a Single Field

You can add a mapping with multiple Source Field values that are mapped to a single Destination Field.

Example: Use multiple values for a single field

Your source data file has two columns with the names Manufacturer and Catalog Name. Combine these columns by selecting both in the Source Field. In this example, the Source Field selection is %Manufacturer% %Catalog Name%.

You can also enter multiple hard-coded values in the Source Field (for example, Document Management Company %model name% IT Department).

Filter Data in the Deletion Import

You can identify a subset of records in your source data file that you want to exclude from the deletion import. The Data Importer exclusion filter allows you to filter a part of your data source using exclusion filter rules.

Example: Define an exclusion filter to process returned assets

A CSV file that you receive from your hardware vendor includes assets that were ordered and returned to the vendor. You want to delete the assets that were returned to the vendor, so you want to process those records only. You define an exclusion filter to exclude records that do not have a status of Returned.

Follow these steps:

1. On the Administration tab, Data Importer page, Exclusion Filter area for a selected deletion import, select the Filter Type.

- **And**
  Excludes a record from the source data file only if all the rules that you specify are valid for the record.

- **Or**
  Excludes a record from the source data file if any of the rules that you specify is valid for the record.

2. Click New.

3. Click the Select icon next to Source Field, select a column from your source data file, and click OK.

   The percent signs before and after the column name identify the name as a column from your source data file.

4. Select the Operator.

   To specify "not equal to", select the "<>" operator.

5. Enter a Filter Value for the rule.

   You can use special characters and wildcards in the filter value. The rules can process text, numeric, and date fields.

6. Click the Complete Record Edit icon.

7. (Optional) Click New and specify more exclusion filter rules.

8. Click Save.
   The exclusion filter rules are saved and are applied when the deletion import processes.

Submit the Deletion Import

To start a deletion import immediately, click Submit in the Schedule area of the page. The data source records from the data file for the selected deletion import are processed.

You can specify a data file other than the default (from the Basic Information) if you want to use a different file.

You can also schedule the deletion import for a particular day and time. For more information, see schedule the deletion import (see page 1637).

To view the import jobs for your current selected deletion import, click Associated Jobs on the left side of the page. To view all import jobs for all imports, click Import Jobs. In the list of import jobs that appears, click Status Message to view the status of an import.

You can also view the log file for more information about the import activity. In the list of import jobs, click View Logs for the selected import.

Schedule the Deletion Import

You can schedule a deletion import for a specific time and you can specify the interval for the deletion import (for example, daily or weekly). You can schedule multiple deletion imports to process simultaneously.

Follow these steps:

1. On the Administration tab, Data Importer page, in the Schedule area for a selected deletion import, select the Is Scheduled check box.

2. Provide the information for the schedule. The following fields require explanation:

   - **Run Time**
     Specifies the time of the day, in 24-hour format, to process the deletion import. When you schedule imports, use the local time zone on the CA APM application server.

   - **Interval Day**
     Specifies the day during the Interval Type to process the deletion import. For example, if the Interval Type is Month and the Interval Day is 1, the import is processed on the first day of the month.

   - **Data File**
     Specifies a data file name other than the default (from the Basic Information) if you want to use a different file.
     If this file is available on the application server, you can search and select the file. If this file is not available on the application server, you can locate and upload the file.

   - **Upload Data File**
     Browse for the source data file. This file is uploaded to the application server.

   - **First Run Date**
     Specifies the date when the first deletion import starts to process.

   - **Interval Type**
     Specifies the type of interval for the deletion import (for example, Day, Month, Quarter, Week, or Year).

   - **Interval**
     Specifies how often the deletion import processes. This interval is based on the specified Interval Type. For example, if the Interval Type is Weekly and the Interval is 2, the import processes every two weeks.

- **Last Day of Interval**
  Specifies that the deletion import processes on the last day of the selected Interval Type. If you select this check box, any previous value that you added to the Interval Day field is removed, and the Interval Day field is disabled.

3. Click Submit.
   The deletion import is scheduled for the specified date and time.

Examples: Using the Schedule Settings

The following examples illustrate the use of the schedule settings.

- Select Day for Interval Type and 2 for Interval. The import processes every other day.
- Select Week for Interval Type, 1 for Interval Day, and 3 for Interval. The import processes every three weeks on the first day (Sunday) of the week.
- Select Month for Interval Type, 15 for Interval Day, and 2 for Interval. The import processes every two months on the 15th day of the month.
- Select Quarter for Interval Type and select Last Day of Interval. The import processes every quarter (every three months) on the last day of the last month in the quarter.
- Select Year for Interval Type, 1 for Interval Day, and 1 for Interval. The import processes on January 1 of every year.

To view the import jobs for your current selected deletion import, click Associated Jobs on the left side of the page. To view all import jobs for all imports, click Import Jobs. In the list of import jobs that appears, click Status Message to view the status of an import.

You can also view the log file for more information about the import activity. In the list of import jobs, click View Logs for the selected import.

View the Schedule Details

You can view the schedule details for a scheduled import job that you created.

First, open the list of import jobs.

- To view the scheduled import jobs for your currently selected import, click Associated Jobs on the left side of the page, select the Scheduled check box, and click Go.
- To view all import jobs for all imports, click Import Jobs on the left side of the page, select the Scheduled check box, and click Go.

In the list of import jobs that appears, click Schedule Details for a selected import.

View the Import Log Files

You can view the Data Importer log files to see the details of all CA-provided and user-defined imports that have completed. The Data Importer creates a log file for each import that you run, including imports that were submitted immediately or scheduled for a future time. All import activities are saved in the log files.

To view the log files, first open the list of import jobs.

- To view the import jobs for your current selected import, click Associated Jobs on the left side of the page.
- To view all import jobs for all imports, click Import Jobs.

In the list of import jobs, click View Logs for a selected import. If more than one log file is available (for example, for a scheduled import that has completed a few times already), all files are listed with their corresponding creation dates.

You can view any available LDAP Import Sync log file. If you click Start LDAP Data Import and Sync on the LDAP Data Import and Sync page (Administration, User/Role Management), an import job ID is displayed. Use this job ID to locate the job in the Data Importer list of import jobs. Then click View Logs for that job.

You can also locate and view the import log files in the following location on the CA APM application server:

```
[ITAM Root Path]\Storage\Common Store\Import\Logs
```

Review the Import Log File - Best Practices

The Data Importer log file contains information and error messages regarding the processing of import jobs. To help you understand the results of your import and to troubleshoot any errors, use the information in this log file. This section contains some recommended best practices for working with the Data Importer log file.

Match the row number in the data file with the error message in the log file.

A log file error message identifies the corresponding row number from your data file. You can also find the data file row number in the row above or below the error message in the log file.

Sometimes the error message in the log file does not show the data file row number. In this situation, the actual data file values are shown immediately after the error message in the log file.

Count the number of error messages in your log file.

1. Search for the following phrases in your log file to find the error messages in the file. These phrases are included with the error messages.

   ```
   Web Service threw exception
   Error at record
   ```

2. After you find a type of error message, search for that error in the log file and count the number of occurrences.

3. Identify and search for more error types that appear in your log file and count the number of occurrences.

4. Compare the count of all errors in your log file with the statistics that the Data Importer generated for the associated import. To view these statistics, click Status Message on the Associated Jobs list or Import Jobs list. This comparison helps you account for all relevant errors and identify error messages that are not valid and can be ignored.

Verify that the Data was Deleted

You verify that your deletion import succeeded by viewing your data in CA APM and by reviewing the Data Importer statistics.

- **Review the Data Importer Statistics.** To review the statistics for your current selected deletion import, click Associated Jobs on the left side of the page. In the list of import jobs that appears, click Status Message for your import.
  You can also view the log file for more information about the import activity. In the list of import jobs, click View Logs for the selected import.

- **View the Data in CA APM.** To view the data in CA APM, navigate to the tab and subtab, if necessary, for the object that you deleted (for example, asset, company, or contact). Search for the objects that you deleted and verify that the objects are not available.

Example: Verify the Deletion of Laptops

After Miriam runs the deletion import, she performs the following steps to verify that the laptops were deleted:

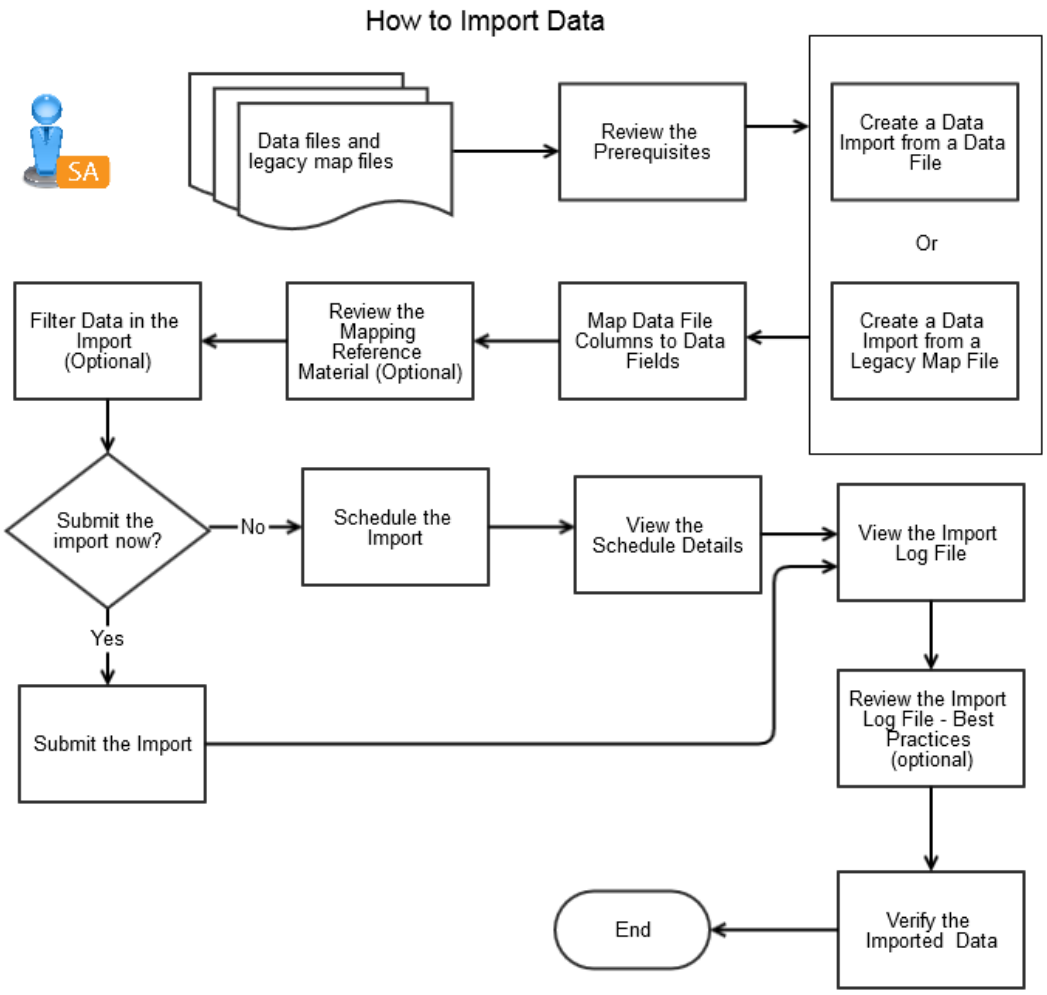
1. Checks the import statistics.
   - Clicks Associated Jobs or Import Jobs on the left side of the Data Importer page.
   - Clicks Status Message for the deletion import and reviews the statistics.
2. Views the import log file and the user interface.
   - Clicks View Logs in the list of import jobs and reviews the contents of the log file.
   - Navigates to the Asset tab. Searches for the deleted laptops and verifies that the deleted laptops are not available.

How to Import Data

When you want to add or update data, import it into CA APM using the Data Importer. The data that you import is inserted, or updates existing data, in the CA MDB.

In this scenario, the system administrator performs the data import. However, the administrator can grant Data Importer User Access or Data Importer Admin Access to any CA APM user role. User access allows users to create imports, modify or delete their own imports, and view any import that was created by another user. Admin access allows users to create imports and modify or delete any import that was created by any user.

The following diagram illustrates how a system administrator imports data.



To import CA APM data, perform these steps:

1. Review the Prerequisites (see page 1642).
2. Create a Data Import from a Data File (see page 1643) or Create a Data Import from a Legacy Map File (see page 1647).
3. Map Data File Columns to Data Fields (see page 1648).
4. Review the Mapping Reference Material (see page 1650).
   - Primary and Secondary Lookup Combinations (see page 1650)
   - Hard-Coded Values (see page 1652)
   - Multiple Values for a Single Field (see page 1653)
5. Filter Data in the Import (see page 1653).

6. Submit the Import (see page 1655).
7. Schedule the Import (see page 1655).
8. View the Schedule Details (see page 1656).
9. View the Import Log File (see page 1657).
10. Review the Import Log File Best Practices (see page 1657).
11. Verify the Imported Data (see page 1658).

Example: Import New Employees

Sam, the CA APM system administrator at Document Management Company, wants to import a group of new employees. The new employees use the product to manage hardware assets. Sam received a comma-separated value (CSV) source data file from Human Resources that contains the employee information. All of the new asset manager employees belong to the IT department and work at the company headquarters. However, the source data file also contains data about some new employees who work at other locations and do not belong to the IT department.

Sam only wants to import the data for the IT employees at headquarters. Using the Data Importer and the source data file, Sam creates a data import to incorporate the new employees into the CA MDB. To ensure that only employees in the IT department at headquarters are imported, Sam creates an exclusion filter. After Sam runs the import, he checks the import statistics and the import log file and user interface to verify that the import was successful.

Review the Prerequisites

To ensure that you can successfully import the data, verify that you have completed the following tasks:

- Prepare a source data file in delimited text format (for example, tab or comma). This file contains the data that you want to import.

We recommend that you include the main destination object in the name of the source data file. This file naming convention helps you locate your data files when you create your import.**Note:** A value of NULL in your source data file clears the corresponding destination field value. An empty field in your source data file leaves the corresponding destination field value unchanged.

If a data value in your source data file contains the selected delimiter, you must use double quotation marks around the data value. For example, you select a comma as the delimiter to import companies. You want to include the data value Document Management Company, Inc. in your source data file. Specify this data value with double quotation marks: "Document Management Company, Inc".

- (Optional) Copy your source data files from your local server to one of the following locations. You can access these locations on the CA APM application server where the Storage Manager Service is installed. The location depends on whether you are using multi-tenancy.

```
[ITAM Root Path]\Storage\Common Store\Import

[ITAM Root Path]\Storage\Tenant_Name\Import
```

If you copy the data file before you create an import, you can then specify the file name when you create the import. If you do not copy the data file first, you can upload the file from your local server when you create the import.

- (Optional) Copy your legacy map files from a previous product release (if you have these files) from your local server to one of the following locations. You can access these locations on the CA APM application server where the Storage Manager Service is installed. The location depends on whether you are using multi-tenancy.

```
[ITAM Root Path]\Storage\Common Store\Import

[ITAM Root Path]\Storage\Tenant_Name\Import
```

Create a Data Import from a Data File

You create a data import using a source data file (delimited text file) that contains the data that you want to import. You select the file, configure the import parameters, and specify the delimiter (for example, a comma or a tab) that separates the data in the file.

You can also create a data import using a legacy map file from a previous product release. For more information, see creating a data import from a legacy map file (see page 1647).

Follow these steps:

1. Log in to CA APM as the administrator.

In this scenario, the system administrator performs the data import. However, the administrator can grant Data Importer User Access or Data Importer Admin Access to any CA APM user role. User access allows users to create imports, modify or delete their own imports, and view any import that was created by another user. Admin access allows users to create imports and modify or delete any import that was created by any user.

2. Click Administration, Data Importer.

3. Click New Import.

4. Enter the required information in the Basic Information area and supply optional information as needed. The following fields require explanation:

- **Data File**
  Specifies the source data file that you want to import.
  If this file is available on the CA APM application server, search for the data file and select the file. If this file is not available on the application server, upload the file.

- **Upload File**
  Browse on your local server for a source data file that you want to import or a legacy map file that you want to use to create mappings. This file is uploaded to the CA APM application server.

  The file size is limited by the product environmental settings. For more information, contact your administrator.

- **Main Destination Object**
  Specifies the main object for the import.
  Asset and Model objects are listed with their corresponding families. You can also specify All Families. Legal Document objects are listed according to legal template. You can also specify All Templates. The objects include all objects that can be imported.

  For assets or models that include multiple asset family types or legal documents that include multiple legal templates, use the following selections for this field. Specify the particular family or template for each record in your source data file.

  - For an asset, select Asset (All Families).
  - For a model, select Model (All Families).
  - For a legal document, select Legal Document (All Templates).

  Important! Ensure that you select the correct main destination object for your import. You cannot change the main destination object after you save or copy an import.

- **First Row Has Column Names**
  Specifies whether the first row in the source data file contains the column names. If the first row does not contain the column names, the names display as generic names, such as Field 1 and Field 2.

- **Tenant**
  Specifies the tenant that applies to the import (if you are using multi-tenancy).
  You can select a tenant only when multi-tenancy is enabled in CA APM and you are authorized to access different tenants. If you have access to public data and you have multiple tenants, you can select all tenants.

If you specify all tenants, your source data file must have a tenant name column that you map to the Tenant Name field.

If you specify one tenant, verify that all data in your source data file belongs to your selected tenant. If you have data for more than one tenant, data for all tenants is imported into the selected tenant.

- **Data Delimiter**
  Specifies the delimiter (for example, comma or tab) that you used in the source data file.

  If a data value in your source data file contains the selected delimiter, you must use double quotation marks around the data value. For example, you select a comma as the delimiter to import companies. You want to include the data value Document Management Company, Inc. in your source data file. Specify this data value with double quotation marks:

  "Document Management Company, Inc"

- **Data File Locale**
  Specifies the locale for the source data file. This setting determines the date and time format.

5. Enter the required information in the Advanced Settings area and supply optional information as needed. The following fields require explanation:

   - **Maximum Error Threshold (in %)**
     Defines the number of errors after which the import stops. The threshold is based on the percentage of records processed. We recommend a minimum threshold of 15 percent.

     The Data Importer processes the number of records that are specified on Administration, System Configuration, Data Importer (Maximum Batch Record Size field) before calculating if the error threshold has been reached.

   - **Primary Lookup Object Processing Type**
     Specifies the type of import activity (for example, insert or update).

   - **Create Secondary Lookup Object**
     Creates new secondary lookup objects during the import process. If this option is not selected and a secondary object does not exist, an error occurs.

   - **Update Secondary Lookup Object**
     Updates the existing secondary lookup objects during the import process. If a secondary object does not exist, an error occurs.

- **Error on Secondary Lookup Object Errors**
  Indicates that the Data Importer does not process a primary object insert or update if the secondary object process fails. If a secondary object insert or update process fails and this check box is selected, the insert or update for the primary object also fails. If this check box is not selected, the primary object is created or updated (as long as the object is not dependent on the secondary object). However, the secondary object value is not created or changed. In both situations, the secondary object error is logged in the import log file.
  Example: You import a location and the location has a country. If the import fails while trying to update the country object and this check box is selected, the location record is not created. If this check box is not selected, the location record is created, and the country information is not updated.

- **Normalization Behavior**
  Specifies whether to normalize the data or write an error message in the log file without normalizing the data.

  
  This field appears only if you have defined normalization rules.

  - **Error on Normalization**
    Writes an error message to the Data Importer log file when data that can be normalized is found in the data that you are importing. The data involved is not imported. The log file error message includes the details about the data.
    For example, your data includes the company name Microsoft. The company normalization rules that you created identify Microsoft as a collected (nonauthoritative) value and specify Microsoft Corporation as the normalized (authoritative) value. If you select this option when importing your data, the object with the company name Microsoft is not imported and an error message is written to the log file.

  - **Apply Normalization without Error**
    Uses the normalization rules to normalize the data that you are importing. If data that can be normalized is found, the data is normalized and imported. No error message about the data is written to the log file.
    For example, your data includes the company name Microsoft. The company normalization rules you created identify Microsoft as a collected (nonauthoritative) value and specify Microsoft Corporation as the normalized (authoritative) value. If you select this option when importing your data, the object with company name Microsoft is normalized. In this example, the company name is changed to Microsoft Corporation and the associated object is imported.

6. Click Save.
   The import is saved. The Mapping, Exclusion Filter, and Schedule areas of the page are now available for your input.

Example: Create a Data Import of New Employees from a Data File

Sam, the CA APM system administrator, performs the following actions to create the data import:

1. Navigates to Administration, Data Importer and clicks New Import.

2. Enters New Employees.csv in the Data File field.
   This CSV file is the source data file that Sam received from Human Resources with the new employee information.

3. Selects Contact for the Main Destination Object and comma for Data Delimiter.

4. Selects Insert or Update in the Primary Lookup Object Processing Type field and clicks Save.

Create a Data Import from a Legacy Map File

You can create a data import using a legacy map file from a previous CA APM release. The map file defines the corresponding data file and the import parameter settings.

We recommend that you copy your legacy map files and corresponding data files to the CA APM application server before you create the data imports. However, if necessary, you can use the optional steps to upload a legacy map file.

You can also create a data import using a data file only. For more information, see creating a data import from a data file (see page 1643).

Follow these steps:

1. Click Administration, Data Importer, New Import.

2. Click Search and Load Map to select a legacy map file that is already available on the CA APM application server.

   The corresponding data file must also be available on the CA APM application server.

   If the legacy map file is not available on the CA APM application server, upload the file using the Upload File field.

3. (Optional) Upload a legacy map file that is not available on the CA APM application server using the following steps:

   a. In the Upload File field, browse on your local server and select a legacy map file.
      The legacy map file is uploaded and is displayed in the Upload File field.

   b. Click Search and Load Map and select the legacy map file that you uploaded.
      The legacy map file is displayed in the Legacy Map File field.
      The Basic Information is loaded.

If you receive a warning about the source data file, upload the data file using the Upload File field.

4. Specify the Advanced Settings and click Save.
   The Exclusion Filter and Mapping data mapping are loaded. The Mapping, Exclusion Filter, and Schedule areas of the page are now available for your input. The Mapping and Exclusion Filter areas display the data from the legacy map file.

   For information about specifying the Advanced Settings, see creating a data import from a data file (see page 1643).

Map Data File Columns to Data Fields

You can map the columns in your source data file to fields in CA APM. You perform column mapping to specify where the source data is imported. You can select most objects and associated fields as destination fields during column mapping.

If you created your data import from a legacy map file, the column mapping exists. If you want to change the values, you can edit the existing mapping rules. You can also add or remove mapping rules and filters.

When you log in, the user role that your administrator assigned to you determines the objects and fields that you can see and use. If your role specifies that you do not have permissions for an object field, the field is not available for a mapping. You can only create a mapping and import data for the objects and fields for which you have permissions.

Note: We recommend that, before you map data, you review the CA APM user interface to determine the required information for a mapping. For example, review the Asset page to see that the asset name, asset family, model, and class are required. Because a model is required to create an asset, you review the Model page to see that the model name and asset family are required. By reviewing the user interface before you create a mapping, you ensure that you have all required information to create a mapping.

Follow these steps:

1. On the Administration tab, Data Importer page, in the Mapping area for a selected import, click New or click Load Source Fields.

   - New allows you to select the source fields individually from the source data file.

- Load Source Fields adds all source fields from the source data file.

> If you have existing mappings, Load Source Fields allows you to replace those mappings with the source fields in the source data file. This option also allows you to add the source fields from the source data file that you do not already have in your mappings.

a. If you clicked Load Source Fields, click the Edit Record icon next to a field.

2. Click the Select icon next to Source Field (if this field is empty), select a column from your data source, and click OK.
   If this field already contains a source field (because you loaded all source fields), you can skip this step.

> The percent signs that appear before and after the column names identify the names as column headers in your source data file. You can also specify a hard-coded value in the Source Field that you want to apply to all records in your source data file. You can then map the hard-coded value to a Destination Field. The hard-coded values do not display with percent signs so that they can be distinguished from the source data file column names. For more information, see hard-coded values (see page 1652).

3. Click the Select icon next to Destination Field, select a Destination Field for the selected Source Field, and click OK.
   The destination fields that appear are based on your selected main destination object.

> The destination fields display in hierarchical order. For example, the fields that are listed under Asset Type Hierarchy are Asset Family, Class, and Subclass. The order of the fields in the list represents the field hierarchy. Follow the field hierarchy when you specify mapping rules. For example, for Asset Type Hierarchy, specify a rule for Class before you specify Subclass.

4. Select the Primary Lookup and Secondary Lookup check boxes as required.

   a. Select a Primary Lookup check box for each destination field that you want to use to find the primary object. Use the following guidelines when selecting this check box:

      - Select at least one Primary Lookup check box in the column mapping for an import.
      - Do not select this check box if the Destination Field is Note Text (under the Note object). The database data type for the Note Text field does not allow it to function as a lookup field.

b. Select a Secondary Lookup check box for each destination field that you want to use to find the secondary objects. Use the following guidelines when selecting this check box:

   - Do not select this check box if the destination field is not one of your lookup fields for the secondary object.
   - Do not select this check box if the Destination Field is Note Text (under the Note object). The database data type for the Note Text field does not allow it to function as a lookup field.

5. Click the Complete Record Edit icon.
6. Click New again, or click the Edit Record icon next to another source field, to specify more mapping rules.

   To delete a specific mapping rule from the list of mapped columns, click the Deletion icon next to the mapping rule. The column mapping rule is removed from the list.

7. Click Save.
   Your column mapping is saved.

Example: Map Data File Columns to Data Fields

Sam performs the following steps to map the data file columns in the source data file to the CA APM data fields:

1. Clicks New in the Mapping area of the Import Details page.
2. Selects %Login ID% in the Source Field by clicking the Select icon next to Source Field and selecting this item from the dialog.
   The items that are listed in the dialog are the columns from the source data file.
3. Selects User ID in the Destination Field by clicking the Select icon next to Destination Field and selecting this object from the dialog.
4. Selects the Primary Lookup check box.
5. Continues to map the remaining columns in the source data file with CA APM data fields and clicks Save when finished.

Review the Mapping Reference Material

Reference the following information when setting up the column mapping for importing or deleting data.

Primary and Secondary Lookup Combinations

The fields that you select as the primary and secondary lookup in your column mapping are used to search for data in the product database.

- **Simple mapping**
  In simple mapping, you specify only the primary lookup. For example, you are importing or deleting a set of company records from a text file into the product database. You specify the Company Name as the primary lookup. If a company with a particular name does not exist in the database when you are importing data, a record is created for the company. The following table shows an example of the lookup for a simple mapping.

Source Field	Destination Field	Primary Lookup	Secondary Lookup
%Company Name%	Company.Company Name	Yes	No

- **Reference field mapping**
  In reference field mapping, you specify primary and secondary lookup values. To search for a unique object, specify more than one primary lookup. For example, to search for a company, you can specify Company Name, Parent Company, and Company Type as primary lookup values. In this example, the Data Importer searches for a company with the specified name, the specified parent company, and of the specified company type. If the object does not exist and you are importing data, the record is created (depending on the insert or update option you selected in Advanced Settings). The following table shows an example of the lookup for reference field mapping.

Source Field	Destination Field	Primary Lookup	Secondary Lookup
%Company Name%	Company.Company Name	Yes	No
%Parent Company%	Company.Parent Company.Company Name	Yes	Yes
%Company Type%	Company.Company Type.Value	Yes	Yes

This mapping has both the Primary Lookup and the Secondary Lookup check boxes selected for Parent Company and Company Type. The Data Importer uses the Company Name to look up the parent company and uses the Parent Company to look up the company name.

- **Secondary object mapping**
  If a mapping rule maps to a secondary object property, the primary lookup values establish a relationship between a secondary object and the reference fields. The following table shows examples of the lookup for a secondary object mapping.

Source Field	Destination Field	Primary Lookup	Secondary Lookup
%Comment%	Legal Document.Legal Party.Comment	No	Yes
%Legal Document ID%	Legal Document.Document Identifier	Yes	No
%Company Name%	Legal Document.Legal Party.Legal Party. Company Name	Yes	Yes
%Legal Template%	Legal Document.Legal Template.Template	Yes	Yes

In the first mapping rule, Legal Document is the primary object, and Legal Party is the secondary object. Comment is a property of Legal Party.

In the third mapping rule, Legal Document is the primary object, and Legal Party is the secondary object. In addition, Legal Party has a reference field in the Company table. The Secondary Lookup check box indicates that the Company Name is used to look up the Company object. The Primary Lookup check box indicates that the Company object is used to look up the Legal Party object.

Hard-Coded Values

In the column mapping, the percent signs that appear before and after column names identify the names as column headers in your source data file. You can also specify a hard-coded value in the Source Field that you want to apply to all records in your source data file. You can then map the hard-coded value to a Destination Field. The hard-coded values do not display with percent signs to distinguish these values from the source data file column names.

1. Source data file column header
2. Hard-coded value

You can define a hard-coded value in the Source Field to expand your source data and to ensure that you include all required fields. Hard-coded values typically do not begin and end with a percent sign (%). If you have hard-coded values with percent signs, the values cannot match the field names in your source data file.

Example: Use hard-coded values for asset family

In this example, the assets in your source data file do not contain asset family, which is required when creating an asset. You can add a hard-coded value to your mapping. If all of your assets are hardware, you can enter Hardware in the Source Field. You can map this value to the Asset Family field. If your assets belong to different families, add a column to your source data file with the corresponding asset families before importing or deleting data.

The following information illustrates the difference between values from your source data file and values that are added through hard-coded values:

- You have an Asset Family column in your source data file. The selection in the Source Field is % asset family%.

You do not have an Asset Family column in your source data file. However, all of your assets are hardware assets. You specify a hard-coded value of Hardware in the Source Field.

You can also use the Main Destination Object to specify that all records in your source data file belong to a particular family or template. For example, the Asset (Hardware) selection for Main Destination Object specifies that all source records belong to the hardware asset family.

Multiple Values for a Single Field

You can add a mapping with multiple Source Field values that are mapped to a single Destination Field.

Example: Use multiple values for a single field

Your source data file has two columns with the names Manufacturer and Catalog Name. Combine these columns by selecting both in the Source Field. In this example, the Source Field selection is %Manufacturer% %Catalog Name%.

You can also enter multiple hard-coded values in the Source Field (for example, Document Management Company %model name% IT Department).

Filter Data in the Import

You can identify a subset of records in your source data file that you want to exclude from the import. The Data Importer exclusion filter allows you to filter a part of your data source using exclusion filter rules.

Example: Define an exclusion filter to process returned assets

A CSV file that you receive from your hardware vendor includes assets that were ordered and returned to the vendor. You want to process only the returned assets, so you want to import data to update those records only. You define an exclusion filter to exclude records that do not have a status of Returned.

Follow these steps:

1. On the Administration tab, Data Importer page, Exclusion Filter area for a selected import, select the Filter Type.
   - **And**
     Excludes a record from the source data file only if all the rules that you specify are valid for the record.
   - **Or**
     Excludes a record from the source data file if any of the rules that you specify is valid for the record.
2. Click New.
3. Click the Select icon next to Source Field, select a column from your source data file, and click OK.

The percent signs before and after the column names identify the names as columns from your source data file.

4. Select the Operator.

   To specify "not equal to", select the "<>" operator.

5. Enter a Filter Value for the rule.

   You can use special characters and wildcards in the filter value. The rules can process text, numeric, and date fields.

6. Click the Complete Record Edit icon.
7. (Optional) Click New and specify more exclusion filter rules.
8. Click Save.
   The exclusion filter rules are saved and are applied when the import processes.

Example: Create an Exclusion Filter

Sam performs the following steps to create an exclusion filter. The filter eliminates non-IT employees and employees who do not work at the company headquarters from the data import.

1. Selects And for the Filter Type and clicks New in the Exclusion Filter area of the Import Details page.
2. Selects %Department% for the Source Field.
3. Selects <> for the Operator.
4. Enters IT for the Filter Value.
5. Clicks the Complete Record Edit icon and clicks New.
6. Selects %Location% for the Source Field.
7. Selects <> for the Operator.
8. Enters Headquarters for the Filter Value.
9. Clicks the Complete Record Edit icon and clicks Save.

Submit the Import

To start an import immediately, click Submit in the Schedule area of the page. The data source records from the data file for the selected import are processed.

You can specify a data file other than the default (from the Basic Information) if you want to use a different file.

You can also schedule the import for a particular day and time. For more information, see schedule the import (see page 1655).

To view the import jobs for your current selected import, click Associated Jobs on the left side of the page. To view all import jobs for all imports, click Import Jobs on the left side of the page. In the list of import jobs that appears, click Status Message to view the status of an import.

You can also view the log file for more information about the import activity. In the list of import jobs, click View Logs for the selected import.

Schedule the Import

You can schedule an import for a specific time and you can specify the interval for the import (for example, daily or weekly). You can schedule multiple imports to process simultaneously.

Follow these steps:

1. On the Administration tab, Data Importer page, in the Schedule area for a selected import, select the Is Scheduled check box.

2. Provide the information for the schedule. The following fields require explanation:

   - **Run Time**
     Specifies the time of the day, in 24-hour format, to process the import. When you schedule imports, use the local time zone on the CA APM application server.

   - **Interval Day**
     Specifies the day during the Interval Type to process the import. For example, if the Interval Type is Month and the Interval Day is 1, the import is processed on the first day of the month.

   - **Data File**
     Specifies a data file name other than the default (from the Basic Information) if you want to use a different file.
     If this file is available on the application server, you can search and select the file. If this file is not available on the application server, you can locate and upload the file.

   - **Upload Data File**
     Browse for the source data file that you want to import. This file is uploaded to the application server.

- **First Run Date**
  Specifies the date when the first import starts to process.

- **Interval Type**
  Specifies the type of interval for the import (for example, Day, Month, Quarter, Week, or Year).

- **Interval**
  Specifies how often the import processes. This interval is based on the specified Interval Type. For example, if the Interval Type is Weekly and the Interval is 2, the import processes every two weeks.

- **Last Day of Interval**
  Specifies that the import processes on the last day of the selected Interval Type. If you select this check box, any previous value that you added to the Interval Day field is removed, and the Interval Day field is disabled.

3. Click Submit.
   The data import is scheduled for the specified date and time.

Examples: Using the Schedule Settings

The following examples illustrate the use of the schedule settings.

- Select Day for Interval Type and 2 for Interval. The import processes every other day.
- Select Week for Interval Type, 1 for Interval Day, and 3 for Interval. The import processes every three weeks on the first day of the week (Sunday).
- Select Month for Interval Type, 15 for Interval Day, and 2 for Interval. The import processes every two months on the 15th day of the month.
- Select Quarter for Interval Type and select Last Day of Interval. The import processes every quarter (every three months) on the last day of the last month in the quarter.
- Select Year for Interval Type, 1 for Interval Day, and 1 for Interval. The import processes on January 1 of every year.

To view the import jobs for your current selected import, click Associated Jobs on the left side of the page. To view all import jobs for all imports, click Import Jobs on the left side of the page. In the list of import jobs that appears, click Status Message to view the status of an import.

You can also view the log file for more information about the import activity. In the list of import jobs, click View Logs for the selected import.

View the Schedule Details

You can view the schedule details for a scheduled import job that you created.

First, open the list of import jobs.

- To view the scheduled import jobs for your currently selected import, click Associated Jobs on the left side of the page, select the Scheduled check box, and click Go.

- To view all import jobs for all imports, click Import Jobs on the left side of the page, select the Scheduled check box, and click Go.

In the list of import jobs that appears, click Schedule Details for a selected import.

View the Import Log Files

You can view the Data Importer log files to see the details of all CA-provided and user-defined imports that have completed. The Data Importer creates a log file for each import that you run, including imports that were submitted immediately or scheduled for a future time. All import activities are saved in the log files.

To view the log files, first open the list of import jobs.

- To view the import jobs for your current selected import, click Associated Jobs on the left side of the page.
- To view all import jobs for all imports, click Import Jobs.

In the list of import jobs, click View Logs for a selected import. If more than one log file is available (for example, for a scheduled import that has completed a few times already), all files are listed with their corresponding creation dates.

You can view any available LDAP Import Sync log file. If you click Start LDAP Data Import and Sync on the LDAP Data Import and Sync page (Administration, User/Role Management), an import job ID is displayed. Use this job ID to locate the job in the Data Importer list of import jobs. Then click View Logs for that job.

You can also locate and view the import log files in the following location on the CA APM application server:

```
[ITAM Root Path]\Storage\Common Store\Import\Logs
```

Review the Import Log File - Best Practices

The Data Importer log file contains information and error messages regarding the processing of import jobs. To help you understand the results of your import and to troubleshoot any errors, use the information in this log file. This section contains some recommended best practices for working with the Data Importer log file.

Match the row number in the data file with the error message in the log file.

A log file error message identifies the corresponding row number from your data file. You can also find the data file row number in the row above or below the error message in the log file.

Sometimes the error message in the log file does not show the data file row number. In this situation, the actual data file values are shown immediately after the error message in the log file.

Count the number of error messages in your log file.

1. Search for the following phrases in your log file to find the error messages in the file. These phrases are included with the error messages.

   ```
   Web Service threw exception
   Error at record
   ```

2. After you find a type of error message, search for that error in the log file and count the number of occurrences.

3. Identify and search for more error types that appear in your log file and count the number of occurrences.

4. Compare the count of all errors in your log file with the statistics that the Data Importer generated for the associated import. To view these statistics, click Status Message on the Associated Jobs list or Import Jobs list. This comparison helps you account for all relevant errors and identify error messages that are not valid and can be ignored.

Verify the Imported Data

You verify that your data import succeeded by viewing your data in CA APM and by reviewing the Data Importer statistics.

- **Review the Data Importer Statistics.** To review the statistics for your current selected import, click Associated Jobs on the left side of the page. In the list of import jobs that appears, click Status Message for your import.
  You can also view the log file for more information about the import activity. In the list of import jobs, click View Logs for the selected import.

- **View the Imported Data in CA APM.** To view the imported data, navigate to the tab and subtab, if necessary, for the object that you imported (for example, asset, company, or contact). Search for the objects that you imported and verify that the objects are available.

Example: Verify the Data Import of New Employees

After Sam runs the import, he performs the following steps to verify the data import of new employees:

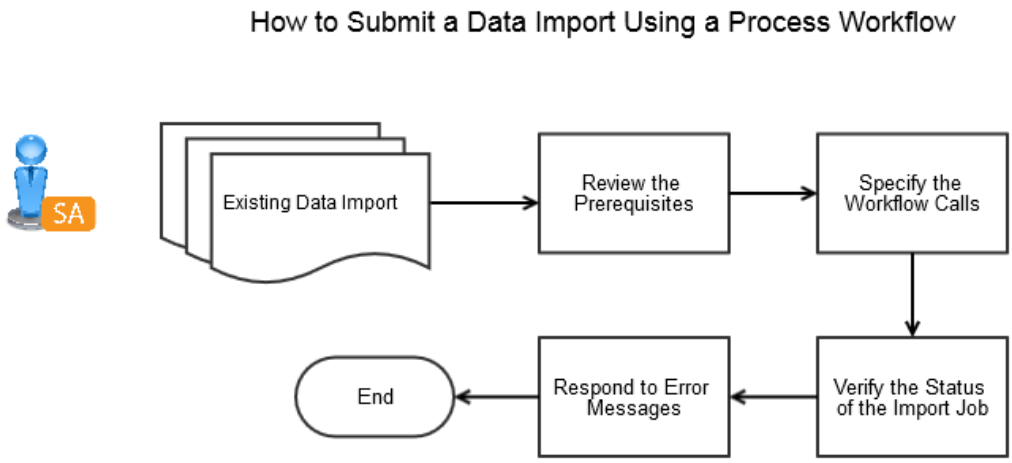
1. Checks the import statistics.
   - Clicks Associated Jobs or Import Jobs on the left side of the Data Importer page.
   - Clicks Status Message for the import and reviews the statistics.
2. Views the import log file and the user interface.
   - Clicks View Logs in the list of import jobs and reviews the contents of the log file.
   - Navigates to Directory, Contact on the CA APM user interface. Searches for the new employees. Verifies that the non-IT employees and employees who do not work at company headquarters are not available.

How to Submit a Data Import Using a Process Workflow

You can use a process workflow (for example, CA Process Automation) to submit a Data Importer data import for processing instead of using the CA APM user interface.

You can create a data import process workflow using a company-provided sample XML file and integrating with CA Process Automation. For more information about this integration, see Implementing CA IT Asset Manager (see page 301).

The following diagram illustrates how a system administrator submits a data import using a process workflow:



To submit a data import using a process workflow, perform these steps:

1. Review the Prerequisites (see page 1660).
2. Specify the Workflow Calls (see page 1660).
3. Verify the Status of the Import Job (see page 1662).
4. (Optional) Respond to Error Messages (see page 1662).

Example: Import New Hardware Devices through a Process Workflow

Sam, the CA APM system administrator at Document Management Company, has defined a business process workflow. The workflow discovers new hardware devices, adds the new devices to the company data repository, and runs reports about the new devices. Sam has already created a data import in CA APM that adds the new hardware devices to the data repository. Sam wants to execute that data import at a specific point in his overall workflow. He wants to integrate the data import with his overall business process workflow. Sam wants the data import to execute at the time that the workflow specifies without the user logging in to the product user interface. Sam updates his business process workflow to include calls to the CA APM web service operations for the Data Importer.

Review the Prerequisites

To ensure that you can successfully submit a data import using a process workflow, verify that you have completed the following prerequisites:

1. Define a data import with all mappings and settings through the CA APM user interface.
2. Verify that the data file path (if you are specifying a path) is accessible from the server where the Import Service is running. Also, the Network Service (application pool identity) user requires access to this path.
3. Define a process workflow using a workflow provider (such as CA Process Automation).

Specify the Workflow Calls

To launch the Data Importer and execute a data import from a process workflow, you provide specific workflow calls to CA APM web service operations. These operations perform the following functions:

- Login operation - Logging in to CA APM.
- Submitting a data import using one of the following ways of providing a data file:
  - SubmitImportwithfilepath Operation - The data file is available on a specified file path. This file path must be accessible from the server where the Import Service is running. The web service operation uploads the file.
  - SubmitImport Operation - The data file content has been converted to byte array binary format. The web service operation receives the byte array content from an application and submits the content to the Data Importer.

    To use this way of providing a data file, create an application, if one is not already available, to convert the data file content to byte array format. The application then sends the content to the web service operation.

Incorporate the calls to these operations into your business process workflow.

For information about creating a process workflow, see the product documentation for your workflow provider.

Login Operation

This operation logs in to CA APM using the specified CA APM user ID and password. The output of this operation is the login token. The login token is used as input to other data import workflow operations.

- **Input Parameters**
  ItamUserName - CA APM user ID
  ItamUserPassword - CA APM user password

- **Output Parameters**
  loginToken - Token that is returned after the CA APM login.

SubmitImport Operation

This operation receives data file content that has been converted to byte array format and submits the content with the data import to the Data Importer. To use this operation, create an application, if one is not already available, to convert the data file content to byte array format. The application then sends the content to this web service operation.

This operation returns a data import job ID, which is used to verify the status of the import job.

- **Input Parameters**
  loginToken - Token that is returned after the CA APM login.
  ImportName - Name of the data import.
  Datafilename - Name of the data file that is associated with the data import.
  Datafilestream - Data file content in byte array format.
  Caprovided - (Optional) Indicator that specifies a product-provided data import. Set this parameter to one (1) to specify a product-provided import.
  Tenant - (Multi-tenancy only) Name of the tenant to which the import applies.

- **Output Parameters**
  Job ID - ID that is returned after a data import is submitted successfully. The GetJobStatus operation uses this ID to verify the status of an import job.

SubmitImportwithfilepath Operation

This operation uploads a data file from a specified file path and submits the data file with the data import to the Data Importer. This file path must be accessible from the server where the Import Service is running.

The operation returns a data import job ID, which is used to verify the status of the import job.

- **Input Parameters**
  loginToken - Token that is returned after the CA APM login.
  ImportName - Name of the data import.
  Datafilepath - Complete path and name of the data file that is associated with the data import. This path must be accessible from the server where the Import Service is running. Also, the Network Service (application pool identity) user requires access to this path.

  If the data file location is a shared path, the CA APM server and the shared computer must be in the same domain.Caprovided - (Optional) Indicator that specifies a product-provided data import. Set this parameter to one (1) to specify a product-provided import.

  Tenant - (Multi-tenancy only) Name of the tenant to which the import applies.

- **Output Parameters**
  Job ID - ID that is returned after a data import is submitted successfully. The GetJobStatus operation uses this ID to verify the status of an import job.

Verify the Status of the Import Job

The Data Importer provides a status summary of each submitted data import job. Your process workflow can include a call to the CA APM web service operation that retrieves the status of a submitted data import job. Incorporate the call to this operation into your process workflow.

GetJobStatus Operation

This operation uses the data import job ID to verify the status of an import job.

- **Input Parameters**
  loginToken - Token that is returned after the CA APM login.
  Job ID - ID that is returned after a data import is submitted successfully.

- **Output Parameters**
  Job Status - Status of the import job.

Respond to Error Messages

If errors occur during the data import workflow process, you can receive error messages. The following messages require explanation:

- **20002 - Cannot access the data import because of user permissions. Contact your administrator.**
  The user role requires Data Importer Admin access or Data Importer User access to submit a data import.

- **20005 - Cannot connect to the Import service. Contact your administrator.**
  Verify the Import Service URL in the ImportProcessor.config file, or contact your administrator.

- **21002 - The data import name is invalid.**
  The data import does not exist, or the user does not have access to the data import. If the data import is product-provided, specify a value of 1 for the Caprovided parameter.

- **21004 - The data file failed to upload.**
  This message can result from a configuration error. Review the Storage Manager Service log files.

- **21005 - No mappings are defined for the data import.**
  Define mappings and resubmit the data import.

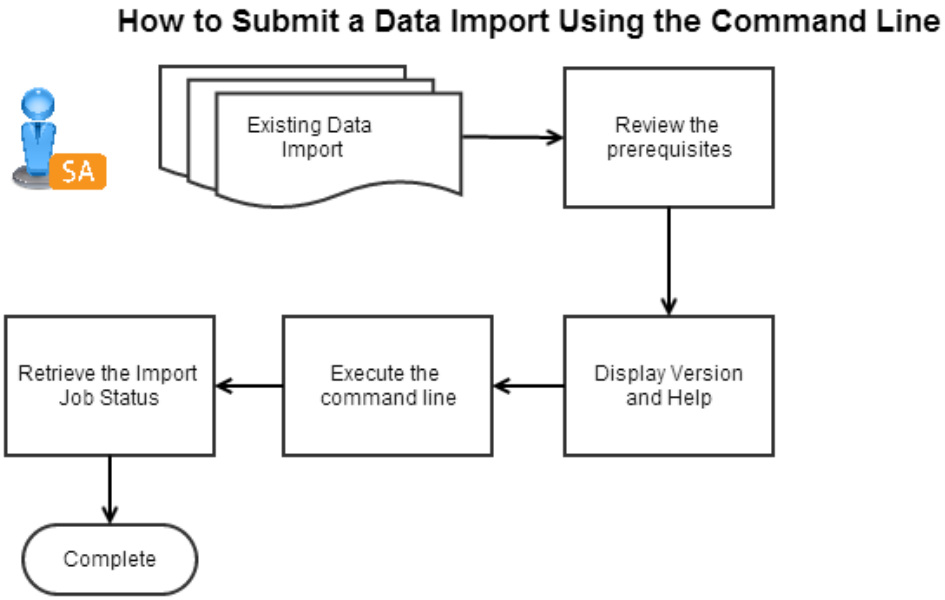
- **22001 - The data import job ID is invalid. Verify the job ID and try to execute the import again.**
  Verify the job ID by logging in to CA APM and locating the data import job. Resubmit the data import with the valid job ID.

How to Submit a Data Import Using the Command Line

You can use a command line to submit a Data Importer data import for processing instead of using the CA APM user interface. You can execute the command line from the Import Processor folder on the application server where the product is installed. You can also copy the Import Processor folder to another computer. The users of that computer can then execute the command line, also.

The data import is submitted immediately and is executed by the Data Importer Engine with other import jobs from the CA APM user interface. You cannot schedule a data import to execute at a particular time using the command line. However, you can use a scheduler (such as the operating system scheduler) to specify dates and times to run the data import.

The following diagram illustrates how a system administrator submits a data import using the command line:



To submit a data import using the command line, perform these steps:

1. Review the Prerequisites (see page 1663).
2. (Optional) Display Version and Help (see page 1664).
3. Execute the Command Line (see page 1664).
4. Retrieve the Import Job Status (see page 1665).

Example: Import New Hardware Devices

Sam, the CA APM system administrator at Document Management Company, has an existing data import that adds new hardware devices to the data repository. Sam wants to execute that data import daily. Sam also wants to verify the status of the submitted import job. However, he does not want to log in to the product to perform the import because he does not always perform other product functions on a daily basis. Sam uses the command line to submit the data import and then verify the status.

Review the Prerequisites

To ensure that you can successfully submit a data import using the command line, verify that you have completed the following prerequisites:

1. Verify that Microsoft .NET Framework 4.0 is installed on the computer where you are executing the command line.

2. Define a data import with all mappings and settings through the CA APM user interface.

3. (Optional) If you change the Import Service URL, modify the ImportProcessor.exe.config file to reflect the new URL. You can locate the ImportProcessor.exe.config file in the Import Processor folder. Update the endpoint address value.
   Example: The following statements show an example of the endpoint address value that you modify to change the Import Service URL.

```
<endpoint address="http://localhost/ImportService/ImportService.svc"
    binding="basicHttpBinding" bindingConfiguration="
BasicHttpBinding_ImportService"
    contract="IImportService" name="BasicHttpBinding_ImportService" />
```

Display Version and Help

Specify the command line parameters to display the command line version and usage help.

Follow these steps:

1. Log in to the application server where you installed CA APM or to a computer that has the Import Processor folder.

2. Access the Import Processor folder.

   On the application server, the Import Processor folder is located in the CA APM installation path.

3. Open a command prompt window and execute the following command:

```
importerprocessor -H | -V
```

   - **-H**
     Displays the command line version number and usage help for the command line parameters.

   - **-V**
     Displays the command line version number.

Execute the Command Line

Specify the command line parameters to submit a data import.

Follow these steps:

1. Log in to the application server where you installed CA APM or to a computer that has the Import Processor folder.

2. Access the Import Processor folder.

   On the application server, the Import Processor folder is located in the CA APM installation path.

3. Open a command prompt window and execute the following command:

```
importerprocessor -usr "user_name" -pwd "password" -i "import_name"
 - df  "data_file_absolute_path" -t "tenant_name"  - ts -c
```

   - **-usr**
     Specifies the CA APM login user name.
   - **-pwd**
     Specifies the CA APM login password.
   - **-i**
     Specifies the name of the data import that was created previously through the CA APM user interface.
   - **-df**
     Specifies the absolute path of the data file that is associated with the data import. The Data Importer Engine uses this file to process the import.
   - **-t**
     (Required for multi-tenancy) Specifies the name of the tenant that is associated with the data import.
   - **-ts**
     (Optional) Specifies that the command line parameters are recorded in the Import Processor log file.

     The Import Processor log file is located in the Import Processor folder.

   - **-c**
     (Optional) Identifies whether the data import was provided with the product or was created by a user.
     Valid values: 1 (product provided) or 0 (created by a user)
     Default: 0

Retrieve the Import Job Status

Specify the command line parameters to verify the status of an import job.

Follow these steps:

1. Log in to the application server where you installed CA APM or to a computer that has the Import Processor folder.

2. Access the Import Processor folder.

   On the application server, the Import Processor folder is located in the CA APM installation path.

3. Open a command prompt window and execute the following command:

   ```
   importerprocessor -usr "user_name" -pwd "password" -j "job_id"  - ts
   ```

   - **-usr**
     Specifies the CA APM login user name.

   - **-pwd**
     Specifies the CA APM login password.

   - **-j**
     Specifies the import job ID.

   - **-ts**
     (Optional) Specifies that the command line parameters are recorded in the Import Processor log file.

     The Import Processor log file is located in the Import Processor folder.

Managing Product-Provided Data Imports

This article contains the following topics:

Product-Provided Data Import Types

The product provides a set of predefined data imports that already contain all mappings and settings. These imports help you get started with data management. The two types of product-provided data imports allow you to perform the following functions:

- Read-only data imports - Allow you to monitor internal system functions, such as the LDAP Sync import of contacts.

- Object imports - Allow you to perform imports of common objects, such as locations, contacts, and assets.

You cannot modify the mappings and settings in the product-provided data imports. However, you can copy the imports and modify the copies.

Monitor the Status of Product-Provided Read-Only Data Imports

The read-only data imports perform internal system functions. You can monitor the status of the read-only imports, but you cannot submit these imports. You can copy the read-only imports and modify the copies to create your own imports.

Follow these steps:

1. Navigate to Administration, Data Importer.
2. Click one of the product-provided read-only data imports (not the object data imports). The following fields require explanation:
   - **CA APM - LDAP Sync Import**
     Submits a data import with the data file that CA EEM generated. This data import creates contacts through the LDAP Sync component.
   - **CA APM - Device Delete Import**
     Submits a data import with the data file that CA SAM generated. This data import deletes the information that is associated with deleted discovered assets.
   - **CA APM - Device Insert or Update Import**
     Submits a data import with the data file that CA SAM generated. This data import adds or updates the information that is associated with discovered assets.
3. Click Associated Jobs on the left side of the page.
4. Click Status Message in the list of import jobs to view the status of an import.

Submit the Product-Provided Object Data Imports

The product-provided object data imports perform imports of common objects. You can submit these imports, and you can monitor the status of these imports. To submit a product-provided object data import, verify that data was added to the associated data files. You can also specify your own data file. However, the column headers in your data file must match the column headers in the product-provided data file.

You can also copy these imports and modify the copies to create your own imports.

In a multi-tenanted environment, these imports add to or update the data in the Public Data tenant.

Follow these steps:

1. Navigate to Administration, Data Importer.

2. Click one of the product-provided object data imports (not the read-only imports). The following fields require explanation:

   - **CA APM - Company Import**
     Creates and updates companies.
   - **CA APM - Cost Center Import**
     Creates and updates cost centers.
   - **CA APM - Location Import**
     Creates and updates locations.
   - **CA APM - Contact Import**
     Creates and updates contacts.

     If you are using multi-tenancy, you cannot submit this import. Copy this import, add a mapping for the tenant, and submit your new contact import.

   - **CA APM - HW Model Import**
     Creates and updates hardware models.
   - **CA APM - HW Asset Import**
     Creates and updates hardware assets.
   - **CA APM - Unreconciled Discovered Assets Import**
     Creates and updates discovered assets.

     A CA Business Intelligence report about unreconciled discovered assets provides input for this data import. This CA Business Intelligence report does not include the Class and Status fields. Add these fields to the data file that corresponds to this import.

3. Specify your own data file in the Schedule area or use the product-provided data file.

   The product-provided data file does not contain data. Add the data that you want to import into the product-provided data file before you submit the import. You can find the product-provided data files at the following locations on the CA APM application server where the Storage Manager Service is installed.

   ```
   [ITAM Root Path]\Storage\Common Store\Import
   ```

4. Click Submit.

CA APM Environment Promotion

The CA Asset Portfolio Management Environment Promotion lets you promote the changes across environments with minimal manual effort. As a system administrator, you can promote any change across development, test, pre-production, and production environments.

Initiate CA Asset Portfolio Management Environment Promotion either through the user interface (UI) or command-line interface (CLI).

This article contains the following topics:

Prerequisites for Environment Promotion

1. Ensure that you meet the CA APM Environment Prerequisites (see page 686).
2. To promote content from the source to the target system, ensure that CA APM 14.1.02 patch is applied on CA APM 14.1 or CA APM 14.1.1.
3. During import, stop all CA APM services and resume them after the import is completed.

How Environment Promotion Works

- Environment Promotion involves the creation of an export package by promoting the configurations and content from the source system.
- To promote content to the target system, the system administrator must copy the export package and perform a dryrun and import.

Important! Initiate Environment Promotion to promote the custom changes.

Operations that are i nitiated through the command-line interface must be performed on the CA APM component server (First application server).

Supported Operations

Note: The supported operations must be executed after you change the directory to CA APM Promotion folder.

The following table lists the supported operations for CLI and CA APM UI:

Operation	Purpose	CLI	CA APM UI
Export	Create an export package to promote the configurations and content from the source system.	Yes	Yes *
DryRun	Validate the compatibility of the export package in the target system without actually importing it.	Yes	No
Import	Import the exported package in the target system.	Yes	No
History	Provide end-to-end execution history details such as package content, change initiator, and reason for change in the production environment.	Yes	No
Help	Display a list of commands applicable for Environment Promotion.	Yes	No
Version	Display the CA APM version that is installed with the patch levels.	Yes	No

* Indicates that only object-level filtering capability is supported.

Important! We recommend that you initiate the export operation through the CA APM UI.

Environment Promotable Objects

The following objects are eligible for Environment Promotion:

- List Management Data
- Configuration (Global and Local)
- Roles
- Search Definition
- Export Definition
- Reconciliation Rule
- Data Filter Definition
- Event Definition
- Data Import Definition

Support for Multi-Tenancy

Important! Before you initiate CA APM Environment Promotion, we recommend that you manually verify tenant hierarchy between the source and the target system.

- Before you promote the content, ensure that the tenant in the source and the target system is the same.
- Environment Promotion does not create, update, or delete any tenant on the target system.
- Before you promote the source content to the target system, Environment Promotion verifies if the tenant name and tenant group on the target system matches with that of the source. If the verification fails, the source content is not promoted to the target.

How to Promote Configurations and Content from the Source to the Target Systems

Syntax for Supported Operations

The following table lists the supported operation and its syntax:

Operation	Command Line Syntax	Command Line Syntax (Target Directory)
Export	>apmp -a export	apmp -a export -fp <File_Path>
Dryrun	>apmp -a dryrun -p <export_pkg_name>.zip	>apmp -a dryrun -fp <File_Path> -p <export_pkg_name>.zip
Import	>apmp -a import -p <export_pkg_name>.zip	>apmp -a import -fp <File_Path> -p <export_pkg_name>.zip
History	>apmp -a history	
Help	>apmp -help	
Version	>apmp -version / -v	

To promote custom configurations and content from the source to the target systems, perform the following tasks:

- Export (see page 1671)
  - Verify Prerequisites (see page 1671)
  - How to Perform Export (see page 1672)
  - Verify the Export (see page 1673)
  - How to Cancel Export (see page 1673)
- DryRun (see page 1673)
  - How to Perform DryRun (see page 1674)
  - DryRun Status Definition (see page 1674)
- Import (see page 1675)
  - Verify Prerequisites (see page 1675)
  - How to Perform Import (see page 1675)
  - Verify the Import (see page 1675)

Export

Verify Prerequisites

- You must have the CA APM administrator account name and password.

- Ensure that you have sufficient disk space (at least 500 MB) on the system where you plan to export.
- Ensure that CA Asset Portfolio Management - Export Service is running.
- While exporting to a shared location, ensure that you have sufficient write permissions and sufficient disk space (at least 500 MB) for the shared path.

How to Perform Export

To promote the configurations and content from the source system, use the **Environment Promotion** option in the CA APM UI.

Note: You can initiate multiple exports. However, only one job can be processed at a time and the other jobs are scheduled in the queue.

Follow these steps:

1. Log in to CA APM as a system administrator.
2. Navigate to **Administration, Environment Promotion**.
3. (Optional) Define the following filter values:
   - From Date
   - To Date
   - Last Modified User
4. Click **Go.**
5. Select the object(s) from the list of **Object Type**.
6. (Optional) Click the magnifying glass icon to sub-select from the list of **Object Type**.
7. Click **Export**.
8. (Optional) Add a comment and click **Submit**.
9. Navigate to **Administration**, **Environment Promotion**, **View Jobs**, **View Log** to view the status of the submitted export package. The status can be any one of the following:
   - **Not Started**: Specifies that the export package is scheduled in the queue.
   - **Running**: Specifies that the export package is running.
   - **Complete**: Specifies that the export package is exported successfully.

- **Canceled:** Specifies that the export is cancelled. Displayed when a user cancels any running operation using the **Cancel** button.
- **Failed:** Specifies that the export job fails.
- **Interrupted:** Specifies that the export job is interrupted.

Verify the Export

- After completion, you can view the exported package in the *Root/APM Promotion/Export* folder. Check the apmp_export_time stamp.zip export package.
- To verify errors or failures encountered during the export process, check the *apmp.log* in the Root */APM Promotion/logs* folder.

How to Cancel Export

You can cancel an export job only if the status is **Not Started**.

Follow these steps:

1. Log in to CA APM as a system administrator.
2. Navigate to **Administration** tab, **Environment Promotion**, **View Jobs**.
3. Select the export job that you want to cancel and click **Cancel Job.**
   The confirmation dialog appears.
4. Click **Ok**.
   The export is cancelled and the job status changes to Canceled.

DryRun

Perform a DryRun to validate the compatibility of the export package in the target system without actually importing it.

For example, Visibility is a property of the foreign key search configuration attribute. The visibility of the foreign key search configuration attribute in the source is promoted to the target environment.

If the source target attributes visibility is set to **Search Criteria** and on the target system it is set to **Search Results,** after Environment Promotion the target environment attributes visibility changes to **Search Criteria**.

Important! We recommend that you perform a DryRun before initiating the import to ensure that the changes are promoted without any failure.

How to Perform DryRun

We recommend that you initiate DryRun before executing the Import process.

Follow these steps:

1. Copy the export package from the source system to target system and paste this package in the *Root/APM Promotion/Import* folder.
2. Click Start, Run to open the command prompt (cmd) window.
3. Change the directory to the CA APM Promotion folder.
4. Execute the DryRun command (see page 1671).
5. Enter the CA APM System Administrator User Name and press Enter.
6. Enter the CA APM System Administrator Password and press Enter.
   The DryRun operation is completed and a summary report is created.
7. Press Enter to exit the console.
8. Navigate to the *Root/APM Promotion/DryRun* folder.
9. Access the apmp_dryrun_timestamp.csv file.
10. Sort the file by status, and take corrective measure for the records with status **Conflict**.

> **Important!** For a successful import, we recommend that you take corrective measure for the records with status **Conflict**.

DryRun Status Definition

The following table lists the DryRun status definition:

Status	Definition
New	The source content does not exist on the target system and hence it is promoted to the target system.
Update	The source content matches the target content and hence it is promoted to the target system.
Skip	The source content is not promoted to the target system as the dependent content does not exist on the target system.
Conflict	Due to a conflict with the target content, the source content is not promoted to the target system. For example, the source and target system **global configuration** names are the same, however the object types/sub-types are different .

Status	Definition
Conditional	The source content is promoted only when the dependent content is available on the target system while importing.

Import

Verify Prerequisites

- Back up your system database (MDB). This ensures safe data recovery if any problems are encountered.
- You must have the CA APM administrator account name and password.
- The target environment must be at the same patch level as the source environment.
- Copy the export package from the source system to target system and paste this package in the *Root/APM Promotion/Import* folder.
- Ensure that you have sufficient disk space (atleast 500 MB) on the target system where you plan to import.
- The DB server (Oracle or MS SQL) on the source and target system must be the same.

How to Perform Import

After a successful DryRun, initiate the Import process to promote the content to the target system.

Follow these steps:

1. Click Start, Run to open the command prompt (cmd) window.
2. Change the directory to the CA APM Promotion folder.
3. Execute the Import command (see page 1671).
4. Enter the CA APM System Administrator User Name and press Enter.
5. Enter the CA APM System Administrator Password and press Enter.
   After a while the import operation completes.
6. Execute the following command to stop and restart IIS:

   ```
   iisreset
   ```

7. Press Enter to exit the console.
8. Copy the Data Importer dependent files from the source system to the target system in the *Root/Storage/Common Store/Import* and *Root/Storage/Tenant Name/Import* folders.

Verify the Import

After importing the content to the target system, verify the changes are reflected on the target system.

1. A summary report is generated in the *Root/APM Promotion/Import* folder. Check the *apmp_import_timestamp.txt* file.

2. If any failures are encountered during import, rerun the import process using the same package.
   The import process restarts from the point of failure.

> **Note:** To verify errors or failures encountered during the import process, check the *apmp.log* in the Root */APM Promotion/logs* folder.

CA APM Environment Promotion Limitations

The following limitation applies to CA APM Environment Promotion:

- The new data importer definitions are promoted, however the job schedules are not promoted.
- The new data importer definitions are promoted, however the related data files and legacy map files are not promoted.

Object Status After Mapping from Source to Target Systems

This article describes the Environment Promotion behavior at an object level.

List Management Data

For example, when the source and target system contain the same list management data and tenant name, then the object is promoted to the target system with operation status as Skip.

List Management Data	Tenant Name	Operation
Same	Same	Skip
Same	Different	New
Different		New

Configuration

For example, when the source and target system contain the same global configuration and type /subtype, then the object is promoted to the target system with operation status as Update

Configuration Name	Global Configuration	Type /Subtype	Operation
Same	Yes	Same	Update
Same	Yes	Different	Conflict
Same	No	Same	Update
Same	No	Different	Conflict
Different	Yes	Same	Conflict
Different	Yes	Different	New
Different	No	Same	New
Different	No	Different	New

Roles

For example, when the source and target system contain the same roles, then the object is promoted to the target system with operation status as Update.

Roles	Operation
Same	Update
Different	New

Search Definition

For example, when the source and target system contain the same search definition name and type /subtype, then the object is promoted to the target system with operation status as Update.

Search Name	Type/Subtype	Operation
Same	Same	Update
Same	Different	Conflict
Different		New

Export Definition

For example, when the source and target system contain the same export definition and tenant name, then the object is promoted to the target system with operation status as Update.

Export Definition	Tenant Name	Operation
Same	Same	Update
Same	Different	Conflict
Different		New

Reconciliation Rule

Source reconciliation rules overwrite the target reconciliation rules.

Data Filter Definition

For example, when the source and target system contain the same data filter definition and type /subtype, then the object is promoted to the target system with operation status as Update.

Data Filter Definition	Type/Subtype	Operation
Same	Same	Update
Same	Different	Conflict
Different		New

Event Definition

For example, when the source and target system contain the same event definition and PAM workflow name, then the object is promoted to the target system with operation status as Update.

Event Definition	PAM Workflow Name	Operation
Same	Same	Update
Same	Different	New
Different		New

Data Import Definition

For example, when the source and target system contain the same data import definition and tenant name, then the object is promoted to the target system with operation status as Skip.

Data Import Definition	Tenant Name	Operation
Same	Same	Skip
Same	Different	New
Different		New

Extended Field

For example, when the source and target system contain the same extended field and type/subtype, then the object is promoted to the target system with operation status as Skip.

Extended Field	Type /Subtype	Operation
Same	Same	Skip
Same	Different	Skip
Different		New

Configuring Unified Self-Service

This section contains the following articles:

Onboard Tenants

This article contains the following topics:

After the Unified Self-Service installation, create tenants by onboarding them. Tenants are your customers or partners who share Unified Self-Service environment and can use the Unified Self-Service capabilities.

Create a Tenant

Create a unique tenant in Unified Self-Service so that the tenant can access the Unified Self-Service capabilities.

Follow these steps:

1. Log in to the following URL as the administrator:

   ```
   http://Web Host:Tomcat Port/web/guest/onboarding
   ```

   Note: On Windows you can also select Start, Program, All Programs, CA, Unified Self-Service, Onboarding to create a tenant.

2. Provide the following details:

- **Company Name**
  Specifies the company name of the tenant that you want to onboard. Depending on your input for this field, Web ID, Mail Domain, and Company Host fields are pre-populated. You can modify these pre-populated fields according to your organization requirements.
  Example: Company Inc

- **Web ID**
  Specifies the web domain of the tenant. This ID is a user-generated ID for the instance. A web ID must be unique.
  Example: company.com

- **Mail Domain**
  Specifies the mail domain of the tenant that you are boarding. Unified Self-Service uses this information to send email notifications from the portal. This mail domain is a domain part of the email address. If your email is someone@company.com, then company.com is the mail domain.
  Example: company.com

- **Company Host**
  Specifies a unique host name for the tenant. There can be multiple examples within the same domain. For example, Finance.company.com, HR.company.com. Here, Finance or HR are tenant host names.
  Example: test.company.com

  Note: The Web ID, Mail Domain, and Company Host must not contain special characters.

3. Click **Next**.

4. Provide the login credentials of the tenant administrator.

   - **Admin ID**
     Specifies the user name of the tenant administrator.

   - **Password**
     Specifies the password for the tenant administrator.

   - **Confirm Password**
     Enter the password again.

5. Click **Next**.
   The OnBoarding summary page is displayed.

6. Click **Start Onboarding**.
   The OnBoarding page is displayed.

> **Note:** Add an entry in the DNS server with the Company Host of the new tenant pointing to the Unified Self-Service server. For the testing purpose, you can add an entry in the C:\Windows\System32\drivers\etc\hosts on the client machine for the onboarded tenant.

Format: <*Unified_Self_Service_Server_IP_Address*> <*Company_Host*>

Example: 10.131.87.34 test.company.com (http://test.company.com)

7. Click **Go to Company Portal**.
   The Company portal opens. Share this portal detail with the tenant. After you create a tenant, the onboarding process creates a set of default users with different roles.

8. Log in to the Unified Self-Service tenant control panel as a tenant administrator.
   Example: http://<*Company_Host_Name*>:8686/group/control_panel

9. Navigate to Control Panel, Users and Organizations.
   The default users are listed. The default users are created with the password aquila.

Disable Onboarded Tenant

An administrator can disable an onboarded tenant from the Unified Self-Service control panel. This action cannot be performed by the tenant administrator from the Unified Self-Service tenant control panel.

Note: A default tenant cannot be disabled.

Follow these steps:

1. Log in to the Unified Self-Service control panel as the administrator.
   Example: http://<*Unified_Self_Service_Server_Name*>:8686/group/control_panel

2. Select Server, Portal Instances, and click on the Web ID of the onboarded tenant.
   The onboarded tenant details are displayed.

3. Clear the **Active** check box and click **Save**.
   The tenant is disabled.

Authenticate Users

You can authenticate Unified Self-Service users using one of the following methods:

- Configure CA EEM Authentication (see page 1682)
- Configure CA EEM With NTLM Authentication (see page 1683)
- Configure CA SiteMinder Authentication (see page 1684)
- Configure CA SiteMinder With CA EEM Authentication (see page 1686)

- Import Users from LDAP (see page 1687)

Configure CA EEM Authentication

If you have an existing installation of CA EEM, you can use the same for authenticating Unified Self-Service users. For more information about installing and configuring CA EEM, see the CA EEM documentation. Specify the EEM authentication details in Unified Self-Service for CA EEM users to log in to Unified Self-Service.

Follow these steps:

1. Log in to the Unified Self-Service tenant control panel as a tenant administrator.
   Example: http://<*Company_Host_Name*>:8686/group/control_panel

   Note: To configure the CA EEM authentication for a default tenant, login to the http://<*Unified_Self_Service_Server_Name*>:8686/group/control_panel URL as the administrator.

2. Under Portal, select Portal Settings, Authentication, EEM.

3. Select the Enabled check box to use CA EEM authentication and enter the following information:

   - **EEM Server Name**
     Specifies the host name of the CA EEM server.

   - **EEM Administrator Username**
     Specifies the CA EEM Admin username.

   - **EEM Administrator Password**
     Specifies the password for the **EEM Administrator Username**.

   - **EEM Application Administrator Group**
     Specifies the CA EEM group whose members are to be imported as administrators in Unified Self-Service.

     Important! This field is pre-populated with the OpenSpaceAdminGroup name, which you can modify. Ensure that a group is created in CA EEM with this **EEM Application Administrator Group** name and all your CA EEM users (who are intended to be Unified Self-Service administrators) are added to this group. All the users who are part of this group are considered as administrators of Unified Self-Service.

   - **EEM Default User Role (Optional)**
     Specifies the CA EEM role (Administrator or Business User) who is added after the authentication.

Important! If this role is not specified, then all the users are imported to Unified Self-Service as Business Users.

- **EEM Application Name (Optional)**
  Specifies the application within a CA EEM server, which is used for authentication.

- **EEM User Default Organization (Optional)**
  Specifies the default organization of the user. Enter the name of the organization (Web ID) that you specified during onboarding.

4. If you want to configure CA EEM with NTLM authentication, select the **Enable NTLM(v1) Authentication** check box. For more information about the CA EEM with NTLM authentication, see the Configure CA EEM With NTLM Authentication (see page 1683) topic.

5. Click **Save**.
   CA EEM authentication is configured.

Note: If the users are unable to log in Unified Self-Service using the CA EEM authentication, disable the CA EEM authentication (see page 1683).

Disable the CA EEM Authentication

If the users are unable to log in Unified Self-Service using the CA EEM authentication (this may happen because of incorrect or modified CA EEM server name) disable this authentication.

Follow these steps:

1. Log in to the Unified Self-Service server.

2. Open the portal-ext.properties file located in the OSOP folder of the Unified Self-Service installation directory.

3. Add the <*tenant-web-id*>.eem.authentication.enabled.override flag to true and save the file.
   For example, tenantA.eem.authentication.enabled.override=true. This Web ID can be obtained from the Portal Instances page of the Unified Self-Service control panel.
   The CA EEM authentication settings for that tenant are ignored by Unified Self-Service. The Enabled check box on Unified Self-Service tenant control panel may still be checked, but it does not affect the CA EEM authentication if the flag is set to true.

Configure CA EEM With NTLM Authentication

Configure the CA EEM with NTLM authentication for a logged in domain user to silently (SSO) log in to Unified Self-Service.

Follow these steps:

1. Ensure the following considerations:

- Unified Self-Service server and CA Service Catalog server must be in the same domain where you want to use the windows authentication. CA EEM server must be configured with Active Directory of the same domain.
- Active Directory users should be able to login to the client machine present in this domain.

2. Log in to the Unified Self-Service tenant control panel as a tenant administrator.
   Example: http://<*Company_Host_Name*>:8686/group/control_panel

   Note: To configure the CA EEM with NTLM authentication for a default tenant, login to the http://<*Unified_Self_Service_Server_Name*>:8686/group/control_panel URL as the administrator.

3. Select Portal Settings, Authentication, EEM.
4. Configure CA EEM Authentication (see page 1682) for the Unified Self-Service server.
5. Verify the CA EEM with NTLM authentication:
   a. Ensure that CA SDM and CA Service Catalog data sources integrated with Unified Self-Service. For more information, see the Configure Data Sources (see page 1687) topic.
   b. Ensure that the integrated CA SDM and CA Service Catalog data sources are also authenticated with NTLM for the CA SDM details and CA Service Catalog widgets to appear on Unified Self-Service. For more information, see the respective product documentation.
   c. Enter the Unified Self-Service URL.

   Windows users should be able to log in without being asked for the credentials.
6. (Optional) To use the NTLM authentication on the Mozilla Firefox browser, complete the following steps:
   a. Enter about:config on the Firefox browser.
   b. Search for ntlm.
   c. Enter the Unified Self-Service URL (that is to be authenticated with NTLM) and CA Service Catalog URL as the network.automatic-ntlm-auth-trusted-uris value, separated by comma.

Configure CA SiteMinder Authentication

Specify the CA SiteMinder authentication details in Unified Self-Service so that users with CA SiteMinder credentials can log in to Unified Self-Service.

Follow these steps:

1. Install the Apache server and install CA SiteMinder agent on the Apache server.

2. Open the httpd.conf file located in conf folder the Apache server.
   Example: C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\

3. Ensure that the httpd.conf file has the following configuration:

```
<IfModule proxy_module>
    ProxyRequests Off
    <Proxy *>
         Order deny,allow
         Allow from all
     </Proxy>

    # This is important -
    # Don't forward URIs which starts with /siteminderagent to open space
server.
    ProxyPass /siteminderagent !

    #Forward all URI to given urls
     ProxyPass / http://<web-id-of-the-company:port>/
    ProxyPassReverse / http://<web-id-of-the-company:port>/
       ProxyPreserveHost Off
     ProxyErrorOverride On
</IfModule>
```

4. Ensure that you have enabled the following modules in the conf file:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule deflate_module modules/mod_deflate.so
LoadModule headers_module modules/mod_headers.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule rewrite_module modules/mod_rewrite.so
```

5. Stop the Apache server, wait till LLAWP.exe is killed, and start the Apache server.
   The Apache server is configured with the reverse proxy pointing to the Unified Self-Service server.

6. If you are not using a default tenant for CA SiteMinder authentication, add an entry in the DNS server with the Company Host of the new tenant pointing to the Unified Self-Service server. For testing purpose, you can add an entry in the C:\Windows\System32\drivers\etc\hosts on the Apache web server machine for the onboarded tenant.
   Format: *Unified_Self_Service_Server_IP_Address Company Host*
   Example: 10.131.87.34 test.company.com

7. Log in to the Unified Self-Service server and add the following configuration details in the portal-ext.properties file located in the OSOP folder of the Unified Self-Service installation directory:

```
#### Reverse Proxy Configuration
web.server.protocol=http
```

```
web.server.http.port=80
web.server.https.port=-1
web.server.host=<apache-host-name>
```

8. Log in to the Unified Self-Service tenant control panel as a tenant administrator.
   Example: http://<*Company_Host_Name*>:8686/group/control_panel

   Note: To configure CA SiteMinder authentication for a default tenant, login to the http://<*Unified_Self_Service_Server_Name*>:8686/group/control_panel URL as the administrator.

9. Select **Portal Settings**, **Authentication**, **SiteMinder**.

10. Select the **Enabled** check box.

11. Import Users from LDAP (see page 1687) and select the **Import Users from LDAP** check box.
    CA SiteMinder authentication is configured.

12. Verify the CA SiteMinder authentication:

    a. Log in to any machine and access the Apache server using the http:// *Apache_Server_Host_ Name*:*Apache Port Number* URL.

    b. Enter the CA SiteMinder credentials on the CA SiteMinder authentication window.
    The Unified Self-Service Home page is displayed.

Configure CA SiteMinder With CA EEM Authentication

Specify the CA SiteMinder with CA EEM authentication details in Unified Self-Service for CA SiteMinder and CA EEM users to log in to Unified Self-Service.

Follow these steps:

1. Ensure that CA SiteMinder is configured with the same LDAP directory that is configured with CA EEM and Unified Self-Service.

2. Ensure that CA Service Catalog should be configured with the same CA EEM and CA SiteMinder for the users to view the CA Service Catalog widgets in Unified Self-Service.

3. Configure CA SiteMinder Authentication (see page 1684) for the Unified Self-Service server.

4. Use the CA SiteMinder server policy configuration to ignore the /usm/services URL from the configuration object of the CA Service Catalog Agent. For more information about how to ignore the URL, see the CA SiteMinder documentation.

5. For users to access the ITSM mobile application, skip the following URLs to ignore the CA SiteMinder authentication:

   - /rest/ (to skip the REST API URLs)

- /itsm/ (to access the mobile application without any CA SiteMinder authentication).

Import Users from LDAP

Import the users from LDAP to Unified Self-Service.

Follow these steps:

1. Log in to the Unified Self-Service tenant control panel as a tenant administrator.
   Example: http://*<Company_Host_Name>*:8686/group/control_panel

   Note: For a default tenant, login to the http://*<Unified_Self_Service_Server_Name>*:8686/group/control_panel URL as the administrator.

2. Click Portal Settings, Authentication, LDAP.
3. Select Enabled and Import Enabled check boxes.
4. Click Add to enter the LDAP details.
5. Click Save.
   The LDAP users are imported to the database.

Note: For more information about importing users from LDAP, see the Liferay documentation.

Configure Data Sources

Unified Self-Service integrates with several data sources to provide rich search results and extended application functionality. You can integrate Unified Self-Service with the following data sources:

- CA Service Desk Manager
- CA Service Catalog
- Google
- Microsoft SharePoint

To learn how to configure the data sources, see the following articles:

- How to Configure CA SDM Data Source (see page 1688)
- How to Configure the CA Service Catalog Data Source (see page 1692)
- How to Configure the Google Data Source (see page 1693)
- How to Configure the Microsoft SharePoint Data Source (see page 1694)

How to Configure CA SDM Data Source

Configure the CA SDM data source for the users to create, review, and update their requests directly within Unified Self-Service, and search knowledge base articles within the CA SDM Knowledge Base. In addition, you can enable Live Chat in the Unified Self-Service interface to allow users to chat with an IT analyst and also allow users to access the CA SDM mobile application.

Follow these steps:

1. Verify Prerequisites (see page).
2. Configure CA SDM Data Source (see page).

Verify Prerequisites

Verify the following prerequisites before configuring the CA SDM data source:

- CA SDM 12.6, 12.7, or 12.9 must be installed and configured with Unified Self-Service.
- Create or use DEFAULT Web Services Access Policy from CA SDM. Ensure that you select the Allow Impersonate check box and you enter the Proxy Contact detail for this policy.
- Generate an authentication certificate for the Access Policy. CA SDM provides a server-side utility that can generate a certificate. Execute the following command from the CA SDM server to generate the certificate for the access policy:

  ```
  pdm_pki -p policy_name
  ```

  This command generates an authentication certificate file *policy_name*.p12. Upload this file during the CA SDM data source configuration with Unified Self-Service.
- Ensure that the Unified Self-Service users available in CA SDM have the same User ID and email address for a successful configuration.
- For Unified Self-Service users to use CA SDM live chat, Support Automation must be set up in CA SDM. For more information, see Support Automation (see page 2821).

Customize CA SDM Data Source Property

As an administrator, define the maximum number of CA SDM fields that a user can configure in the Unified Self-Service (USS) console.

Follow these steps:

1. Log in to Unified Self-Service server as an administrator.
2. Navigate to the OSOP folder and edit the file: *portal-ext.properties*
3. In the *sdm.configFields.maxFieldsToShowInConfigOptionsPage* property, define the maximum number of CA SDM fields that you want to configure on the USS console.
   The default value is 10.

4. (Optional) In a tenanted environment, you can set the maximum number of fields for each tenant using the *someCompany.com.sdm.configFields.maxFieldsToShowInConfigOptionsPage* property.

    a. Replace *someCompany.com with the* Web ID of the tenant.

    You can obtain the Web ID from the Portal Instance in the Control Panel: *http (s)://server-name:<port-no>/group/control panel > Portal Instances*
    For example, *ca.com.sdm.configFields.maxFieldsToShowInConfigOptionsPage=20*

    > **Note:** The value in the *sdm.configFields. maxFieldsToShowInConfigOptionsPage* property is overridden by the tenant specific values.

5. Save the file and restart (see page 1704) the services.

Configure CA SDM Data Source

Configure CA SDM data source for the users to create, review, and search information from CA SDM directly in Unified Self-Service.

Follow these steps:

1. Log in to Unified Self-Service as an administrator.
2. In the menu, click Settings, Data Sources.
3. Click the arrow for the CA SDM data source and enter the following configuration information:

    - **NAME**
      Specifies the name for the CA SDM data source. This name is displayed in the header for search results from the CA SDM Knowledge Base.
    - **TICKET TYPE**
      Indicates the type of Help desk tickets that are implemented in your organization.
    - **LABEL FOR TICKET TYPE**
      Specifies the label that you want to associate with the selected ticket type.
    - **DEFAULT PRIORITY**
      Specifies the default priority level for new requests.
    - **URGENT PRIORITY**
      Specifies the priority level for urgent requests.
    - **BASE URL**
      Specifies the CA SDM server URL. To verify this value, enter the URL in a browser. If you see the CA SDM interface, then the value is correct.
      Format: http://*<CA_SDM_Server_Hostname>:<Port_Number>*/
      Example: http://servicedesk.test.com:8080

- **WSDL URL**
  Specifies the relative URL of the web services endpoint on the CA SDM server. By default, this URL is generated for you. For some CA SDM deployment configurations, you may have to override this value with a value provided to you by CA Support.
  To verify this value, enter the complete URL in a browser, that is, the Base URL plus the WSDL URL. If the value is correct, you see an XML document (the WSDL).
  Example: http://servicedesk.test.com:8080/axis/services/USD_R11_WebService?wsdl

- **SERVER HOST NAME**
  Specifies the servlet server as defined in CA SDM for Service Desk attachment repository. Since this host name is case-sensitive, run the *hostname* command from the CA SDM server and enter exactly the same value that is returned from the command.

  Important! In the advanced availability configuration, if you have used the background server host name for this field and the system administrator performs a scheduled failover, the background server becomes the standby server. You must add the new background server host name to this field after the failover.

- **ACCESS POLICY**
  Specifies the name of the Web Services Access Policy as configured during the CA SDM installation and that is used to generate the authentication certificate. Use the access policy mentioned in the Verify Prerequisites (see page) topic.

4. Click **UPLOAD CERTIFICATE** to upload the authentication certificate that you created in the Verify Prerequisites (see page) topic. The certificate file name must match the name of the **ACCESS POLICY**.

5. Follow these steps to enable live chat:

   a. Select **YES** to enable Live Chat from the Search, Home, and Request pages.

   b. (Optional) Customize the Live Chat link text (Default text: Chat with an IT Analyst now!).

   Important! Users with OOTB Customer access type cannot create tickets (incident or request) or launch live chat from Unified Self-Service. The Customer access type must have Employee as the role in CA SDM to perform these actions. For more information, see Support Automation (see page 2821) .

6. In the **INSTRUCTIONS** field, enter information that should appear at the top of new request forms.

7. In the **SERVICE DESK REST URL FOR MOBILE APP** field, enter the CA SDM server URL (where REST is installed and configured) to allow users to access the ITSM mobile application.
   Format: http://<*CA_SDM_Server_Host_Name*>:<*Rest_Port_Number*>/
   Example: http://<*CA_SDM_Server_Host_Name*>:8050/

8. Click **TEST CONNECTION**. If it fails, review the data that you entered and correct as necessary.

9. When you are ready to enable the data source for your organization, set the **STATUS** to **Enabled**.

10. Click **SAVE**.
    Unified Self-Service is integrated with CA SDM and the data source is available for your users. You can now configure the request form to include the fields and information that your organization requires.

11. Configure Request Form (see page 1691).

Configure Request Form

You can configure the request form that your organization users use to create a CA SDM request. The request form comes prepopulated with some standard fields that cannot be modified. You must add the fields that your implementation of CA SDM requires to create requests. You can also add optional fields to record any other information. The requester can fill these fields, or you can design fields that automatically pass preset information. You can add as many fields as you need to the request form. The number of fields that you can configure is defined in the *portal-ext.properties* file. For more information about configuring the maximum number of default or tenant specific fields, see Configure CA SDM Data Source Property (see page 1688).

Note: This task assumes that you are working with a CA SDM administrator. Unified Self-Service cannot discern what fields your CA SDM installation requires to create a valid request.

Follow these steps:

1. On the Data Sources page for CA SDM, click **CONFIGURE NOW**.
   The field table listing the fields that are currently in use for request forms appears.

2. To add new fields to the request form, do the following steps for each addition:

   a. Click the drop-down arrow and select the required field to add.

   b. Click **ADD FIELD**.

   c. Set values and properties for the new field as follows:

   - **DEFAULT VALUE**
     Sets a default value for the new field.

   - **DISPLAY NAME**
     Defines the field name that displays on the request form.

   - **HINT TEXT**
     Defines the instructional text that appears in the field.

- **DISPLAY**
  Controls whether the field is visible on the request form.
  Limit: Five fields.

- **REQUIRED**
  Indicates the mandatory fields that you must define before you submit the request.

> **Note:** When you select the ticket type as an Incident, the **DISPLAY NAME** and **HINT TEXT** values of the priority (string) field must be changed to an Urgent Incident. As a result, while creating the incident, you can see an Urgent Incident check box instead of an Urgent Request check box.

3. (Optional) Drag and drop the new fields into the required order.

4. Click **SAVE**.
   Your request form changes are saved and all new requests reflect the new configuration.

How to Configure the CA Service Catalog Data Source

Configure the data source for the users to create, review, and search for information from CA Service Catalog in Unified Self-Service. Before you configure this data source, verify that the Unified Self-Service tenant is configured with same CA EEM server that is configured for CA Service Catalog.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.

2. In the menu, click Settings and then click Data Sources.

3. Click the arrow for the CA Service Catalog data source and enter the following fields:

   - **NAME**
     Specifies the name of the data source.

   - **BASE URL**
     Specifies the URL to access CA Service Catalog.
     Format: http://*CA_Service_Catalog_Server_Hostname*:*Port_Number*/usm/

   - **DEFAULT REQUEST OFFERING ID**
     Specifies the ID related to the **Report an Issue** offering from CA Service Catalog. When the Unified Self-Service user clicks REPORT AN ISSUE to create a request, the request form that is displayed corresponds to this ID. You can obtain this ID from CA Service Catalog. For example, log in to CA Service Catalog, navigate to Catalog, Offerings, IT Support Services, Service Management, Report an Issue, and obtain the ID from the Details page. Ensure that the CA Service Catalog server is imported with the Service Management content pack. For more information about the content pack, see the CA Service Catalog documentation.

- **(Optional) COMMON ADMINISTRATION OFFERING ID**
  Specifies the offering ID to display the administrative service offerings of the solution. As an administrator, if you want to access the common administration service offerings quickly from the menu bar, specify the common administration offering ID from CA Service Catalog.

- **Service Desk (Tickets) View**
  Indicates whether you want users to view the CA SDM tickets (incidents or requests) on Unified Self-Service. These tickets were created before configuring the CA Service Catalog data source.

- **(Optional) MY RESOURCE OFFERING ID**
  Specifies the offering ID to display the assets owned by the logged in user. If you want the Unified Self-Service users to view the assets requested from CA Service Catalog, you must enter the **My Resources** offering ID from CA Service Catalog. You can obtain this ID from CA Service Catalog.
  For example, log in to CA Service Catalog , navigate to Catalog, Offerings, IT Support Services, Service Management, My Resources, and obtain the ID from the Details page. Ensure that the CA Service Catalog server is imported with the Service Management content pack. For more information about the content pack, see the CA Service Catalog documentation.

- **(Optional) BUSINESS UNIT**
  Specifies the name of the business unit in CA Service Catalog.

- **(Optional) EEM APPLICATION CONTEXT**
  Specifies the application context name used in CA EEM for CA Service Catalog.

4. Upload the PEM File and Key File to access CA Service Catalog. These files can be obtained from the CA Service Catalog installation directory.

5. Click **TEST CONNECTION** to test the data source connection.

   - If the connection is not successful, review the data that you entered and correct as necessary.

   - If the connection is successful, select the **STATUS** as **ENABLED**.

6. Click **SAVE**.

The CA Service Catalog data source is configured for the Unified Self-Service users to access.

How to Configure the Google Data Source

Unified Self-Service integrates with Google Search to provide search results from Google directly within Unified Self-Service. Google Search is configured for you; no additional setup is necessary. You enable or disable this feature for all users by editing the Google data source. The Google data source includes a global local setting. This setting allows you to specify a country to focus your users search results. This setting is a global setting that affects all users; users cannot set this value individually.

Follow these

1. Log in to Unified Self-Service as an Administrator.
2. In the menu, click Settings and then click Data Sources.
3. Select Data Sources from the Administration page.
4. Click the arrow for the Google data source.
5. Select STATUS as Enabled.
6. Specify the country to focus your search results for the selected geography.
7. Click SAVE.
   Google Search is enabled. When Unified Self-Service users search for information from the Google Data source, the results are provided by Google from the respective geographic region of the user.

Note: If the user is using a proxy server to use the internet, add the following entries in the portal-ext.properties file located in the OSOP folder of the Unified Self-Service installation directory:

```
# Aquila Search
aquila.search.googleProxyUserName=
aquila.search.googleProxyPassword=
aquila.search.googleProxyIP=
aquila.search.googleProxyPort=
aquila.search.useProxyForGoogle=yes
```

How to Configure the Microsoft SharePoint Data Source

This article contains the following topics:

Microsoft SharePoint is widely used as an enterprise business collaboration platform and for storing documents. Unified Self-Service search integrates with Microsoft SharePoint to include search results from your SharePoint server.

Follow these steps:

Enable SharePoint Access from the Internet

Unified Self-Service search integrates with Microsoft SharePoint to include search results from your SharePoint server. If your organization has Microsoft SharePoint (that is implemented within your Intranet), integration with Unified Self-Service requires some additional configuration. This configuration requires a SharePoint server that can be accessed from the Internet. The SharePoint server can either be your primary application server, if it is accessible from the Internet, or a secondary server could be deployed in the DMZ.

Follow these steps:

1. On Microsoft SharePoint 2003/2007, open the SharePoint Central Administration Site.
   Note: The navigation may vary based on the Microsoft SharePoint version you deployed. Microsoft SharePoint 2003/2007 is considered only as an example.

2. Select the Operations tab.

3. Under Global Configuration, click Alternate access mappings.

4. Click Add Internal URL.

5. Select the Alternate access mappings collection for the SharePoint site that you want to connect to Unified Self-Service.

6. Add all Unified Self-Service server hostname URLs.
   Example: http://*Unified_Self_Service_Server_Hostname*/
   Once you add the hostnames to the SharePoint Alternate access mappings, you can integrate Unified Self-Service with your SharePoint instance.

Configure the Microsoft SharePoint Data Source

Configure the Microsoft SharePoint.data source to search information from the SharePoint server in Unified Self-Service.

Follow these steps:

1. Log in to Unified Self-Service as an Administrator.

2. In the menu, click Settings and then click Data Sources.

3. Click the arrow to enter the following configuration information.

   - **NAME**
     Defines the data source name.

   - **URL**
     Defines the URL of your web service that your SharePoint server hosts and is accessible from the Internet.
     Format: http://<hostname>

- **USER NAME**
  Identifies the user name of a user who has access to documents stored in SharePoint. This name is used for authentication for the search API. However, it is the logged in user that determines the document access level.

- **PASSWORD**
  Identifies the password of the user that is listed for User Name. This password is used for authentication.

4. If you enabled the Unified Self-Service Connection, select YES to use it.

5. Click **TEST CONNECTION** to test the data source connection. If the test is not successful, review the data that you entered and correct as necessary.

6. When you are ready to enable the data source for your organization, set the **STATUS** to **ENABLED**.

7. Click **SAVE**.
   Microsoft SharePoint data source is configured in Unified Self-Service.

How to Create and Manage Communities

This article contains the following topics:

As a tenant administrator, you create a community in Unified Self-Service and assign the community owners. Community owners manage the communities in your organization.

Create a Community

A tenant administrator creates a community (apart from the existing General Topics community) in Unified Self-Service to facilitate communication among members on a specific subject. You can create two types of communities using Unified Self-Service:

- **Open**
  Specifies an open community that is accessible to every Unified Self-Service user. All users can view posts in an open community, however only members can reply or post messages. Members can join or leave the community any time.

- **Private**
  Specifies a private community that is restricted and designed for a limited audience to use for private conversations. Members outside the private community cannot see these communities or post messages. Only the community owner and the tenant administrator can add or remove members.

Follow these steps:

1. Log in as the tenant administrator and access the following URL:

   ```
   http://<Company_Host_Name>:<Port_Number>/
   ```

   Note: For a default tenant, log in as an administrator and access http://<*Unified_Self_Service_Server_Name*>:<*Port_Number*> URL.

2. In the Menu bar, click Settings, Communities.

3. Click Add Community.

4. Enter a name for the new community, select the type, and specify a description that explains the purpose and scope of the community.

5. Click Save.
   The community is created.

Assign Community Owners

The tenant administrator assigns owners to a community.

Follow these steps:

1. On the Manage Communities page, find the community to which you want to assign an owner and click the edit icon  .
   The Community details page appears.

2. Select the Owner check box against the user that you want to assign as an Owner.

   Note: You can assign more than one owner for a community.

3. Click Save.
   The community owners are assigned.

Add Community Members

Users can either join a community directly or request to join depending on whether the community is open or private. Community owners are responsible for individual communities.

Note: Only a community owner can add community members.

Follow these steps:

1. On the Manage Communities page, navigate to the community you want to add members and click the icon  .
   The Member Directory page appears.

2. Select the check box next to the names you want to add as members.

3. Click Save, Done.
   The new community members are added.

Note: The tenant administrator creates communities. The community owners can monitor their own communities.

Monitor the Community

Community owners monitor the community content for its accuracy and track activities on the Unified Self-Service console. The community owner takes care of the memberships.

Email notifications are sent for every post on the community. Community owners need to monitor the posts and delete inappropriate posts, if any.

Follow these steps:

1. Open the email notification about the inappropriate post and click the link provided in the email.
   The Unified Self-Service login page opens.

2. Log in to Unified Self-Service.

3. Verify the inappropriate post that the community member has reported.

4. Delete the post by clicking the delete icon or modify the inappropriate post.

After you create and manage the communities, the members of the communities can communicate and collaborate effectively.

Enable or Disable the Community

As a USS administrator, you can enable or disable the community from the USS console for all or specific tenants.

Follow these steps:

1. Log in to Unified Self-Service server as an administrator.
2. Navigate to the *$US4SM/*OSOP folder and edit the file: *portal-ext.properties*

   Note: *$US4SM* is the default Open Space installation directory.

3. Set the *disable.uss.community* property value to *true* to disable the community from the console.
   By default, the community board is enabled.
4. (Optional) Disable the community for a specific tenant by setting the value in the *someCompany.com.disable.uss.community* property.
5. Replace *someCompany.com* with the Web ID of the tenant.
   You can obtain the Web ID from the Portal Instances in the Control Panel: *http(s)://server-name:<port-no>/group/control panel > Portal Instances*
   For example, ca.com.*disable.uss.community=true*
   The value in *disable.uss.community* property is overridden by the tenant specific values.

   Note: By default, the community is enabled for all tenants.

6. Save the file and restart (see page 1704) the services.

Configure Notifications

This article contains the following topics:

Enable Web Notification Feature

By default, the web notification feature in Unified Self-Service is disabled. You must enable it to use the feature.

Important! Enabling this feature may lead to performance degradation.

Follow these steps:

1. Log in to the Unified Self-Service server.
2. Open the portal-ext.properties file located in the OSOP folder of the Unified Self-Service installation directory.
3. Set the value for the following variables:

```
cometd.enable=true
live.users.enabled=true
session.tracker.memory.enabled=true
```

4. Save the file.
5. Restart Unified Self-Service services.
   Web notification is enabled.

Configure Email Notification for Default Tenant

OOTB, the email notification is enabled in Unified Self-Service, but, you are required to configure it for a default tenant.

Note: This action is not required for a newly onboarded tenant.

Follow these steps:

1. Log in to the Unified Self-Service control panel as the administrator.
   Example: http://<*Unified_Self_Service_Server_Name*>:8686/group/control_panel
2. Select Server, Portal Instances, and click on the Web ID of the default tenant (whose virtual host is specified as the localhost).
3. Change the virtual host name to Unified Self-Service server host name and click Save.
   Email notification is configured for the default tenant.

Support Non-English and Multi-Byte Characters in Screen Name

You can enter non-english and multi-byte characters in Screen Name. By default, this feature is disabled.

Follow these steps:

1. Log in to the Unified Self-Service server.
2. Open the portal-ext.properties file located in the OSOP folder of the Unified Self-Service installation directory.

3. Set the value for the following variable:

   ```
   bypass.liferay.screenname.validation=true
   ```

4. Save the file.

5. Restart Unified Self-Service services.
   Non-english and multi-byte characters are supported in Screen Name.

Change the Debug Log Settings

The administrator can change the log level settings in Unified Self Service to debug any error and to know the flow of request in the code.

Example: If you face some error while configuring DataSource, you can increase the log level of com.ca.sfo.portlet.datasource.action.ViewAction class.

com.ca.sfo.portlet.datasource.action.ViewAction is the Struts Action class, which gets the code to fulfill the web request.

Follow these steps:

1. Log in to the Unified Self Service control panel as the administrator.
   Example: http://*Unified_Self_Service_Server_Name*:8686/group/control_panel

2. Click Server Administration from the left pane.

3. To view the present log levels for each package, select the Log Levels tab.

4. To debug any error and to know the flow of request, change the level to Debug.
   You can find the log file (liferay.<date>.log) located in the OSOP folder of the Unified Self Service installation directory.

Add a New Category

Add a new category (package or class) to mention the log levels.

Follow these steps:

1. Click Add Category under the Log Levels tab.
   You can change the default log level from Debug, if necessary.

2. Enter package name and click Save.
   Example: com.ca
   Changes that are made to the log level take effect immediately. You need not re-start the server.

For any issues with DataSource configuration or Request creation, check the related data source logs.

Modify Unified Self-Service

You can change any of the following settings:

- Tomcat Settings
- Database Settings
- Administrator Settings
- Mail Server Settings

Important! Before you modify Unified Self-Service, ensure that you install JRE 1.7.51 or higher and set JAVA_HOME to the JRE path. Ensure to add JAVA_HOME in the Environment PATH variable.

Follow these steps:

1. Depending on your operating system, perform one of the following steps:
   - (Windows) Click Start, All Programs, CA, Unified Self-Service, Change Unified Self-Service Installation for Windows.
   - (LINUX) Navigate to the install directory, run Change Unified Self-Service Installation, select Modify Unified Self-Service Settings.
     The Manage Instances page opens.
2. Select Modify an Existing Instance and click OK.
3. Follow the on-screen instructions to modify the settings.

Configure Organization Name and Logo

You can customize Unified Self-Service to reflect the name and logo of your organization. Use the Unified Self Service Web client, Settings, Customization and set the following options:

- **HEADER LOGO**
  The logo appears in the banner area, next to the product name.

  Note: Use a transparent background for the logo, or match the color of the header background.

- **FAVICON**
  The favicon is the small icon displayed in the browser address bar and in bookmark lists.

Important! For supported IE browsers, use only .ico file, and select an icon that is of equal height and width.

- **COMPANY NAME**
  The company name appears on the browser title bar and tabs, and in bookmark lists.

Apply the Unified Self-Service Theme to the User Interface

Unified Self-Service has a new and improved user interface. If you are installing Unified Self-Service for the first time, the new user interface theme is automatically applied.

If you are upgrading from CA Open Space 2.0, 2.0 SP1, or 3.0, the Unified Self-Service user interface prompts you to apply the theme changes. However, if you do not see a prompt message on the user interface, you can apply the theme manually.

Note: We recommend you to apply the new theme to the user interface to leverage all the features of Unified Self-Service.

Follow these steps:

1. Log in to Unified Self-Service control panel as an administrator.

   `http://<Unified_Self_Service_Server_Name>:<port_number>/group/control_panel`

2. Click General Topics > Site Pages.
   The Site Pages page opens.

3. Click Public Pages and click Import.
   The Import window opens.

4. Under **Import a LAR file to overwrite the selected data**, click Choose Files and select the following location:
   C:\Program Files\CA\Open Space\OSOP\data\aquila\OpenSpace-v4.0.lar

5. Under Applications, uncheck the Archived Setups check box.

6. Under Other, check the Categories check box.

7. Click Import.

8. Log out from Unified Self-Service and log in again.

9. Verify the new theme changes.

Configure Unified Self-Service to Support a New Language

For information on how to configure Unified Self-Service to support a new language, click here (https://communities.ca.com/docs/DOC-231152439).

Managing Unified Self-Service Services

This article explains how to start and stop the Unified Self-Service (USS) services.

Start the USS Services on Windows

Follow these steps:

1. Navigate to *Start*, run and type *services.msc.*
2. Locate the service name: *CA Unified Self Service Server*
3. Right-click on the service and click **Start** to start the USS services.

Start the USS Services on Linux

Follow these steps:

1. Navigate to the *$US4SM* folder.
2. Locate the service name: *Start Unified Self-Service*
3. Execute the following command to start the USS services:

```
./Start\ Unified\ Self-Service
```

Stop the USS Services on Windows

Follow these steps:

1. Navigate to *Start*, run and type *services.msc.*
2. Locate the service name: *CA Unified Self Service Server*
3. Right-click on the service and click **Stop** to stop the USS services.

Stop the USS Services on Linux

Follow these steps:

1. Navigate to the *$US4SM* folder.

2. Locate the service name: *Stop Unified Self-Service*
3. Execute the following command to stop the USS services:

```
./Stop\ Unified\ Self-Service
```

Building

CA Service Desk Manager

Modifying Web Interface (see page 1723)

Modifying Notifications and Queries (see page 1713)

Modifying CA Business Intelligence Reports (see page 1820)

Versioning System Customizations (see page 1890)

More... (see page 1706)

CA Service Catalog

Modifying Catalog Content (see page 1994)

Modifying Branding (see page 2020)

Using Web Services to Automate Business Processes (see page 2033)

Adding Custom Fields to the Interface (see page 2002)

More... (see page 1994)

Building CA Service Desk Manager

CA SDM lets you fulfill various IT Service Management functions. The product provides a broad feature set, and various best-practice content to help meet your service management needs.

The default implementation of CA SDM closely matches the processes and terminology that is used in most IT organizations. You can extend CA Service Desk Manager to work with the unique aspects of your organization. The product includes the following spectrum of approaches to build the product to meet your unique needs:

- End-user personalization
- System-wide configuration
- Tool-based adaptation
- Code-level modifications

This section contains the following articles:

Modify Notification Methods

This article contains the following topics:

The CA SDM automatic notification methods notify personnel at key points in the service desk management process. The standard notification methods are shown as follows:

- Email
- Notification (Log)
- Pager_Email

You can define modified notification methods to specify new methods of transmission. For example, voice mail, display boards, or a specific printer. You can also access data from another application and include it in the notification message.

The Notification Process

Ticket notifications (applicable to issues, change orders, and requests) are processed when the ticket is saved:

- If the notification method is other than Notification, such as Email, the notification processor executes the notification method for each contact in the list. This method is typically an executable or shell script, which is launched in a new process. Details about the notification are stored in environment variables for easy access by the executable/script.

- For each notification requested, the notification processor sets the NX_NTF_MESSAGE and NX_NTF_SUMMARY environment variables using the Notification Message Title and Notification Message Body information that is provided on the Message Template notebook page of the Activity Notifications Detail window. If the recipient is a valid contact, other environment variables are created using information in their Contact Detail record.

- If the Write To File option is selected for the notification, a text file is created. The text file indicates that the notification method can use to obtain more detailed information.

- A list of contacts to receive the notification is built from the information that is provided on the Objects, Contacts, Types, and Survey notebook pages of the Activity Notifications Detail window. For those having a notification method matching the Notify Level and the log_all_notify Options Manager option that is installed, a notification is generated first to the notification log.

Notification Method Variables

Two sets of variables are created and made available to the notification method.

Basic Environment Variables

The first set of variables is created for every notification that is sent, independent of whether you select the Write To File option for the notification. They are written to the environment as environment variables that the notification method can access in the standard way.

The following environment variables give you basic information about the notification. They are always defined, even if the corresponding value is empty:

Environment Variable	Description
NX_NTF_MESSAGE	The completed message template text, including full expansion of all variables
NX_NTF_SUMMARY	The completed message template header, including full expansion of all variables
NX_NTF_URGENCY	The notification urgency (1 is low, 4 is emergency)

The following environment variables are created only if the recipient is a valid CA SDM contact. The variables are set using values from the Contact Detail record of the recipient as shown in the following table:

Variable	**Contact Detail Window Fields**
NX_NTF_BEEPER_PHONE	Pager Number
NX_NTF_COMBO_NAME	Last Name, First Name, Middle Name
NX_NTF_CONTACT	Contact ID
NX_NTF_EMAIL_ADDRESS	Email or Pager Email Address (depending on notification type)

Variable	Contact Detail Window Fields
NX_NTF_FAX_PHONE	Fax Number
NX_NTF_PUBLIC_PHONE	Phone Number
NX_NTF_USERID	User ID
NX_NTF_VOICE_PHONE	Alt. Phone #

Note: These variables are not created if the corresponding values are empty (except for NX_NTF_CONTACT, which cannot be empty).

Attribute Variables

The second set of variables is available only if you select the Write To File option when you define the notification method. The following attributes are called attribute variables and are written to the notification file only -- not to the environment. They are of the form:

NX_NTF_attribute[**.**secondary_attribute]=value

- ***attribute***
  The name of the attribute whose value you want to obtain. This value is the attribute name as defined for the object. For a complete list of all attribute names for any object, see CA Service Desk Manager Reference Commands (see page 3496). The most common objects that are associated with notifications are the ticket, which has an object name dependent of the type of ticket (for example, cr for requests), and the contact identifying the recipient, which has an object name of cnt. For example, the environment variable for the description attribute of a ticket can look as follows in the notification file:

  NX_NTF_DESCRIPTION=<sample description>

- ***secondary_attribute***
  If the first *attribute* is an internal identifier for another object, a secondary attribute is attached to give more meaningful information using the dot notation. In database terms, attribute is a foreign key that points to a row in another table, rather than a simple data value. Using this raw key value would probably have little meaning. Many of these types of fields are resolved or de-referenced for you. The secondary_attribute is the value in the referenced table. For example, instead of writing the value for the assignee attribute, which is stored as the unique ID of the contact record for the assignee, the assignee's combined name is the combo_name attribute for the contact object, as shown in the following example:
  NX_NTF_ASSIGNEE.COMBO_NAME=Armstrong, Beth
  If an attribute does not have a value, the corresponding value is usually (NULL) or blank. For example:
  NX_NTF_CALL_BACK_DATE=(NULL)
  NX_NTF_GROUP.COMBO_NAME=

Note: An attribute variable that exists for both the ticket and the recipient is NX_NTF_ID (the id attribute), which is the unique database ID for the object.

The Notification File

If you select the Write To File option when you define a notification method, all the basic environment and attribute variables are written to a text file. This file is closed before executing the notification method script or program. This notification file is updated every time the notification method is invoked for a contact. This method is a handy mechanism for passing relevant information to the notification script that is not otherwise available in the environment.

The full path of the notification file is set in the NX_NTF_FILENAME environment variable, which is available to the notification method . The file name is also added to the end of value you enter in the Notification Method field when defining the notification method. For example, if the Notification Method is 'pdm_perl - w mymethod.pl', then the actual process executes 'pdm_perl - w mymethod.pl *unique_notification_file_name*'.

Important! The administrator can clean up the notification files. This clean-up is especially important for a site using a high volume of notifications. The files are located in the standard temporary directory (TEMP on Windows and TMP on UNIX). One suggestion is to delete the file at the end of the notification method script/program.

The notification file is a standard text file that is divided into sections. Each line contains either an attribute/value pair or a section marker. Each notification file has three sections. All sections begin with "-----" followed by a new line.

- **SECTION=obj**, where obj identifies the object type of the ticket
  - **Iss**
    Provides information about the issue.
  - **Chg**
    Provides information about the change order.
  - **Cr**
    Provides information about the request.
- **SECTION=cnt**
  Provides information about the recipient.
- **SECTION=notification**
  Provides the same information that is available from the basic environment variables.

Note: The section names for the ticket and recipient are actually the object names for the attributes in that section. For a complete list of all attribute names for any object, see the CA Service Desk Manager Reference Commands (see page 3496) section.

Several lines of attribute/value pairs, each of which represents an attribute of the corresponding object, are contained in each section. The Attribute Variables in this section provide the detailed information about how these lines are formatted and what they mean.

Line breaks in an attribute value are reproduced as new lines in the notification file. Your notification method process can only use the attribute or value lines that begin with NX_NTF, and section markers. Generate a sample file and look at its contents before working with a notification file in your notification method process.

Using Perl Scripts

Most notification methods invoke an executable or shell script to read the environment variables and send the message. This action works well on most UNIX servers, but difficulties arise reading the environment variables on a Windows server.

You can use a Perl script to overcome environment problems on Windows. CA SDM includes a ready-to-use installation of the Perl interpreter named pdm_perl. Any Perl script that is invoked with pdm_perl as a notification method can reliably obtain the environment variables. The Perl script can read and format the environment variable values. The script can also carry on with the rest of the notification, such as invoking a pager or sending an email.

For Windows-based servers, consider using the launchit utility. You can invoke your scripts or programs in a shell environment with the proper environment variables set.

For example, suppose that you write a Perl script that is named read_env.pl to read several of the environment variables. You can invoke this script for a notification by entering the following command in the Notification Method field on the Notification Method Detail window:

pdm_perl *script_path*/read_env.pl

This notification method starts the Perl interpreter and executes the instructions in read_env.pl script.

Create a Notification Method

Follow these steps:

1. Create a script to process the message template and transmit it to the recipient. The script can be any executable, depending on the platform. Third-party or public domain interpreters can also be used. Typically, Bourne shell scripts are used on UNIX and .bat files are used on Windows. If your script requires a special template, create it.

2. Add the new notification method to your site using the web interface.

Create a Script

You can create a notification method script.

Follow these steps:

1. Determine how you want the notification to be delivered (for example, printed on a particular printer).

2. Determine the contents of the notification message.
3. Specify what information from the message template to include in the notification.
4. Set up a script to transmit the notification.
5. Place the script in an executable file in the path of the CA SDM server.

Add the Notification Method

After you create a script, define the new notification method to CA SDM. You can use *one* of the following methods to add a notification method:

- Using the web interface
- Using a UNIX shell script

Add a Notification Method Using the Web Interface

Use the web interface to add a notification method (see page 834).

Add a Notification Method Using a UNIX Shell Script

The following steps create a notification method shell script that sends the notification message to the service desk printer, SDPR2. In this example, the notification message consists of the message header and the message text from the message template:

1. Set up the shell script to assemble the notification text and transmit it, as follows:

```
#!/bin/sh
echo "
TO:       $NX_NTF_USERID
SUBJECT:  $NX_NTF_SUMMARY
MESSAGE:
$NX_NTF_MESSAGE" |lp -dSDPR2
```

2. Name the executable file sd_print. Place it in any directory that is used for common scripts at your site, such as /usr/local/netbin.
3. Make the shell script an executable file using chmod.
4. Select Notification Methods from Notifications on the Administration Interface.
5. Select New from the File menu.
6. Enter data in these fields:
   - **Symbol**
     SDPR2
   - **Description**
     Send backup notification to service desk printer SDPR2

- **Notification Method**
  /usr/local/netbin/sd_print

7. Click the Save button to save the new record. Then click Close Window to close the detail window.

Query and Message Modifications

CA SDM provides a number of features that let you narrow the focus of information so you can concentrate on requests, change orders, and issues that apply to your immediate situation. One of these functions stores queries that you can use to see relevant information on the scoreboard of the administrative or web interface. Another lets you modify the messages that notify key personnel of ticket activities.

Stored queries can provide a focus on tickets related to the logged-in user and modify the counter fields in the scoreboard area of the administrative and web interfaces. You can modify activity notification messages to include attributes from the activity log object and information on specific tickets.

Activity Notification Messages Modifications

This article contains the following topics:

Notification messages can be sent automatically when request activities occur.

Note: For information about notification messages and instructions for defining activity notifications, see the Activity Notification Messages Modifications (see page 1713) section.

Two of the fields that must be defined on the Activity Notifications Detail window are Notification Message Title and Notification Message Body. Both of these fields can contain attributes from the activity log object (alg for Requests/Incidents/Problems, chgalg for Change Orders and issalg for Issues. These three activity log objects are almost identical) and can identify the specific request related to the activity.

Formatting Attributes for Activity Notifications

Optional formatting and escaping of individual attributes can be achieved using the properties listed below. This can be useful especially if formatting HTML notification where the data in the attribute may need to be escaped to conform to HTML standards.

To include formatting, use the following syntax:

```
@{property=value property=value:attribute_name}
```

Property values pairs are separated by at least one space and are not case sensitive. A colon separates the formatting properties from the attribute name. If no properties are listed, no formatting or escaping will be done on attribute.

The following table the available formatting properties:

Property	Description
DATE_FMT	Specifies the date format for attribute. Valid values are: MM/DD/YYYY MM-DD-YYYY DD/MM/YYYY DD-MM-YYYY YYYY/MM/DD YYYY-MM-DD Valid only for Date attributes. Dates embedded in strings are not affected.
ESC_STYLE=NONE | HTML | URL	Specifies the escape type of the formatted text. Valid values are: **NONE** Default setting. Specifies that no special treatment be given to any character in the content body. **HTML** Give special treatment to the following characters, which are meaningful in HTML text: & becomes & ”_becomes " < becomes < > becomes %gt; **URL** Translate all characters other than letters, digits, and '@*-_.#' to '%xx', where xx is the hexadecimal coding of the translated character.
JUSTIFY=LEFT | CENTER | RIGHT | TRUNCATE| WRAP | LINE	Specifies the justification of the formatted text. Valid values include: **TRUNCATE** (default if formatting) Truncates text to WIDTH property value if a positive integer. If ESC_STYLE=HTML, eliminates HTML formatting by replacing '<' and '>' with < and > (see KEEPLINKS and KEEPTAGS). **LEFT|CENTER|RIGHT** Produces exactly WIDTH characters, truncated or padded with spaces as necessary, with any embedded new lines replaced by a single space. If ESC_STYLE=HTML, the output text is delimited by [set the pre variable for your book] and </pre> tags. The WIDTH argument must be specified as a positive integer. **WRAP** Same as LEFT, except that text wrapping honors word boundaries (line breaks are not placed within words). **LINE** Same as TRUNCATE, except that it also replaces all embedded line breaks with tags if ESC_STYLE=HTML.
KEEPLINKS=YES|NO	If KEEPLINKS=YES is specified, the action of JUSTIFY=LINE or JUSTIFY=TRUNCATE is modified to preserve HTML anchor tags (Action:) while converting all other '<' and '>' characters. Mutually exclusive with KEEPTAGS. Only valid if ESC_STYLE=HTML.
KEEPNL=YES|NO	The normal action of PDM_FMT is to convert all embedded new lines and any following spaces to a single space. If KEEPNL=YES is specified, embedded new lines are preserved. This argument is ignored for JUSTIFY=LINE.

Property	Description
KEEPTAGS=YES|NO	If KEEPTAGS=YES is specified, the action of JUSTIFY=LINE or JUSTIFY=TRUNCATE is modified to preserve all HTML tags. Mutually exclusive with KEEPLINKS. Only valid if ESC_STYLE=HTML.
PAD=YES|NO	If PAD=NO is specified, PDM_FMT does not convert empty strings to a single space. This is the normal action when WIDTH is non-zero, or JUSTIFY is TRUNCATE or WRAP.
WIDTH=*nn*	When non-zero, specifies that the text should be formatted to exactly WIDTH characters.

For example, to format the Request description for an HTML notification by escaping HTML specific characters, adding
 tags for line breaks and keeping any HTML Links as links, enter the following:

```
@{ESC_STYLE=HTML JUSTIFY=LINE KEEPLINKS=YES:call_req_id.description}
```

To format the open_date of a Request to European format, enter the following:

```
@{DATE_FMT=DD-MM-YYYY:call_req_id.open_date}
```

Attributes from the Activity Log Object

To include an attribute from the activity log object, include this in the Notification Message Title or Notification Message Body field:

```
@{att_name}
```

The name of the object, alg or chgalg or issalg, is the default and need not be specified. For example, to include the type of activity in the message title, enter this in the Notification Message Title field (along with the rest of what you want in the title):

```
@{type}
```

To include the description of the activity in the message body, enter this in the Notification Message Body field (along with the rest of what you want in the body):

```
@{description}
```

Information on Specific Change Orders

For messages to provide information on the specific change order that triggered the notification, the Notification Message Title or Notification Message Body fields must contain an attribute in the activity log object that references the change order object. Enter the reference in this format:

```
@{change_id.chg_att_name}
```

In this reference, the following information applies:

- **@**
  Indicates to replace this expression.
- **change_id**
  The attribute in the activity log object that links it to a specific instantiation of the change order object (chg).

- ***chg_att_name***
  Any attribute in the chg object.

For example, to include the priority of the change order in the message title, enter the following in the Notification Message Title field, along with the rest of what you want in the title:

```
@{change_id.priority.sym}
```

To identify who reported the change order (Affected End User) in the message body, enter the following in the Notification Message Body field, along with the rest of what you want in the body:

```
@{change_id.requestor.combo_name}
```

If you want to reopen a specific change order by number, and want the message to appear as follows, use the following syntax:

```
Reopen Change Order @{change_id.chg_ref_num}
```

Note: For messages to provide information about an issue that triggered a notification, the Notification Message Title or Notification Message Body fields must contain an attribute in the activity log object that references the issue object, iss. For more information about objects and attributes, see the CA Service Desk Manager Reference Commands (see page 3496) section.

For example, to include the priority of the issue in the message title, enter the following in the Notification Message Title field, along with the additional information you want in the title:

```
@{issue_id.priority.sym}
```

Information on Specific Requests

For messages to provide information on the specific request that triggered the notification, the Notification Message Title or Notification Message Body fields must contain an attribute in the activity log object that references the request object. Enter this reference in this format:

```
@{call_req_id.cr_att_name}
```

- **@**
  Indicates to replace this expression.

- **call_req_id**
  The attribute in the activity log object that links it to a specific instantiation of the request object (cr).

- ***cr_att_name***
  Any attribute in the cr object.

For example, to include the impact of the request in the message title, enter this in the Notification Message Title field (along with the rest of what you want in the title):

```
@{call_req_id.impact.sym}
```

To identify the affected resource in the message body, enter this in the Notification Message Body field (along with the rest of what you want in the body):

```
@{call_req_id.affected_resource.name}
```

If you want to reopen a specific request by number, and want the message to appear as follows, use the following syntax:

```
Reopen Request @{call_req_id.ref_num}
```

There are several other mechanisms by which messages can be sent which are in the context of the request itself (or change order or issue). When the context is the request itself, you do not need (and cannot use) the "call_req_id" part of the reference. So, in these cases, you need to use:

```
"@{ref_num}" rather than "@{call_req_id.ref_num}"
```

ITIL-Specific Queries

Problems and Incidents are requests with one of two values in the *type* attribute: “I” for Incidents or “P” for Problems.

The following stored query obtains all Incidents in which the Assignee's Organization or the Group's Organization equals the logged-in Analysts Organization:

```
assignee.organization IN @cnt.organization OR group.organization IN @cnt.
organization) AND active = 1 AND type = \'I\'
```

For Problems, the query is identical except for type = \'P\'

Scoreboard Queries

This article contains the following topics:

One of the tables in the database, Cr_Stored_Queries, defines stored queries. These stored queries, which are similar to SQL queries, can be used to customize the counter fields on nodes in the scoreboard area of the administrative and web interfaces. The counter fields tell how many records match the query. For example, they can tell how many of various types of requests have been assigned to the logged-in user.

Each user can customize the counter fields that appear on his or her scoreboard (this is explained in the online help.) However, the system administrator must first define the various types of requests that can be counted in these counter fields as stored queries.

Note: Scoreboard counts will be incorrect if database query values are equal to NULL. For example, if your Scoreboard query specifies that assignee.organization = xyz, and an assignee field is blank (NULL) for a record, then that record will not be part of the Scoreboard count.

Stored Queries for Logged in User

Two of the fields that must be defined on the Stored Query Detail window are Where Clause and Label. Both of these fields can contain expressions that are customized to the logged-in user. Stored queries refer to objects and attributes, rather than to table names and columns. A stored query that is customized to the logged-in user consists of two parts, as follows:

- **The object (such as cr for a request)**
  This is usually specified on the left of the equal (=) sign. The syntax for this part of the stored query is:

```
att_name[.att_name...].SREL_att_name
```

A stored query always has a Type, which is an object name that the query is executed against and provides context for the query. In the syntax above, the first att_name must be an attribute name of the context object.

- **The logged-in user (the instance of the cnt object for this user)**
  This must be specified on the right of the equal (=) sign if the tickets are to be selected based on an attribute of the logged-in user. The syntax for this part of the stored query is:
  @att_name[.*att_name*...].*SREL_att_name*

Note: For more information about objects and attributes, see the CA Service Desk Manager Reference Commands (see page 3496) section.

Syntax for cr Object

Use this syntax if the reference is to the request (cr) object:

```
att_name[.att_name...].SREL_att_name
```

This example identifies the location of the person assigned to handle a ticket. In this example, the object name is omitted, as the type of the Stored Query implies the cr object:

```
assignee.location=@cnt.location AND active=1
```

- **assignee**
  The attribute in the request object that maps to the assignee field in the corresponding table. For example, the assignee attribute is defined in the cr object with SREL agt, which means it refers to the agt factory. The agt factory is part of the cnt object definition.

- **location**
  The attribute in the cnt object that maps to the c_l_id field in the Contact table. The location attribute is defined in the cnt object with SREL loc, which means it refers to the loc object.

WHERE Clause

The following example demonstrates a value you can code in a WHERE clause:

```
assignee.location=@cnt.location AND active=1
```

Given the Stored Queries type is a Request, this query selects all active requests where the assignee's location is the same as the location of the logged-in user.

Label

Attributes in the cnt object can be included in labels the same way they are included in WHERE clauses. Here is an example of the use of an attribute in the cnt object in a label:

```
@cnt.location.name Calls
```

This label will include the name of a location, for example, Phoenix, where Phoenix is substituted for @cnt.location.name when the label is displayed on a window. The label will be displayed as Phoenix Calls.

The IN Keyword

The IN keyword allows a stored query to reference two (or more) tables without creating a join. This can result in significant efficiency in executing the query. It is coded as follows:

```
SREL_att_name IN ( value1 [, value2 [,...]] )
```

For example, a request query could be coded as:

```
category.sym IN (\'Soft%\', \'Email\')
```

This results in the following SQL WHERE clause:

```
category IN (SELECT persid FROM prob_ctg WHERE sym LIKE 'Soft%' OR sym = 'Email')
```

One use of IN is to avoid Cartesian products. For example, the following query results in a Cartesian product and is very inefficient:

```
assignee.last_name LIKE 'MIS%' OR group.last_name LIKE 'MIS%'
```

By using IN, the query does not create a Cartesian product; in fact, it creates no joins at all, as illustrated by the following example:

```
assignee.last_name IN 'MIS%' OR group.last_name IN 'MIS%'
```

Note: The parentheses that normally enclose the list of values on the right side of IN can be omitted if there is only one value in the list. Similarly, you should avoid joins in data partitions by converting a data partition, illustrated as follows:

```
assignee.last_name LIKE 'Smith'
to:
assignee = U'374683AA82ACE34AB999A042F3A0BA2E'
```

where:

- **U**
  indicates that the value is a uuid.
- **'374683AA82ACE34AB999A042F3A0BA2E'**
  The 32 characters in single quotes indicates the string representation of an actual uuid.

This avoids the join with some loss in clarity. Using IN, the same partition can be written as illustrated in the next example, with the clarity of the first version and almost the same efficiency as the second version:

```
assignee.last_name IN 'Smith'
```

CA SDM supports the IN clause applied to QREL or BREL lists. For example, if you want to find all the Requests with Assets that are parents of another specific Asset (with id 374683AA82ACE34AB999A042F3A0BA2E), the appropriate where clause is as follows:

affected_resource.[parent]child_hier.child IN (U’374683AA82ACE34AB999A042F3A0BA2E’)

The first part of the clause, *affected_resource*, is an SREL (foreign key) of the cr (Request) object, pointing to the Network_Resource table. The *child_hier* portion is a list of hier objects pointing to the hierarchical relationships. The last part, *child*, forms the first part of the where clause for the IN sub query. The *374683AA82ACE34AB999A042F3A0BA2E* portion is the foreign key value to match on *child* . *[parent]*specifies thesub query return. Since the id value is a string representation of a UUID it must be indicated as such and written as U’374683AA82ACE34AB999A042F3A0BA2E’

The following is an example of the actual SQL generated, which provides all the Requests where the Asset is a parent of a specific Asset:

```
SELECT Call_Req.id FROM Call_Req WHERE Call_Req.affected_rc IN (SELECT hier_parent
FROM Asset_Assignment WHERE hier_child = U'374683AA82ACE34AB999A042F3A0BA2E')
```

To query on multiple parents, you can provide a comma-separated list in the () portion of the SQL, as shown by the following example:

```
affected_resource.[parent]child_hier.child IN (U'374683AA82ACE34AB999A042F3A0BA2E',
U'374683AA82ACE34AB999A042F3A0BA2E')
```

The attribute name in brackets ([]) is used to form the SELECT portion of the sub-clause. Bracket notation is not used for the group Stored Queries shipped with CA Service Desk Manager Version 6.0, as illustrated in this example:

```
(assignee = @cnt.id OR group.group_list.member IN (@cnt.id)) AND active = 1
```

Note: If bracket notation is not used, the SQL subsystem assumes that it is the attribute name of the first symbol in the dot-notation portion. It works in this case, more out of luck, that the group_list object has an attribute named ‘group’ in it. If it were named anything else, the where clause would fail to parse! The equivalent clause with brackets illustrated as follows:

```
(assignee = @cnt.id OR group.[group]group_list.member IN (@cnt.id)) AND active = 1
```

Note: You cannot extend the dot notation. For example, the following does not work:

```
affected_resource.[parent]child_hier.child.name IN ('chicago1')
```

Query Based on Priority

In the database, the Priority table has two columns named sym and enum. The value the users see are the sym values. But the application sees the sym based on the enum values. At present, the default sym values 1 to 5 are reversed in their enum value.

Example

Sym	Enum
1	5
2	4
3	3
4	2
5	1

Therefore, when writing the stored query, when you reference a value of 5, you are actually looking for priority 1 unless you use a .sym to specify which attribute to look at.

Important! Do not change the default enum values the product assigns. Instead, when adding new sym values, just continue from the highest enum value and so on.

Time-Based Queries

Time spans can be used to create time-based stored queries. A time span specifies a period of time, which can be relative to the current date. For example, a time span could refer to today, yesterday, last week, or last month. A time span has a name, such as TODAY or YESTERDAY. You refer to a time span in a stored query by using either of two built-in functions, as follows:

- **StartAtTime (*timespan-name*)**
  This refers to the beginning of the period described by the time span.

- **EndAtTime (timespan-name)**
  This refers to the end of the period described by the time span.

The syntax rules for stored queries require that the time span name be enclosed in single quotes, with each single quote preceded by a backslash. For example, to refer to the beginning of last week, you would specify:

```
StartAtTime(\'PAST_WEEK\')
```

The passage of time makes it necessary to periodically refresh a stored query containing a reference to a time span. For example, the interval described by “yesterday” changes at midnight. You specify the Start Time, End Time, and Trigger Time for refreshes in the Timespan Detail window.

Start Time

Start Time specifies the beginning of the time span in absolute or relative terms. The following table describes the fields within the Start Time section of the Timespan Detail window:

- **Year**
  An explicit year, such as 2000, or a relative year, such as +1 (next year) or - 1 (last year)

- **Month**
  An explicit month from 1 (January) to 12 (December), or a relative month, such as +1 (next month) or - 1 (last month)

- **Day**
  An explicit day from 1 to 31, or a relative day, such as +1 (tomorrow) or - 1 (yesterday)

- **Hour**
  An explicit hour from 0 to 24, or a relative hour, such as +1 (next hour) or - 1 (last hour)

- **Minute**
  An explicit minute from 0 to 59, or a relative minute, such as +1 or - 1

End Time

End Time specifies the end of the time span in absolute or relative terms. The End Time fields of the Timespan Detail window are the same as the Start Time (see page 1722) fields of the Timespan Detail window.

Trigger Time

The Trigger Time field specifies when the WHERE clause of a stored query containing a reference to the time span is recreated and the stored query refreshed. Trigger Time must be relative to the current time as described in the following table:

- **Year**
  Must be a relative year from - 1 (last year) to +36 (36 years from now).
- **Month**
  Must be a relative month from - 1 (last month) to +11 (11 months from now).
- **Day**
  Must be a relative day from - 1 (yesterday) to +31 (31 days from now).
- **Hour**
  Must be a relative hour from - 1 (last hour) to +23 (23 hours from now).
- **Minute**
  Must be a relative minutes from +9 (9 minutes from now) to +59 (59 minutes from now).

Web Interface Modifications

Contents

The CA SDM web interface(also referred to as the browser interface) provides you with CA SDM functionality through the Internet. This functionality includes the ability to open, update, or close tickets, display and post announcements, and access supporting data tables. It enables independent browsing of the knowledge base to help reduce the number of calls to the service desk and speeding resolution times. The web interface can be fully customized and can be used with many web browsers.

If you installed and configured the web interface, you can integrate it into your existing web interface and customize it to suit your needs. For customization, be familiar with HTML and the web browser in use at your site.

Note: WSP Design view works for CA SDM controls (PDM_MACROs). When working on forms that do not contain CA SDM controls, you can only work on the Source tab. The Employee and Customer web forms do not contain CA SDM controls and therefore appear on the Source tab rather than the Design tab. Some Analyst forms do not contain CA SDM controls, and therefore would appear on the Source tab too.

Important! CA SDM no longer uses any customized .mac files for pdm_macro in the NX_ROOT\site\mods\www\macro directory. You cannot customize macros.

Important! Technical support cannot provide assistance with design or debugging of customizations (including documentation, such as online help systems). We provide general information for customizing the CA SDM web interface. When doing so, be aware that you are solely responsible for your own customizations. CA SDM technical support can assist you in interpreting and understanding customization.

Support for the customization techniques here extends to helping ensure that the techniques and facilities perform as documented. Be careful not to exploit undocumented features or to extend documented features beyond their documented capabilities. Such exploitation is not supported and can result in system problems or instability that may appear unrelated to the customization. For this reason, support may ask you to remove customizations to reproduce the problems. Sites should prepare for this eventuality by carefully following the guidelines on placing all modifications in the site mods directory tree and maintaining change logs. Sites that make frequent, complex, or extensive changes should consider approaching CA SDM customization as a software engineering project with disciplined source control, testing, and controlled releases to production.

Migrating customizations between releases can present unique challenges, and we have developed the product in ways to preserve the efforts put into customization. In addition, if Level Two support supplies a patch to a system, the patch is written with these same assumptions. Patching or upgrading a system with undisciplined customizations is a risky undertaking that often results in costly system down time. Avoid it by following these guidelines and practising sound software engineering principles.

Modify the Scoreboard

The Scoreboard on this tab allows you to view the requests, change orders, issues, call backs, and tasks assigned to you or your group. You can customize your Scoreboard to display only specific folders and nodes. By default, the Scoreboard displays nodes that itemize the records for the entire application. These records can include requests, issues, change orders, assets, configuration items, callbacks, documents, and tasks.

Follow these steps:

1. Select File, Customize Scoreboard.

   The Customize Scoreboard window opens.

2. Select the Scoreboard you want to customize from the following options:

   UserDisplays the Scoreboard for the username under which you are logged in. RoleAllows you to customize the Scoreboard for all members of one type of user, such as administrators. Select a value from the drop-down list.

3. Navigate the Scoreboard tree and select an item to work with.

To update or delete an item, select the item. To add a new node or folder, select the item after which you want to add the new item.

Note: The Add Node and Add New Folder options are disabled when the system reaches the Scoreboard limit. To add more nodes or folders, you can remove them or ask your administrator to use Options Manager to increase the scoreboard_entry_limit.

4. Complete the entry fields for the task you want to complete. Depending on the task, you can edit the following fields:

   Node LabelDisplays the name of the node that you want to add or update.Node's Stored QueryShows the stored query of the node that you want to add or update. Enter a value directly or select the Node's Stored Query link to search for a stored query.Folder LabelDisplays the name of the folder that you want to add.

5. Click the button for the task you want to complete.

   The Scoreboard tree refreshes to display your changes.

6. (Optional) Click Reset Tree to undo your changes to the Scoreboard tree.

7. Click Finished.

   The Customize Scoreboard window closes and the Scoreboard displays your changes.

Set Preferences

Setting preferences allows you to define the desired default behaviors.

Follow these steps:

1. Choose View, Preferences in CA SDM Web UI.

   The Preferences window appears.

2. Set the appropriate preferences
   For example, select the Using Screen Reader option.

   Note: For more information about using a screen reader with CA SDM, click Help, Screen Reader Usage.

3. Click Save to save the preferences. The new settings take effect immediately.

Preferences Fields

General Settings

- **Avoid Popups**
  Opens new forms in the main browser window whenever possible, reducing the number of popups.Note: If this option is selected, the Back to List button is activated and is used to navigate from detail forms back to the previously displayed list window. The Back to List button appears in the upper right-hand side of the window.

- **Display Score Count**
  Displays the score count as left-justified.Keep Log Reader WindowKeeps the Log Reader window open when you close all popups, and when you log off. This setting has no effect when the Log Reader window is not open.

- **Preserve Popup Size**

  Causes new popup windows to open with the same dimensions as the most recently resized popup window. The popup size that is preserved is dependent on the window size used by that type of popup (Large, Medium, Small, or Xsmall). For example, if you resize a Large popup, such as a Request detail page, the new size is preserved for all Large popups. If you resize a Medium popup, such as an activity log page, the new size is preserved for all Medium popups.Note: If you maximize a popup window, subsequent popup windows may cover any other window you have open. However, new popup windows appear slightly off the screen, to the right and lower. This is because there is a 10 pixel (left and top) offset for popups to prevent them from completely overlaying the currently displayed window. We recommended that you do not maximize popup windows when using this option.

- **Mouseover Menus**

  Causes a menu to display when the mouse pointer is over the menu's link, without clicking the mouse button. You must reload any active forms for this setting to take effect on the page.

- **Using Screen Reader**

  Modifies system behavior for optimal use with a screen reader for blind and limited vision users. You must log off and log back on for this change to take effect. From the Help menu, select Screen Reader Usage for an overview of using CA SDM with a screen reader.Use Default RoleUses the default role assigned to a Contact or a Contact's Access Type as the initial role when the Contact logs in.

- **Disable Mouseover Previews**

  Select this check box if you do not want to see preview forms pop up automatically.Note: Mouse-over previews are disabled automatically when either Using Screen Reader or Mouseover Menus is enabled.

Support Automation Analyst UI Localization

English is the default language.

Knowledge Search Document Settings

- **Search Type**

  Select either Keyword Search or Natural Language Search.

- **Match Type**

  Select the default method to use for text matching during a search. Possible values are Any of the Words (OR), All of the Words (AND), and Exact Phrase.

  Important! Match Type and Match preferences only set the default search criteria when you search in Knowledge Management. For example, you log in as an analyst and click the Knowledge tab of any ticket. Knowledge searches from within a ticket always default to Match Type=Any of the words (OR) and Match=Whole Words, regardless of your preference settings.

- **Match**

  Select the default method by which CA SDM searches documents, either Whole Words or Words Beginning With.

- **Order By**

  Select the default property for sorting retrieved documents.

- **Search In**

  Select the document fields where you want to search for specified keywords. These options only display when Keyword Search is the selected search type.

Knowledge Document List Settings

- **Documents Per Page**
  The number of documents (10, 25, or 50) that the product that display on each page of the Knowledge Document List pane.

- **Show Document List Details**
  If selected, the Knowledge Document List pane on the Knowledge tab includes the following detailed information:
  Title
  Summary
  Document ID
  Modify Date
  If not, only the document title displays.

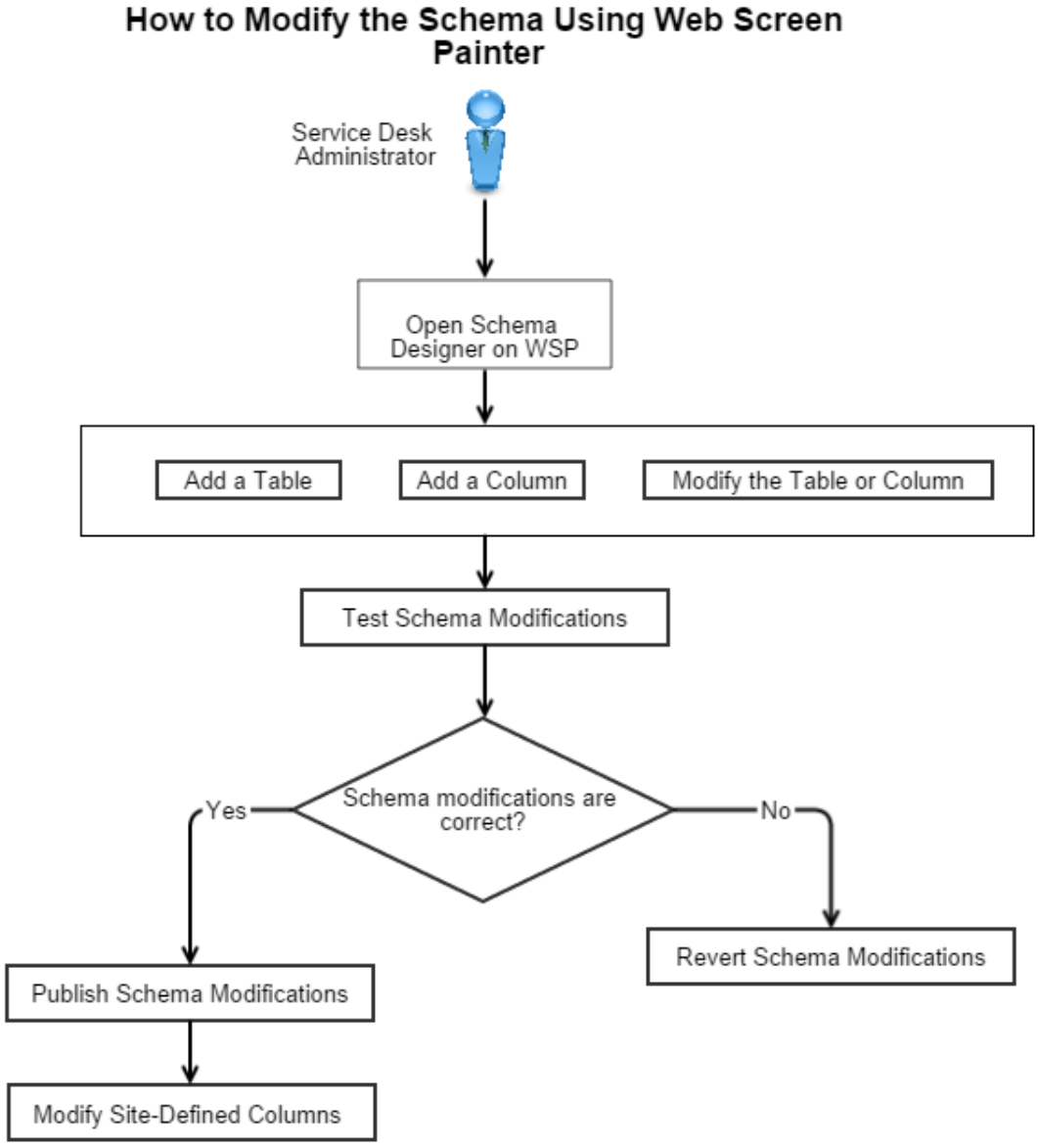
Knowledge Categories Document List Settings

- **Documents Per Page**
  The number of documents (10, 25, or 50) that the product that display on each page of the Knowledge Document List pane.

- **Attributes to be shown in list**
  Select the properties to be listed for each document in the Knowledge Document List pane. Select the desired attributes from the Available list and click the arrows to move them to the Selected list.

How to Modify Schema Using Web Screen Painter

Use the Schema Designer of Web Screen Painter to modify the database schema of CA SDM. Schema Designer provides a graphical user interface to review and modify this schema. The following diagram shows how to modify the schema using Web Screen Painter:



Follow these steps:

1. Verify the Web Screen Painter Considerations (see page).
2. Open Schema Designer on WSP (see page 1729).
3. Add a Table (see page 1730) or Add a Column (see page 1733) or Modify the Table or Column (see page 1738).
4. Test Schema Modifications (see page 1739).
   - If the schema modifications are correct, Publish Schema Modifications (see page 1739).
   - If the schema modifications are incorrect, Revert Schema Modifications (see page 1743).
5. (If necessary) Modify Site-Defined Columns After Publishing (see page 1744).

Verify the Web Screen Painter Considerations

Consider the following information before using Web Screen Painter:

- You cannot use WSP to change the length of an existing column, and we strongly recommend that you *do not* use other tools to do so. Changes to the length of an existing column are not supported, and may cause other applications accessing the CA SDM database to fail.

  Important! Do not shorten a field or delete an existing field, because these actions could cause CA SDM to fail.

- Be careful when adding columns to an existing table, because you can inadvertently exceed the record length capacity of the underlying database. Check the specifications for the database that you are using with CA SDM and make modifications within the limits of that database.
- Publishing changes to the database schema could require limited or considerable downtime, depending on the changes you make and the capabilities of your underlying database.
- If you are a new user of CA SDM, it is easier to make all of your changes during testing instead of waiting until you are in production.
- Review general procedures you must complete before and after changing the database schema.
- Use specific procedures to modify your schema. Most of these procedures are followed by an example of a change you might want to make to the standard database schema.

Open Schema Designer on WSP

To start working on the Schema Designer, ensure that you have WSP installed on the CA SDM server. For more information about the WSP installation, see Install Web Screen Painter (see page 498).

Follow these steps:

1. Log in to the following CA SDM server where WSP is installed, depending on your CA SDM configuration:

- Conventional: Primary server
- Advanced availability: Background server

2. Start WSP using any of the following actions, depending on the operating system that is installed on the CA SDM server:
   - (Windows) From the Start menu, select Program Files, CA, CA SDM, Web Screen Painter.
   - (UNIX) Enter the command pdm_wsp with $NX_ROOT/bin in your path.

   The Web Screen Painter login window opens.
3. Enter your login credentials.
4. Select Tools, Schema Designer.
   The Schema Designer window opens. The left side of the Schema Designer window shows the CA SDM database in a tree format. The tables and columns are displayed by their Object Name. If the Display Name differs from the Object Name of the table or column, the Display Name is displayed in parentheses along with the Object Name.

Add a Table

Use the Schema Designer to add a table in the database.

Follow these steps:

1. Select Edit, Add Table.
   The Add New Table dialog opens.
2. Enter the table name in the New Table Name field and click OK. Ensure that you begin the name of a site-defined table with the letter z to prevent conflict with possible future standard tables.
   WSP adds a z to the beginning of the table name if you do not add.
3. Complete the following fields, as appropriate:
   - **Name**
     (Read-only) Specifies the object name of the table. For example, the object name of the cr table is cr.
   - **Display Name**
     Specifies the user-friendly name of the table. For example, the Display Name of the cr table is Request. You can change the Display Name of a table by entering a new name in this field.
   - **Schema Name**
     (Read-only for standard tables) Specifies the name used to refer to the table in CA SDM utilities, such as pdm_userload. For site-defined tables, Schema Name defaults to the Object Name. You can change the Schema Name by entering a new value in this field.

- **DBMS Name**
  Specifies the name used to refer to the table in the physical DBMS. This field is read-only for all tables. For site-defined tables, it is always the same as Schema Name.

- **Default Display Field (common name)**
  Specifies the column displayed on the UI for a field that references this table. For example, the assignee field of a request is a reference to the Contact table. Because the common name of the Contact table is combo_name (last, first middle), the combo name of the referenced contact displays as assignee. You cannot change the value of common name.

- **Foreign Key Field (rel attr)**
  Specifies the column stored in the database for a field that references this table. For example, the assignee field of a request is a reference to the Contact table. Because the rel attr of the Contact table is id, the assignee column in a Request contains the id of the referenced contact. You cannot change the value of rel attr.

- **Function Group**
  Specifies the name of the group that controls the level of access that users have to records in this table. Each access type of a contact specifies whether they have read, modify, or no access to data in tables in each function group. You can change the value of rel attr by selecting a new value from the drop-down list.

Important! The Schema Designer includes an Advanced tab. Information on this tab is intended for CA Technologies Support and field representatives. You will not need to work with this tab for most uses of the Schema Designer, and it will not be discussed further in this document.

The Advanced tab of the Schema Designer column dialog shows information meaningful only to persons with internals knowledge of CA SDM. Its contents vary with the column type. We recommend that you modify the values in this tab only on direction from a CA Technologies employee. It contains the following fields if a table is selected:

- **Active Triggers**
  Enter the triggers currently active in the Object Engine for the column. A trigger is a small program that runs under the direction of the Object Engine at certain times when a column is modified. The active trigger list includes both standard and site-defined triggers (so that site-defined triggers are listed both in the active list and in the site-defined list).

- **Site-Defined Triggers**
  Enter the triggers that have been installed at your site. For example, these may be triggers that have been activated as a result of installing a CA SDM option, or triggers that have been written for your site by CA Technical Services. The active trigger list includes both standard and site-defined triggers (so that site-defined triggers are listed both in the active list and in the site-defined list).

- **LRel Specification**
  Enter the specification of a many-to-many relationship between two tables, in the form: table1 column1 <> table2 column2
  This shows that the LREL is a many-to-many relationship between table1 and table2, with virtual column column1 containing the relationship in table1, and virtual column column2 containing the relationship in table2.

- **Active xRel Query Information**
  Enter the active specification of the query that defines a BREL or QREL virtual column. The specification is in Object Engine Majic format.

- **Site-Defined xRel Query Information**
  Modify the query associated with a BREL or QREL. It is recommended that you enter data into this field only under the direction of a CA employee.

- **Active Derived Expression**
  Enter the active specification of the expression that the Object Engine uses to construct the value of a DERIVED virtual column.

- **Site-Defined xRel Query Information**
  Modify the expression associated with a DERIVED column. It is recommended that you enter data into this field only under the direction of a CA employee.

The Domsets tab of the Schema Designer Table dialog contains the following:

- **MLIST_DYNAMIC**
  A dynamic domset with no WHERE clause.

- **MLIST_STATIC**
  A static domset with no WHERE clause.

- **RLIST_DYNAMIC**
  A dynamic domset with a WHERE clause defined in the STANDARD_LISTS section of the FACTORY statement.

- **RLIST_STATIC**
  A static domset with a WHERE clause defined in the STANDARD_LISTS section of the FACTORY statement.

If you double-click one of the Domsets, the Properties dialog opens and contains the following fields:

- domset_name
- fetch_columns
- max_fetch
- sort columns **(**This is the only editable field)
- volatility

- where

4. Do one of the following to save the table:

   - If you are working on the test system, select File, Save.

   - If you are working on the production system, select File, Save and set to Test Mode.
     This selection saves your changes in the database, and creates a file (wsptest.mods) on the server defining your changes to the Object Engine. This file is stored in the site/mods /majic subdirectory of your CA SDM installation directory. After creating the wsptest.mods file, WSP causes its Object Engine to recycle so that it will use the new changes. This may take from a few seconds to a couple of minutes, depending on the complexity of your schema.
     A message is prompted. Click Yes to continue. The wsptest.mods file affects only the Object Engine designated by the wsp_domsrvr option. Other Object Engines on the same server do not process this file, and the file is not distributed to other servers. In addition, new tables and columns in Test mode are defined to the Object Engine as local objects. This means that the Object Engine knows about them and you can use them on web forms. However, they do not exist in the database, and do not affect other users. Typical CA SDM users do not use WSP Object Engine, so they are unaffected by the schema modifications you are testing.

   The table is added.

Add a Column

Use the Schema Designer to add a column in the database.

Follow these steps:

1. Select the table for which you want to add a column (or select any of its existing columns).

2. Select Edit, Add Column.
   The Add New Column dialog opens.

3. Enter the column name in the New Column Name field and click OK. Ensure that you begin the names of a column with the letter z to prevent conflict with possible future standard columns. WSP verifies that you added the prefix, but adds a z to the beginning of the column name if necessary.

4. Complete the following fields as appropriate:

   - **Name**
     (Display-only) Specifies the object name of the column. For example, the object name of the Contact alt_phone column is alt_phone.

   - **Display Name**
     Specifies the user-friendly name of the column. You can change the Display Name of a column by entering another name in this field. For example, the display name of the Contact alt_phone column is alternative phone.

- **Schema Name**
  (Read-only for standard tables) Specifies the name used to refer to the column in CA SDM utilities, such as pdm_userload. For site-defined tables, Schema Name defaults to the Object Name. You can change the Schema Name by entering another value in this field.

- **DBMS Name**
  (Read-only for all tables) Specifies the name used to refer to the table in the physical DBMS. For site-defined tables, the DBMS Name equals the same as Schema Name.

- **Description**
  Provides a brief description of the column.

- **Field Type**
  (Read-only for all standard columns in standard tables, and saved site-defined columns) Specifies the data type of the column. You can specify or change the field type of new site-defined columns by selecting a value from the drop-down. The following list describes the available Field Types:

  - **INTEGER**
    Indicates a numeric value.

  - **STRING**
    Indicates a text string. The String Length field indicates the number of characters in a string.

  - **DATE**
    Indicates a date and time. The integer value stored in the database contains the number of seconds since midnight on January 1, 1970.

  - **DURATION**
    Indicates a period of time. The value stored in the database is an integer containing a number of seconds.

  - **DOUBLE**
    Indicates a real (floating point) number.

  - **SREL**
    Indicates a foreign key reference to another table. The SREL Table field specifies the referenced table. The value stored in the database is the rel attr of the referenced table, which can be either an integer or a string. The value displayed in the product is the common name of the referenced table row. For information on setting SREL attributes with foreign key values, see CA Service Desk Manager Reference Commands (see page 3496).

  - **BREL**
    Indicates a virtual column representing the set of all objects with an SREL to this table. It exists only in the Object Engine and is not physically stored in the database. Select this field type only on direction from a CA Technologies employee.

- **QREL**
  Indicates a virtual column representing a set of objects selected by the where clause on the Advanced tab. It exists only in the Object Engine and is not physically stored in the database. Select this field type only on direction from a CA Technologies employee.

- **DERIVED**
  Indicates a virtual column constructed by the Object Engine from the values of other columns, under the direction of a formula specified on the Advanced tab. It exists only in the Object Engine and is not physically stored in the database. Select this field type only on direction from a CA Technologies employee.

- **String Length**
  The length of a string column. This field is blank for non-string columns. It is read-only for all standard columns, and for site-defined columns that have been saved. You can specify or change the length of new site-defined STRING columns by entering an integer between 1 and 32767 in this field.

- **SRel Table**
  The table referenced by an SREL column. This field is blank for non-SREL columns. It is read-only for all standard columns, and for site-defined columns that have been saved. You can specify the table referenced by a new site-defined SREL by selecting it from the drop-down list.

- **On New Default**
  The default value assigned to this column when a new row of the table is defined. It should be a value appropriate to the field type. Some keyword values are available for particular field types:

  - **NOW**
    Specifies the current date and time for a DATE column.

  - **USER**
    Specifies the active user for an SREL to the Contact table.

- **On Save Set**
  The value assigned to this column when a row of the table is updated. It should be a value appropriate to the field type. Some keyword values are available for particular field types:

  - **NOW**
    Specifies the current date and time for a DATE column.

  - **USER**
    Specifies the active user for an SREL to the Contact table.

- **Required**
  When checked, this option indicates that a value must be supplied for the column before a row of the table containing it can be saved. You can set this option for both standard and site-defined columns, and you can disable an option that you have set. However, you cannot turn off the option of a standard column unless it was set by your site.

- **Updatable only for new record**
  When checked, this option indicates that a value for this column can be provided only when a row of its table is initially created, and cannot thereafter be changed. You can set this option for both standard and site-defined columns, and you can disable an option that you have set. However, you cannot turn off the option of a standard column unless it was set by your site.

- **Key for pdm_userload**
  When checked, this option indicates that this column is one of the columns tested by pdm_userload to determine whether or not its input is an update to an existing row. This option is available only for STRING columns. It is read only for all columns in standard tables.

- **DBMS Index Options**
  These options specify characteristics of a column that is an index of the physical DBMS. They are available only for columns in site-defined tables.

  - **Unique**
    Specifies that the column is unique within the table and that no two rows have the same value for the column.

  - **Ascending**
    Specifies that the DBMS index is listed in ascending sequence by this column. Mutually exclusive with Descending.

  - **Descending**
    Specifies that the DBMS index is listed in descending sequence by this column. Mutually exclusive with Ascending.

Important! The Schema Designer includes an Advanced tab. Information on this tab is intended for CA Technologies Support and field representatives. You will not need to work with this tab for most uses of the Schema Designer, and it will not be discussed further in this document.

The Advanced tab of the Schema Designer column dialog shows information meaningful only to persons with internals knowledge of CA SDM. Its contents vary with the column type. We recommend that you modify the values in this tab only on direction from a CA Technologies employee. It contains the following fields if a table is selected:

- **Active Triggers**
  Enter the triggers currently active in the Object Engine for the column. A trigger is a small program that runs under the direction of the Object Engine at certain times when a column is modified. The active trigger list includes both standard and site-defined triggers (so that site-defined triggers are listed both in the active list and in the site-defined list).

- **Site-Defined Triggers**
  Enter the triggers that have been installed at your site. For example, these may be triggers that have been activated as a result of installing a CA SDM option, or triggers that have been written for your site by CA Technical Services. The active trigger list includes both standard and site-defined triggers (so that site-defined triggers are listed both in the active list and in the site-defined list).

- **LRel Specification**
  Enter the specification of a many-to-many relationship between two tables, in the form:
  table1 column1 <> table2 column2
  This shows that the LREL is a many-to-many relationship between table1 and table2, with virtual column column1 containing the relationship in table1, and virtual column column2 containing the relationship in table2.

- **Active xRel Query Information**
  Enter the active specification of the query that defines a BREL or QREL virtual column. The specification is in Object Engine Majic format.

- **Site-Defined xRel Query Information**
  Modify the query associated with a BREL or QREL. It is recommended that you enter data into this field only under the direction of a CA employee.

- **Active Derived Expression**
  Enter the active specification of the expression that the Object Engine uses to construct the value of a DERIVED virtual column.

- **Site-Defined xRel Query Information**
  Modify the expression associated with a DERIVED column. It is recommended that you enter data into this field only under the direction of a CA employee.

The Domsets tab of the Schema Designer Table dialog contains the following:

- **MLIST_DYNAMIC**
  A dynamic domset with no WHERE clause.

- **MLIST_STATIC**
  A static domset with no WHERE clause.

- **RLIST_DYNAMIC**
  A dynamic domset with a WHERE clause defined in the STANDARD_LISTS section of the FACTORY statement.

- **RLIST_STATIC**
  A static domset with a WHERE clause defined in the STANDARD_LISTS section of the FACTORY statement.

If you double-click one of the Domsets, the Properties dialog opens and contains the following fields:

- domset_name

- fetch_columns

- max_fetch
- sort columns (This is the only editable field)
- volatility
- where

5. Do one of the following to save the column:
   - If you are working on the test system, select File, Save.
   - If you are working on the production system, select File, Save and set to Test Mode.
     This selection saves your changes in the database, and creates a file (wsptest.mods) on the server defining your changes to the Object Engine. This file is stored in the site/mods /majic subdirectory of your CA SDM installation directory. After creating the wsptest.mods file, WSP causes its Object Engine to recycle so that it will use the new changes. This may take from a few seconds to a couple of minutes, depending on the complexity of your schema.
     A message is prompted. Click Yes to continue. The wsptest.mods file affects only the Object Engine designated by the wsp_domsrvr option. Other Object Engines on the same server do not process this file, and the file is not distributed to other servers. In addition, new tables and columns in Test mode are defined to the Object Engine as local objects. This means that the Object Engine knows about them and you can use them on web forms. However, they do not exist in the database, and do not affect other users. Typical CA SDM users do not use WSP Object Engine, so they are unaffected by the schema modifications you are testing.

   The column is added to the table.

Modify the Table or Column

To modify information about a table or column, click table or column on the Schema Designer, and enter the new information in the appropriate fields. The information you can modify depends on the status of the table or column:

- **Standard Tables**
  Lets you modify the Display Name, Description, and Function Group fields.
- **Standard Columns**
  Lets you modify Display Name, Description fields, the On New Default Value, and the On Save Set value. In addition, if the check boxes for Required or Updatable only for new record are not selected, you can select them. You cannot remove these options if they are set by default. However, you can reverse your own changes.
- **Site-Defined Table**
  If the table is not published, you can modify all fields, except Name, which cannot be changed after the new table has been saved. After a site-defined table has been published, you can modify only the Display Name, Description, and Function Group fields.

- **Site-Defined Column**
  If the column is published, you can modify all fields, except Name, which cannot be changed after the new column has been saved. After a site-defined column has been published, you can modify only the Display Name and Description fields, the On New Default Value, the On Save Set value, and the check box for Required, Updateable only for new record, Key for pdm_userload, and the DBMS index options.

Test Schema Modifications

You can test your schema modifications and create, update, and view web forms using them before making any changes to the physical database. Putting schema changes in Test mode defines them to the Object Engine, but does not physically store their data in the database. Because putting schema modifications in Test mode has the potential of impacting other users, this option is available only if your installation has installed the wsp_domsrvr and wsp_webengine options to dedicate an Object Engine to WSP.

To put schema changes in Test mode, select Save and set to Test Mode from the File menu. This selection saves your changes in the database, and creates a file on the server (where you are logged in) defining your changes to the Object Engine. This file is called wsptest.mods, and is stored in the site/mods/majic subdirectory of your CA SDM installation directory.

After creating the wsptest.mods file, WSP causes the Object Engine to recycle so that it will use the new changes. This may take from a few seconds to a couple of minutes, depending on the complexity of your schema.

Once the Object Engine has completed recycling, your schema modifications are available, and can be used and test on web forms created with WSP. Data in table and columns in test mode is saved only in internal storage in the WSP Object Engine. It cannot be seen by, and does not affect, other users of the system.

Publish Schema Modifications

After you are satisfied with your schema modifications, you can make them available to all users by publishing them. WSP stores your new or updated tables and columns in the wsptbl and wspcol tables of the database, respectively.

Follow these steps:

1. Create or update files describing the modified schema to the Object Engine and to CA SDM utility programs. WSP creates the following files on the web engine designated by the wsp_webengine option (which defaults to web:local):

   - **wsp.mods**
     Describes all Web Screen Painter-maintained schema changes to the Object Engine.

   - **wsp_schema.sch**
     Describes all Web Screen Painter-maintained tables and columns.

   - **wsp_index.sch**
     Describes DBMS indexes for Web Screen Painter-maintained tables.

- **wsp.altercol**
  Names new columns created by WSP but not yet defined to the DBMS.

- **wsp.altertbl**
  Names new tables created by WSP but not yet defined to the DBMS. In addition, WSP distributes the wsp.mods file to all CA SDM servers with an Object Engine.

2. Select File, Save and Publish.
   The necessary files are created on the CA SDM servers, but does not recycle any of them. Thus, the new files have no immediate impact. However, after the files are created, they will be used the next time CA SDM services are recycled.

3. If you are using the *conventional configuration*, complete the following steps:

   - Shut down the CA SDM services on the primary server and run the following command:

     ```
     pdm_publish
     ```

     This command modifies the physical DBMS to contain information about the new schema.

     Important! Running pdm_publish process has a significant impact on other users. Ensure that you carefully plan the publishing of the schema changes. We recommend you use CA SDM Change Orders to schedule and obtain approval for your planned schema publication.

4. If you are using the *advanced availability configuration,* complete the following steps:

   a. Execute the following command on the background server to notify all active users using Support Automation to save their work:

      ```
      sa_server_notifier [-h] | [-q seconds] | [-c]
      ```

      - **-h**
        Displays the help page.

      - **-q seconds**
        This option notifies a local server (background) to quiesce in a specified time interval. This interval is the number of seconds before the server goes offline. This option cannot be used for a standby server or application server.

      - **-c**
        This option cancels a previously sent quiesce request.

      A pop-up message is displayed to all the active users using Support Automation on the background server. This message notifies the users about the server shutdown and the scheduled time left for the shutdown. The users must save their work and logout within that scheduled time.

   b. Shut down the CA SDM services on the background server.

Important! Do not restart the CA SDM services on standby or application servers after "save and publish" is performed from WSP. This action corrupts the advanced availability configuration. If the CA SDM services on standby or application servers are stopped and you want to start the services, run the pdm_server_control -v command on the servers to suppress the version control before starting the CA SDM services.

Important! If the background server fails during the publishing activity, ensure that you recover the WSP changes. For more information, see the Recover WSP Changes During Background Server Failure (see page 1742) topic.

c. Execute the following command on the standby server that you wish to promote as the new background server:

```
pdm_server_control  -b
```

- **-b**
  Notifies a local standby server to become the background server. The standby server must already be running. If the server is not running, it is started but no failover is performed; to start a failover, run the command again.

The background server shuts down automatically and the standby server is promoted as the new background server. This change does not affect the end-user sessions. The in-progress updates (if any) are stored and delayed, until the new background server comes online.

d. Run the following command on the original background server (now the standby server) to update the DBMS with the schema changes:

```
pdm_publish
```

The pdm_publish command creates a control file that causes the next CA SDM startup to suppress synchronizing the standby server with the background server. This action is necessary to preserve the schema file changes made by pdm_publish. This command optionally performs the second fail-over after successful publishing of the schema changes. The following message is prompted to the user at the end of successful publishing:

```
Do you want pdm_publish to start CA Service Desk Manager in this standby
server and perform fail-over(Y/N)?
```

- If you enter Y, pdm_publish starts the CA SDM services on the standby server and performs fail-over automatically. Skip to step g to apply the schema changes on all the application servers.

- If you enter N, go to Step e.

e. Start CA SDM services on the standby server (original background server).
The startup detects the control file that is created by pdm_publish, but does not synchronize the standby server with the background server. This lack of synchronization preserves the changes made by pdm_publish for this startup.

> **Important!** Ensure that you follow these directions exactly, as the failure to failover to the original background server after a pdm_publish results in corrupted services.

f. Run the following command on the standby server (original background server) to make it the background server again:

```
pdm_server_control  -b
```

This command also deletes the control file, so that version control works normally when this server again becomes a standby server.

g. Execute the following command on the application servers:

```
pdm_server_control -q interval -s server_name
```

- **-q interval -s server_name**
  Notifies a local or remote application server to quiesce in a specified time interval. This interval is the number of seconds before the server goes offline. When using this option without a server_name, the local server is notified to quiesce. This option cannot be used for a background or a standby server.

A pop-up message is displayed to all the active users on the specified application server. This message notifies the users about the server shutdown and the scheduled time left for the shutdown. The users must save their work and logout within that scheduled time. The users log on to the updated application server to resume their work.

h. Restart all standby servers.

Recover WSP Changes During Background Server Failure

You can recover the MDB schema changes when the background server fails during the publishing activity.

> **Important!** We recommend you not to perform the recovery steps directly on the production environment. Ensure that you first validate them on the test or development environment.

Follow these steps:

- If the background server has crashed before publishing, the last saved schema changes are preserved in MDB. You log in to the new background server and resume your publishing tasks.
- If the background server crashed after publishing, perform the following actions:

  1. Stop CA SDM services on the crashed background server.
  2. Choose a standby server that you want to promote as the new background server.
  3. Copy the following files from crashed background server to the same location on the standby server:
     - "NX_ROOT/site/mods/majic/wsp.mods"
     - "NX_ROOT/site/mods/wsp.altertbl"
     - "NX_ROOT/site/mods/wsp.altercol"
     - "NX_ROOT/site/mods/wsp_index.sch"
     - "NX_ROOT/site/mods/wsp_schema.sch
  4. Run the following command on the standby server to publish the schema changes and to perform the automatic fail-over:

     ```
     pdm_publish
     ```

  5. Select Y on the message prompt that appears after successful publishing of schema changes. The CA SDM services are started on the standby server.

     Note: If automatic fail-over does not occur, run the pdm_server_control -b command from the standby server to promote it as the new background server.

  6. Quiesce and recycle each application server. Restart all standby servers. For more information, see the Publish Schema Modifications topic.

Revert Schema Modifications

If you change your mind about your schema modifications after putting them in test mode, you can revert back to the published, version of the schema. Reverting schema modifications has the potential of impacting other users. For this reason, this option is available only if your installation has installed both the wsp_domsrvr and wsp_webengine options to dedicate an Object Engine and a Web Engine to WSP.

Follow these steps:

Select File, Revert Test Mode.
WSP deletes the wsptest.mods file, causing WSP Object Engine to revert its schema back to the published version.

After deleting the wsptest.mods file, WSP causes its Object Engine to recycle so that it can rebuild its internal schema. This may take from a few seconds to a couple of minutes, depending on the complexity of your schema.
After the Object Engine has completed recycling, the active schema is back to its published version.

Note: Web forms modified to work with the new schema are not automatically reverted, and may not work correctly when used with the published schema.

Modify Site-Defined Columns after Publishing

After site-defined schema modifications are published, WSP treats them similarly to the standard schema and restricts further changes. You can delete a site-defined column or can change the length of a site-defined string column by manually updating the DBMS and schema external to WSP. Then you run the pdm_wspupd script to update the database wspcol table to synchronize WSP with the external changes.

Follow these steps:

1. Log in to the following server, depending upon your CA SDM configuration:
   - Conventional: Primary server
   - Advanced availability: Background server
2. Find the site/mods subdirectory in your CA SDM installation directory.

   Tip: Create a backup of the wsp_schema.sch file, at a location other than the site /mods subdirectory, to avoid processing the duplicate files.
3. Edit the wsp_schema.sch file to delete unwanted site-defined columns or change the length of site-defined STRING columns. These updates are the only changes supported by this procedure. You can use any standard text editor to edit the wsp_schema.sch file.

   Important! If any of the index options (such as, UNIQUE) were specified for deleting a column, edit the wsp_index.sch file and remove references to the column. If the column was the only indexed column in the table, remove all references to the table from wsp_index.sch.
4. Edit majic/wsp.mods file with the same changes made to wsp_schema.sch:
   - Delete unwanted site-defined columns.
   - Change the length of site-defined STRING columns.

5. Enter the following command using the command prompt:

   ```
   pdm_wspupd
   ```

   The pdm_wspupd script reads wsp_schema.sch and compares it with the wspcol table in the database, writing a line to the console for any differences. For example, see the following output:

   ```
   PDM_WSPUPD - Update wspcol table from wsp_schema.sch
   Reading wsp_schema.sch to for current DBMS information...
   Reading wspcol table for WSP schema information...
   String column zSalesOrg.description length changed from 350 to 400
   Column zSalesOrg.sym not found in wsp_schema.sch - deleting wspcol row
   pdm_wspupd found 1 WSP-maintained column(s) to update and 1 to delete. Please
   verify that your DBMS has been manually updated to correspond to wsp_schema.
   sch, then reply Y to update wspcol or anything else to cancel.
   ```

6. Verify that the changes found by pdm_wspupd correspond exactly to the changes you made to wsp_schema.sch. If they match, type **Y** to confirm the changes.
   After you confirm the update, the script uses standard CA SDM utilities to update the wspcol table. Then, Schema Designer shows your changes.

7. Stop the CA SDM servers.

8. Using the appropriate utility for your DBMS, alter the DBMS definition of the columns you changed:

   - Delete any columns from the database that you deleted from wsp_schema.sch.
   - Change the database length of any string columns you changed in wsp_schema.sch.

   Take care that the changes you make to the DBMS correspond exactly to the changes you made to wsp_schema.sch.

9. Publish Schema Modifications (see page 1739).

10. Start the CA SDM servers.

How to Modify the Web Interface using Web Screen Painter

Web Screen Painter (WSP) lets you modify web forms to the requirements of your site without programming.

Some of the Knowledge Management forms cannot be modified in the design view of WSP. For these forms, there are alternate approaches to providing the customization, such as:

- Document view -- the document template that is used when creating the document determines the contents of this page. These templates can be modified on the administration tab under documents, document templates.

- Knowledge categories document list -- you can modify this page by using WSP, but it is also managed by user preferences. The “preferences” screen provides personalization per user for defining which document properties displays in the document list and how many documents display per page.

Follow these steps:

1. Verify the Prerequisites (see page 1747)

2. Start WSP (see page)

3. Choose the Form to Modify (see page)

    - Create a Form (see page 1747).

    - Open an Existing Form (see page 1749).

4. Modify a Form (see page)
   WSP always saves changes on the server where WSP is installed. When you save a file, it becomes accessible to other WSP users in a preview session, but is invisible to typical CA SDM users. This is because WSP saves all files in the site/mods/wsp directory, and this directory is not used by a typical CA SDM session.

5. If you are making web form changes in the test system, Migrate from Test to Production System (see page 1762).

6. Publish Form Changes (see page 1763).

7. (If necessary) Delete Forms After Publishing.

Verify the Prerequisites

Verify the following prerequisites before you begin the customization:

- Modified the schema that you want to add in the web forms.
- (For advanced availability configuration only) Verified that the following prerequisites to publish the web forms successfully:
  - (Recommended) CA SDM services are up and running on all the CA SDM servers. Otherwise WSP publishes only on the CA SDM servers that are up and running.
  - (Required) At least one webengine instance running on every CA SDM server.

Start WSP

Start WSP to modify web forms.

Follow these steps:

1. Log in to the computer where you have WSP installed.
2. Start WSP.
   - (Windows) Click Start, Programs, CA, Service Desk, WSP.
   - (UNIX) Enter the command *pdm_wsp* with $NX_ROOT/bin in your path.

     Important! When you use UNIX, ensure that you have Firefox installed to use WSP.

   The WSP login window opens.
3. Enter your credentials.
   WSP displays the main form.

Choose the Form to Modify

You can create a form or can open an existing form to modify. Choose from the following possibilities:

- Create a Form (see page 1747).
- Open an Existing Form (see page 1749).

Create a Form

Create a form in WSP.

Follow these steps:

1. Click File, New.
   The New Form dialog opens.

2. Complete the following fields, as appropriate:

   - **Interface or File Type**
     Indicates the file type of the form. For example, to create an HTMPL form select an interface (Analyst, Customer, Employee, Default, or PDA). To create a form of other file type by select the type directly (CSS Stylesheet, HTML, or JavaScript). When you select an interface or file type, WSP displays a list of all available templates for the selected file type in the File Name field.

   - **Form Group**
     Indicates the form group (as defined for your CA SDM installation) where you want to create your new form or file. If you have not defined any form groups, only the DEFAULT form group is listed.

   - **File Name**
     Indicates the template for the selected interface or file type. A template contains the basic requirements for a new form or file of the desired type.

   - **Select table for new list or detail form**
     Indicates the CA SDM tables for which you can create a new list or detail form. This field is populated according to your selection of an interface (Analyst, Customer, Employee, Default, or PDA).

     Note: Only one detail or list form can exist for each table in a forms group, so edit an existing form (rather than create one) for tables that already have an existing form. If you want to have multiple versions of a form, create one or more form groups to hold the additional versions.

3. Click New.

4. The form is displayed for your customizations. The following two tabs are displayed:

   a. **Design**
      Available for detail forms, list forms, and menu bar forms, and shows the controls on the form laid out more or less as a user would see them. It is not an image of how the form looks to an end user. To see this, select **Tools**, **Preview**.

   b. **Source**
      A Notepad-style editor allowing you to review and edit the source code for a form. Some forms are editable only in the Source tab. For those forms, the edit window opens up on the Source tab, and the Design tab is disabled.

   The form is ready for customization.

Important! When you create or edit a detail or list form, use the list_ and detail_ prefixes to name the HTMPL file. For example, use list_test.htmp" and detail_test.htmpl. This prefix lets you correctly preview a form. When you save a detail template with a custom name, you must also manually edit the <PDM_WSP> tag. For example, <PDM_WSP mode=edit preview="test.htmpl+OP=CREATE_NEW" factory=cr>.

Open an Existing Form

Open an existing form in WSP to modify it.

Follow these steps:

1. Select File, Open.
   The Open Form dialog opens.

2. Select the Interface (Analyst, Customer, Employee, Default) or File Type (CSS Stylesheet, JavaScript, or HTML) and the forms group that contains the form you want to edit.

3. Select either the form you want from the list, or enter its name in the textbox.
   When you enter a name in the textbox, WSP automatically scrolls the list to the first name matching the characters entered. You can use the Files of Status drop-down list to restrict the list of files displayed:

   - **Site Modified with Unpublished Changes (+)**
     Restricts the list to files that have been modified with WSP, but not yet published. These files are identified with a plus sign (+) after the file name.

   - **Site Modified (*)**
     Restricts the list to forms modified at your site, both published and unpublished. The unpublished files are identified with a plus sign (+) after the file name. The published site modifications are identified with an asterisk (*) after the file name.

   - **All**
     Displays the list with no restrictions. The unpublished files are identified with a plus sign (+) after the file name. The published site modifications are identified with an asterisk (*) after the file name.

4. Click Open.
   The form is displayed and ready for your customization.

Modify a Form

After you open the form you want to edit in WSP, you can use the toolbar, menu commands, and shortcuts to customize it. You can perform the following customization:

- Insert a Control
- Edit Control Properties
- Modify Menu Bars

- Modify Stylesheets
- Modify Mouse-Over Preview Form
- Modify Data Grid List on List Form
- Modify Notebooks on Detail Form
- Modify HTML and JavaScript Files

Insert a Control

Add a control on the form. For example, add a textbox in the form.

The controls that can be inserted on both list and detail forms are the following:

Control	Icon	Description
Insert Row	 BSVC_r12.1--Inserting a Control	Causes the selected control to be the last in its current row (moves following controls to the next row).
Delete Row	N/A	Deletes all controls on the same row as the currently selected control.
Textbox	 BSVC_r12.1--Inserting a Control (2)	Inserts a single or multi-line textbox for editing a string or text field.
Dropdown	 BSVC_r12.1--Inserting a Control (3)	Inserts a drop-down list for editing a field validated against a table.
Lookup	 BSVC_r12.1--Inserting a Control (4)	Inserts a lookup control for editing a field validated against a table. The control consists of a textbox with a hyperlink in the label that pops up a select form.
Button	 BSVC_r12.1--Inserting a Control (12)	Inserts a button.

Control	Icon	Description
Hierarchical Lookup	 BSVC_r12.1--Inserting a Control (5)	Similar to a Lookup control, except that it is used for a field with a hierarchical selector (such as request category).
Date	 BSVC_r12.1--Inserting a Control (6)	Inserts a date field. The control consists of a textbox with a hyperlink in the label that pops up a date selector.

The following additional controls are available for detail forms only:

Control	Icon	Description
Checkbox	 BSVC_r12.1--Inserting a Control (7)	Inserts a check box.
HTML Editor	 BSVC_r12.1--Inserting a Control (8)	Inserts an HTML editor for a text field that contains HTML.
Read Only Textbox	 BSVC_r12.1--Inserting a Control (9)	Inserts a non-editable text field.
Read Only Lookup	 BSVC_r12.1--Inserting a Control (10)	Inserts a non-editable lookup field. The field is displayed as a hyperlink to pop up the detail form defining it.
Read Only	 BSVC_r12.1--Inserting a Control (11)	Inserts a non-editable date field.

Control	Icon	Description
Notebook	 BSVC_r12.1--Inserting a Control (13)	Inserts a notebook. There can only be one notebook on a detail form, so this control can be inserted only on forms that do not already contain a notebook.

The following additional control is available for list forms only:

Control	Icon	Description
List	 BSVC_r12.1--Inserting a Control (14)	Inserts a list. There can only be one list on a list form, so this control can only be inserted on new list forms.

Follow these steps:

1. Right-click the form at the location where you wish to add the control and select Insert Control.
   A dropdown list is displayed.

2. Select the insert control dialog options (see page 1752).
   The control is placed on the form.

3. Select Tools, Preview to check how the form is displayed to the end user. Although it resembles a standard CA SDM window, and most buttons and menus are functional, it is not a standard session, and you should not attempt to use it that way.

4. Click File, Save.
   The controls are added on a form.

Insert Control Dialog Options

Open the Insert Control dialog from the File menu. The dialog lists all of the appropriate UI controls for the section of the form you select to edit.

The dialog contains the following options:

- **Insert Before**
  Inserts the selected control from the list before the currently selected control on the base form, and makes it the currently selected control.

- **Insert After**
  Inserts the selected control from the list after the currently selected control on the base form, and makes it the currently selected control.

- **Prev**
  Moves the currently selected control to the control that precedes it on the form.

- **Next**
  Moves the currently selected control to the control that follows it on the form.

- **Properties**
  Opens the Properties dialog for the currently selected control.

- **Close**
  Closes the Insert Control form.

- **Close Form After Insert**
  (Enabled) Inserts the selected control and closes the Insert Control dialog when you click Insert Before or Insert After.
  (Disabled) Inserts the selected control when you click Insert Before or Insert After. The Insert Control dialog remains open to insert additional controls or request properties for the currently selected control. After you clear the check box, the Close Form After Insert check box remains unchecked until you either select it again or end your WSP session.
  Default: Enabled

Edit Controls Properties

Edit the properties of a control.

Follow these steps:

1. Select the control and press F4.
   The Properties dialog opens.

2. Change properties as appropriate. For example, the Caption property specifies the header label that is displayed above a control. To specify this property, enter the desired value in the cell to the right of the Caption property.

3. Close the Properties dialog.

4. Select Tools, Preview to check how the form is displayed to the end user. Although it resembles a standard CA SDM window, and most buttons and menus are functional, it is not a standard session, and you should not attempt to use it that way.

5. Click File, Save.
   The properties of the control is modified and the form is saved.

Modify Menu Bars

Forms with names beginning *menubar_* define a menu bar. The Design view for a menu bar displays the menu at the top. You can click a menu item to lower the menu, but cannot otherwise edit the menu bar directly in Design view. To edit a menu bar, double-click the menu item to display the Menu Designer.

Note: Menus (and menubar forms) are used only in the analyst interface. The customer and employee interfaces use a "launch bar" containing actual links, not drop-down lists. To modify the customer or employee launch bar, edit form std_body_site.htmpl from the appropriate interface.

Follow these steps:

1. Select Tools, Menu Designer or double-click the menu shown in the Design tab of a menubar form.
   The Menu Designer dialog is displayed.

2. Complete the fields in the Menu Designer dialog (see page) to add or edit menu items.
   For more information about adding menu items, see the Functions Useful in Menu Items (see page 1755) topic.

3. Click OK to close the dialog.

4. Select Tools, Preview to check how the form is displayed to the end user. Although it resembles a standard CA SDM window, and most buttons and menus are functional, it is not a standard session, and you should not attempt to use it that way.

5. Click File, Save.
   The menu bar is modified in the form.

Menu Design Dialog

The Menu Designer dialog appears when you select Menu Designer from the Tools menu, or double-click the menu shown in the Design tab of a menubar form. Use the Menu Designer dialog to add a menu bar, menus, submenus, and menu commands to the open form.

Note: You can access the Menu Designer only while editing HTMPL forms with a name beginning with “menubar_”, such as menubar_admin.htmpl.

The Menu Editor dialog contains the following controls:

- **Menu List**
  From the menu list, select the menu item you want to change. To change the menu label, for example, select a menu label from the list, type a new name in the Caption text box, and click Apply. You can add, insert, delete, and move the menu items using the controls in the Menu Designer.

  Note: Only one level of indentation is possible.

- **Caption**
  Enter the name for the selected menu item. See the property for more information.

- **Function**
  Enter the JavaScript function to execute when the user clicks the menu. See the description of the Function property for more details, including some pre-defined functions that may be useful in menus.

- **ID**
  Enter the HTML/JavaScript id to be assigned to the menu item.

- **Hot Key**
  Enter a list of characters directing CA SDM's selection of the hotkey for this menu item. The hotkey is underlined in the menu caption when it is displayed. CA SDM typically selects the first key in the menu caption not already in use as a hotkey. You can specify one or more characters here to restrict the selection to those characters, or specify one or more characters preceded by an explanation point to prevent selection of those characters.

- **Image**
  Enter the location of the image that you want to appear next to the menu item.

- **Internal**
  Select this option to specify that the JavaScript invoked by the function should be executed in the context of the current window (which could be a pop-up detail window). Leave this option unchecked to specify that the function should be executed in the context of the main form.

- **Variable**
  Enter the JavaScript variable to be assigned to the menu item.

- **Tool Bar**
  Adds a tool bar icon and tooltip that corresponds to a non-top-level menu item.

- **Icon File**
  Identifies the location of the Tool Bar icon.

- **Tip**
  Specifies the tooltip text.

Functions Useful in Menu Items

CA SDM provides a menu bar on almost every form to control its functions. The menu bar is generated by an HTMPL form with a name of the form menubar_*xx*.htmpl. We recommend that you use WSP to modify existing menu bars and define new ones.

The following predefined functions may be useful for scripts invoked by menu items:

- **upd_frame(form)**
  Loads a new form into the main window content frame.

- **create_new(factory, use_template, width, height [,args])**
  Pops up a form to define a new record.
  Popup_window(name, form[, width, height [,features [,args]]])
  Pops up a new window.

- **showDetailWithPersid(persid)**
  Pops up a detail record.

The following terms and definitions apply to the previous functions:

- **Form**
  This is either an HTMPL file name of the form xxx.htmpl or an operation code (for example CREATE_NEW).

- **factory**
  This is the name of a database object.
- **use_template**
  This is either true or false.
- **width**
  This represents the desired form width or zero for default.
- **height**
  This represents the desired form height or zero for default.
- **features**
  This is a list of window features, in the same format used with the standard window.open function.
- **args**
  This is one or more args of the form "keyword=value" for the operation specified for form.
- **persid**
  This is a persistent ID in the form factory:ID.

Modify Stylesheets

You can use WSP to edit or create CSS (cascading stylesheet) files.

Note: For performance reasons, CA SDM stylesheets are delivered in two forms: Individual files (such as search_filter.css) and combination files grouping a number of individual files with comments and excess white space removed (such as analyst_styles.css). WSP always edits the individual files; you cannot edit a combination file directly. When you publish stylesheet changes, WSP automatically builds the associated combination file if necessary.

Follow these steps:

1. Create or open CCS stylesheet file.
   WSP displays the Source view of the stylesheet.
2. You can edit directly in Source view, or display the Style Designer by selecting Tools, Style Designer.
3. Complete the fields in the Style Designer dialog (see page 1757), as appropriate. There are a number of style attributes, such as margin and border that can neither be seen nor edited in the Style Designer. These must be edited in Source view.
4. Click OK in the Style Designer.
   WSP reformats the stylesheet and updates the Source view.
5. Click File, Save.
   The stylesheet is modified.

Style Designer Dialog

The Style Designer lets you modify or customize style sheets. By default the Style Designer dialog opens in the Font and Color tab and contains the following controls:

- **Style Classes**
  From the drop down list, select a style element you want to modify.

- **Add**
  Click to add a new style class.

- **Rename**
  Click to rename the style class selected in the Style Classes dropdown list.

- **Delete**
  Click to delete the style class selected in the Style Classes dropdown list.

- **Installed Fonts**
  This property lists the fonts that are installed on the system. Click the left and right arrows to move the selected fonts between the Installed Fonts list and the Selected Fonts list.

- **Selected Fonts**
  This property specifies a hierarchical list of preferred fonts that a browser uses to draw the style class element. A browser uses the first font in the list that is installed on the system it is running on.
  Click the up and down arrows to move the selected fonts up or down the hierarchy.

- **Font Size**
  Select the font size from the dropdown list.

- **Bold**
  Select a font style from the dropdown list.

- **Italics**
  Select a font style from the dropdown list.

- **No Effect**
  Select this option if you do not want any text decoration or special effects.

- **Underline**
  Select this option if you want the text to be underlined.

- **Strikethrough**
  Select this option if you want the text to appear with a line through it.

- **Overline**
  Select this option if you want the text to appear with a line above it.

- **Foreground Color**
  Select the foreground color for the text element by clicking the Browse button to the right of the Foreground Color property. Then select the color you want from the Color palette, and click OK.

- **Background Color**
  Select the background color for the text element by clicking the Browse button to the right of the Background Color property. Then select the color you want from the Color palette, and click OK.

- **Transparent**
  Select this option if you want the background of the style element to be transparent.

A sample of the style element is displayed in the preview area at the bottom of the dialog.

To set the position of the style element, click the Position tab. The Position tab contains the following controls:

- **Position**
  From the dropdown list, select one of the positions for the element. The position property places an element in a static, absolute or relative position. Selecting a Static value will place the element in accordance with the normal flow. Selecting an Absolute value will place the element anywhere on a page. Selecting a Relative value moves the element relative to its normal position.

- **Left**
  Enter a value for the left margin in the text box for the element. Select a size from the dropdown list. This property is disabled when the selected position is Static.

- **Top**
  Enter a value for the top margin in the text box for the element. Select a size from the dropdown list. This property is disabled when the selected position is Static.

- **Width**
  Enter a value for the width in the text box for the element. Select a size from the dropdown list.

- **Height**
  Enter a value for the height in the text box for the element. Select a size from the dropdown list.

- **Z-Index**
  Enter a value for the stack order in the text box for the element. An element with greater stack order is always in front of an element with lower stack order. Z-index only works only on elements that have Absolute position

Note: Elements can have negative stack orders.

Click the Other tab to set some of the specific properties for the element. The Other tab contains the following controls:

- **Visibility**
  Select the type of the visibility for the element from the dropdown list. The Visibility property sets how the content of an element is displayed if it overflows its area.

- **Overflow**
  Select the type of overflow for the element from the dropdown list. The Overflow property sets what happens if the content of an element overflow its set area.

- **Display**
  Select the type of the display for the element from the dropdown list. The Display sets how an element is displayed.

- **Cursor**
  Select the type of cursor for the element from the dropdown list. The cursor property specifies the type of cursor to be displayed when pointing on an element.

- **OK**
  Click to close this dialog and save your changes.

- **Cancel**
  Click to close the Style Designer dialog.

Modify Mouse-Over Preview Form

The Mouse-over previews let you view key details within the current form without the need to click a link or open a new web page. The mouse-over preview appears when you place a cursor over an object link on a list or detail form for a certain amount of time. If you move the mouse away from the link before the delay time expires, the preview does not appear. Mouse-over previews appear by default on all list and detail forms in read-only mode.

You can create mouse-over previews for forms that do not have preview_ forms by default. You can also create mouse-over previews for custom forms you created in your CA SDM environment.

The following predefined mouse-over preview forms are available:

- preview_chg.htmpl (Change Order)
- preview_cnt.htmpl (Contact)
- preview_cr.htmpl (Request)
- preview_in.htmpl (Incident)
- preview_iss.htmpl (Issue)
- preview_KD.htmpl (Knowledge Document)
- preview_nr.htmpl (Configuration Item)
- preview_pr.htmpl (Problem)

Follow these steps:

1. Open one of the following forms for the customization:
   - Open an existing form that does not have a preview_ form by default.For example, detail_loc.htmpl
   - Open an existing mouse-over preview form. For example, preview_chg.htmpl.
2. Modify the form. For example, add or remove custom controls from the form.

3. Click File, Save As, specify a file name using the preview_ prefix, and click Save. For example, enter preview_loc.htmpl.
   The mouse-over preview form is created and modified.

Modify Data Grid List on List Form

Data grid lists let you view the contents of a product page on a list form without opening a new page. This data-bound control lists items from the data source in a table so you can select items, sort items, and fetch data. For example, the expand and collapse options on the Incident List form.

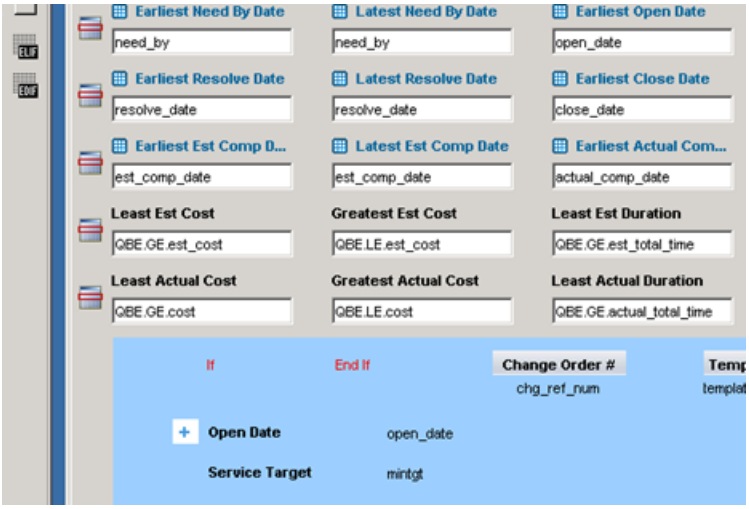
Follow these steps:

1. Open a list form.

2. Locate the blue area after the labeled fields near the end of the form in the Design view. If you prefer Source view, the data grid appears between the following lines of code:

   ```
   <PDM_MACRO name=lsStart>
   <PDM_MACRO name=lsEnd>
   ```

   The following example shows this data grid area in Design view:



The plus sign in the data grid area represents the beginning of the expansion section of the row (the fields that are displayed only when a user clicks plus on the row in the list form grid). The following code generates the plus sign in the Source view:

```
<PDM_MACRO name=lsCol attr=open_date label="Open Date" sort="DESC" startrow=yes>
```

The *startrow=yes* parameter specifies to start a row, and it starts the expansion section of the row.

- Drag-and-drop columns to move them in a list. You can move columns between the main part of the row and the expansion section. You cannot move an existing control after the grid area.

- To insert a list column, right-click a control or anywhere within the blue background, and select either Insert Column or Insert Control.

- If you select Insert Column, WSP inserts a column to the left of the currently selected control.
- If you select Insert Control, WSP displays the Insert Control dialog that lets you add the desired control to the form.

- Select Tools, Preview to check how the form is displayed to the end user. Although it resembles a standard CA SDM window, and most buttons and menus are functional, it is not a standard session, and you should not attempt to use it that way.
- Click File, Save.
  The data grid list is modified on the list form.

Modify Notebooks on Detail Form

The Nested tabs (notebook) control lets you expand or collapse key details within the current form. For example, use the control to customize how you organize tabs on the Incident Detail Form. From the Design View, you can use the Notebook control to add nested tabs to a detail form that does not already contain one. Double-click the Notebook control to modify it. Use drag-and-drop to add, insert, and delete notebook tabs, and to change their captions. You can also use the up and down arrow buttons to rearrange tabs by changing the position of the currently selected tab. The New Row check box specifies whether or not the selected tab begins a new row in the notebook header.

Follow these steps:

1. Open a detail form.
2. Locate the blue area of the form in the Design view that contains the first numbered label. If you prefer Source view, the notebook area appears between the following line of code:

```
<PDM_MACRO name=startNotebook hdr=cng_nb><PDM_MACRO
name=endNotebook>
```

Note: In CA SDM r12.6, a notebook can contain nested tabs. In WSP, a high-level tab (a tab containing other tabs) is named a tab group. WSP displays a tab group as a dark blue solid bar that spans the entire blue notebook area, with a numbered label in its center. A low-level tab (a tab that does not contain other tabs) is named a tab. WSP displays low-level tabs as rectangles with rounded corners.

3. Click a tab to select it. Selecting a tab highlights and displays a link to the contents of the tab at the bottom of the notebook.
   You can move tabs and tab groups within a notebook using drag-and-drop. Moving a tab group moves all the tabs within the group with it.
4. To insert a tab or tab group, right-click a control or anywhere on the blue notebook background and select Insert Tab, Insert Tab Group, or Insert Control.
   If you select Insert Tab or Insert Tab Group, WSP inserts a new tab or tab group to the left of the currently selected control. If you select Insert Control, WSP displays the Insert Control dialog that lets you add the desired control to the form.

5. Select Tools, Preview to check how the form is displayed to the end user. Although it resembles a standard CA SDM window, and most buttons and menus are functional, it is not a standard session, and you should not attempt to use it that way.
   Click File, Save.

Modify HTML and JavaScript Files

You can use WSP Source view to edit HTML and JavaScript forms.Open an HTML or JavaScript file and make the necessary changes.

Note: For performance reasons, some CA SDM JavaScript files are delivered in two forms: Individual files (such as window_manager.js) and combination files grouping a number of individual files with comments and excess white space removed (such as std_head.js). WSP always edits the individual files; you cannot edit a combination file directly. When you publish script changes, WSP automatically builds the associated combination file if necessary.

Migrate from Test to Production System

One of the design goals for WSP was to make it safe to develop and test forms modifications on a production database. Such features as a WSP-only directory tree on the server, dedicated WSP server processes, and read-only preview sessions support this goal. However, many users prefer to develop their forms modifications in an independent test system and then migrate the forms to a separate production system after they are complete as follows:

1. Copy any HTMPL forms to be migrated from the appropriate subdirectory of site/mods/www /htmpl on the test system to the same subdirectory of site/mods/wsp/project on the production system.

2. Copy any CSS, JavaScript, and HTML files to be migrated from the appropriate subdirectory of site/mods/www/wwwroot on the test system to the same subdirectory of site/mods/www /wwwroot/wsp/project on the production system.

   Note: Ensure that you copy the files and forms on the following servers of the production system, depending on your CA SDM configuration:

   - **Conventional:** Primary server
   - **Advanced availability:** Background server

Note: You can use any file copying method supported by your operating system to perform the copying described in steps 1 and 2 above. Windows users should substitute backslash (\) for slash (/) in the directory paths shown.

Publish Form Changes

When you are satisfied with the changes, you can make them available to all CA SDM users by publishing them. Publishing updates all CA SDM servers with new or revised forms.

Follow these steps:

1. Select File, Publish.
   If you have any unsaved changes, WSP prompts you to save them, and then displays a confirmation dialog showing all pending Web Screen Painter changes (including those saved in previous sessions, or saved by other Web Screen Painter users). By default, all changes are selected for publication. You can change the selection of changes to be published by clicking them.

2. Click OK when you are satisfied with the selection.

3. (Advanced availability configuration only) If the webengine is not running on any of the CA SDM servers, an error message is displayed with the list of CA SDM servers on which WSP failed to publish. Complete the following steps:

   a. Configure the CA SDM server (the server specified in the error message) to make the corrections.

   b. Edit the file in WSP to add a white space character in the <PDM_IF 0> macro and save it.

   c. Go back to step 1 to republish the web form.

   Note: If you do not want to make any configuration changes, you have to manually copy the nx_root/site/mods/www folder from the background server to all the other servers.

4. (Advanced availability configuration only) If the background server crashes while publishing, recover the HTMPL changes.

5. (For mouse-over preview forms) Execute the following command after publishing the changes:

   ```
   pdm_webcache  - H
   ```

   The web cache is refreshed. WSP makes the selected changes available to all users active on all the servers.

Note: Only site-modified forms can be deleted. Requests to delete a previously published form take effect when you publish changes. To cancel a pending delete request, select File, Undelete Form. You undo changes to a form after publication.

Recover the HTMPL Changes

You recover the HTMPL changes when the background server fails during the publishing activity.

Important! We recommend you not to perform the recovery steps directly on the production environment. Ensure that you first validate them on the test or development environment.

Follow these steps:

1. Go to the following directory on the crashed background server:

   ```
   $NX_ROOT$/site/mods/www/wwwroot/wsp/project/web
   ```

2. Copy all the content from the web folder.

3. Log in to the new background server and paste all the copied content in the NX_ROOT/site /mods/www/wwwroot/wsp/project/web folder.

4. Resume publishing the changes on the new background server.

HTML Templates (HTMPL Form)

This article contains the following topics:

Forms in the CA SDM web interface are delivered as HTML templates, in files with a suffix of .htmpl. These are called HTMPL forms in the remainder of this document.

An HTMPL form contains standard HTML (including JavaScript) plus language extensions that are interpreted by a CA SDM server daemon (or service) called the web engine that delivers standard HTML to the browser. These extensions are:

- References to server variables. These are indicated by a name beginning with a dollar sign. They can be the values of columns in the CA SDM database, references to web engine configuration properties, or other server information.

- Special tags directing the web engine to perform tasks on the server, such as read information from the CA SDM database. These tags have names of the form <PDM_...> or <pdm_...>.

Note: You do not need to understand the HTMPL extensions or even HTML itself to be able to customize CA SDM forms with WSP.

Template Naming Conventions

The following naming conventions are used to identify the four basic types of HTMPL files, where *xxx* is the object:

Template Type	Name
List (search filter and results)	list_*xxx*.htmpl
Combined read-only and edit detail form (analyst interface)	detail_*xxx*.htmpl
Read-only detail form	detail_*xxx*_ro.htmpl
Edit detail form	detail_*xxx*_edit.htmpl

You can find the definitions of the objects and their properties in the following locations:

- (UNIX) $NX_ROOT/bopcfg/majic/*.maj
- (Windows) *installation-directory*\bopcfg\majic*.maj

For information about the objects and attributes that define CA SDM, see CA Service Desk Manager Reference Commands (see page 3496).

HTMPL Directories

There are different sets of HTMPL files supplied to implement these interfaces, as shown in the following table:

Operating System	Directory Containing HTMPL Files
Windows	*Installation-directory*\bopcfg\www\htmpl\web*interface*
UNIX	$NX_ROOT/bopcfg/www/htmpl/web/*interface*

In this table, *interface* is the name of the interface (analyst, customer, or employee).

Note: There is no separate directory for guest interface files; by default, this interface uses the employee interface files. You can change the guest user interface by changing the access type associated with user System_Anonymous. Both the customer and employee files dynamically modify themselves depending on whether the current user is a known user or a guest, using the <PDM_IF> template command described in this document.

There are three additional interface subdirectories under the htmpl directory:

- **default:**
  Contains HTMPL files common to all interfaces. When searching for a file, the web engine looks first in the directory corresponding to the current user's interface, and then in the default directory.
- **pda/analyst: (UNIX)**

- **pda\analyst: (Windows)**
  Contains HTMPL files used by the mobile device interface. In CA Service Desk Manager r11.0, the mobile device interface is provided only for analysts.

- **web/*interface*/legacy: (UNIX)**

- **web*interface*\legacy: (Windows)**
  Contains HTMPL files from your previous release of CA SDM that are no longer used. This directory is automatically created if you upgrade from a previous release when you install CA SDM. You can delete the legacy directory when none of its files are referenced by your customized files.

We strongly recommend that you do not directly modify the supplied HTMPL files. Instead, either use WSP, or manually copy the file you want to modify to the site mods directory, and modify it there. The CA SDM web server looks for a new form in the appropriate site mods directory before checking the distribution directory. The standard site mods directories for each of the interfaces are as follows:

Operating System	Directory For Site-Modified HTMPL Files
Windows	***installation-directory**site**mods**www**htmpl**interface**interface***
UNIX	$NX_ROOT/site/mods/www/htmpl/*interface/interface*

Note: If you change the form and save it into the *install directory**site**mods**www**htmpl**interface* directory, the form will be seen by everyone, regardless of the form group to which they belong. If you save it into the *install directory* \site\mods\www\htmpl\interface*interface* directory, only those Contacts that are defined as belonging to that form group will see the changed forms.

In the previous table, *interface* is the name of the interface (analyst, customer, or employee). There is no separate directory for guest interface files; this interface uses the employee interface files. The advantage of storing your modified HTMPL files in the site mods directory is that this directory is preserved when you install CA SDM maintenance or a new release. In addition, keeping your modified files in site mods while preserving the originals ensures that you always have a correct copy of the originally distributed HTMPL file.

Each web interface page has a primary function, as indicated in the following table that lists the major HTML templates. However, you can add <PDM_FORM> blocks to any template to directly access any web interface supported operation. For example, you can modify the main menu to include fields for submitting an issue without using the intermediate page, or you can add search criteria fields and a search button to a list form:

Web Page	HTML Template
Main form	menu_frames.htmpl
Display/create/update a change order	detail_chg.htmpl
Display a list of change orders	list_chg.htmpl
Display/create/update and issue	detail_iss.htmpl

Web Page	HTML Template
Display a list of issues	list_iss.htmpl
Display/create/update a request	detail_cr.htmpl
Display a list of requests	list_cr.htmpl
Display announcement detail information	detail_cnote_html
Display a list of announcements	list_cnote.html
Login	login.htmpl

Note: For a complete list of templates, view the contents of the directories in the table at the beginning of this section.

Web Form Groups

You can collect customized web pages into one or more form groups. Form group directories are in the following directories:

- **Windows**
  install-directory\site\mods\www\htmpl\web*interface*
  install-directory\site\mods\www\wwwroot\subdirectory

- **UNIX**
  $NX_ROOT/site/mods/www/htmpl/web/*interface*
  $NX_ROOT/site/mods/www/wwwroot/subdirectory

Each form group is a subdirectory under these directories. You specify the customized form directory in the Customization Form Group field of the access type.

When a user requests a form, the web engine looks first in the appropriate customized form group directory, then in the standard directory for the user's web interface, and finally in the default directory. You can define more than one access type for the same web interface, each with a different customized form group. This lets you define a few specialized forms for different types of users, and still take the majority of the forms from the standard interface.

A similar process occurs when a web page requests a file from one of the subdirectories of wwwroot (css, html, img, or scripts). The webengine examines an HTMPL reference of the form CAisd/img/xxx.gif and converts it to one of the following GIF files, selecting the first one where it finds xxx.gif:

- /CAisd/sitemods/img/formgroup/xxx.gif
- /CAisd/sitemods/img/xxx.gif
- /CAisd/img/xxx.gif

How to Create a Web Form Group

You can create a web form group.

Follow these steps:

1. If you want a form group besides the predefined Analyst, Customer, or Employee form groups, create a form group by selecting Save As from the File menu in WSP and clicking the Add Form Group button on the Save Form As dialog. For example, if you want to provide two separate customized versions of the Analyst interface, you might create form groups called Analyst1 and Analyst2 to handle these. You might also define a new form group if the interface you are defining does not logically fit into one of the predefined form groups.

2. On the web interface (not a Web Screen Painter preview session), select Security, Access Types from the Administration menu. Then click an access type (or create one) and use the Customization Form Group drop-down list on the Access Type Detail window to assign a form group to an access type. CA SDM determines the access type when a contact logs in and uses customization form group to determine where to look in the site mods directory structure for customized forms. If the web engine does not find a form in the form group directory, it looks first in the standard directory for the user's access type, and then in the default directory.

3. In WSP, select Save from the File menu, or manually copy the customized HTMPL files to the following directory:
   In Windows: *installation-directory*\site\mods\www\htmpl\web*form_group_name* directory
   In UNIX: $NX_ROOT/site/mods/www/htmpl/web/*form_group_name*

After you set up a new web form group and copied any supporting files to the appropriate subdirectories, you must restart the web service before the changes take effect.

PDM_MACRO Insert Text from a Macro File

The <PDM_MACRO> tag is used to insert a macro file into an HTMPL file. Its functionality is similar to PDM_INCLUDE, with two important differences:

- A file included by PDM_MACRO has a formal argument list, with required arguments and arguments with default values.

- A file included by PDM_MACRO always comes from the directory specified for the configuration property MacroPath, regardless of the current user's access type.

- **NAME=*macroname***
  (Required) Specifies the macro to include. The web engine affixes the suffix ".mac" and searches for the file in the path specified by configuration file property MacroPath.

Other properties may be required, depending on the macro included. A macro file has the general layout:

```
comments
#args
name1 [= value1]
name2 [= value2]
...
#data
data to insert
```

The following descriptions explains the file layout, line by line:

- **comments** -- The only valid statements in a macro prior to the #args statement are comments. Comments are indicated by either a # sign or a // as their first non-blank character or characters.

- **#args** -- Must be coded exactly as shown, with the # sign in column one and no other information on the line. This statement begins the args section, which can contain argument definitions and comments.

- **name [= value]** -- Defines an argument for the macro. Only arguments explicitly mentioned in the args section are valid for the macro. A value specified for an argument in the args section is that argument's default value. Arguments without a default value are required, and must be supplied by the caller on the <PDM_MACRO> statement itself.

- **#data** -- Must be coded exactly as shown, with the # sign in column one and no other information on the line. This statement begins the data section, which is the part of the macro inserted into the file using PDM_MACRO. Everything in the data section is inserted into the calling file, including lines that would be comments prior to the data section.

- **data to insert** -- The data to insert into the calling file. This data can contain references to arguments in the form:

- **&{arg_name}** -- These references are replaced with the value of the argument supplied by the caller, or with the default value if the caller did not supply a value.

The web engine normally reads a macro file only once, the first time it is used, and then stores the parsed macro in its own memory. This improves performance, but can be inconvenient if you are developing a macro. Use the configuration file property SuppressMacroCache to prevent this behavior and cause the web engine to discard all macros in its memory each time it begins processing a new form.

To Comment Out PDM_MACRO Tags

To comment out <PDM_MACRO> tags, enter an exclamation point in front of the P as follows: <! PDM_MACRO>. To prevent the browser from processing the commented out portion of the form, place <PDM_IF 0> before the <!PDM_MACRO> tag, and </PDM_IF> after the line you commented out.Example:

```
<PDM_IF 0>

<!PDM_MACRO NAME=dtlDropdown hdr="Status" attr=status lookup=no
evt="onBlur=\\\"detailSyncEditForms(this)\\\"">
<!PDM_MACRO NAME=dtlDropdown hdr="Priority" attr=priority lookup=no
evt="onBlur=\\\"detailSyncEditForms(this)\\\"">

</PDM_IF>
```

Predefined Macros Used by WSP

This article contains the following topics:

- Menubar Macros (see page 1773)

CA SDM includes a number of predefined macros. Most of these macros insert JavaScript text to create an element on a web form. Use Web Screen Painter to create and modify forms using these macros.

Detail Form Macros

The following list describes the Detail Form macros:

- **button**
  Inserts a graphic button.
- **dtlCheckbox**
  Inserts a check box on a detail form.
- **dtlDate**
  Inserts a date field on a detail form.
- **dtlDateReadonly**
  Inserts a read-only date field on a detail form.
- **dtlDropdown**
  Inserts a drop-down list on a detail form.
- **dtlEnd**
  Ends a detail form.
- **dtlEndTable**
  Ends a table within a detail form.
- **dtlForm**
  Begins a detail form.
- **dtlHTMLEditBox**
  Inserts a detail form field that is a text box containing an HTML editor.
- **dtlHier**
  Inserts a detail form field that is a text box validated against an external table with a hierarchical lookup.

  Important! We recommend that you do not change the dtlHier macro to dtlLookup in the HTMPL file. Use the Options Manager suppress_web_hier_search option instead so that autocomplete works correctly.

- **dtlLookup**
  Inserts a detail form field that is a text box validated against an external table.
- **dtlLookupReadonly**
  Inserts a detail form field that is a read-only hyperlink to an external table.

- **dtlReadonly**
  Inserts a read-only text field on a detail form.

- **dtlStart**
  Begins the first table in a detail form.

- **dtlStartExpRow**
  Begins an expandable row on a detail form.

- **dtlStartRow**
  Begins a normal row on a detail form.

- **dtlTextbox**
  Inserts a text box on a detail form.

contactLookup

The contactLookup macro creates a contact lookup. This macro has the following arguments:

```
contactLookup("&{header}","&{frameName}","&{factory}","&{lookupName}");
```

- **header**
  Identifies the lookup header.

- **frameName**
  (Required) Identifies the form name.

- **factory**
  Specifies the factory.
  Default: agt

- **lookupName**
  (Required) Identifies the lookup name.

You can also enable and disable this element by using the following:

```
contactLookupDisable( Name, bDisable )
```

- **bDisable=**

- true
  Disables the element.

- false
  Enables the element.

dtlCheckboxReadonly

The dtlCheckboxReadonly macro specifies a readonly checkbox field on an HTMPL detail form. The macro has the following arguments:

```
detailCheckboxReadonly("&{hdr}","&{attr}",&{colspan},"$args.&{attr}", "&{on}", "&
{off}");
```

- **hdr**
  Specifies the text of the header.
  Default: "$args.&{attr}.DISPLAY_NAME"

- **attr**
  (Required) Specifies the name of the attribute.

- **on = "X"**
  Specifies the value shown on readonly form when field is checked.

- **off = ""**
  Specifies the value shown on readonly form when field not checked.

- **colspan = 1**
  Specifies the number of columns on the form.

On both the readonly and edit forms, the field is displayed as specified in "on" and "off" arguments.

Note: This macro is similar to dtlCheckbox.mac, except that it is always read-only, even in Edit mode.

List Form Macros

- **lsCol**
  Specifies a column in a list form.

- **lsEnd**
  Ends the list portion of a list form.

- **lsStart**
  Begins the list portion of a list form.

- **lsWrite**
  Inserts text into the repeating section of a list form.

- **sfDate**
  Inserts a date field in a search filter.

- **sfDropdown**
  Inserts a drop-down list on a search filter.

- **sfEnd**
  Ends a search filter.

- **sfHier**
  Inserts a search filter field that is a text box validated against an external table with a hierarchical lookup.

- **sfLookup**
  Inserts a search filter field that is a text box validated against an external table.

- **sfStart**
  Begins a search filter.

- **sfStartRow**
  Begins a row within a search filter.

- **sfTextbox**
  Inserts a textbox into a search filter.

Menubar Macros

The following list describes the Menubar macros:

- **endMenu**
  Ends a menu within a menu bar.

- **menuItem**
  Defines a global item on a menu.

- **endMenubar**
  Ends a menu bar.

- **menuItemLocal**
  Defines an item on a menu invoked in the context of the current window.

- **menubarItem**
  Defines a menu within a menu bar.

- **startMenu**
  Begins a menu within a menu bar.

- **startMenubar**
  Starts a menu bar.

HTMPL Tags

This article contains the following topics:

This section outlines PDM commands to add HTMPL tags.

PDM_EVAL Insert the Value of a Pre-Processor Variable

The pdm_eval tag is used to insert the value of a pre-processor variable into the input of the webengine parser. If used inside a macro, its effect is deferred until the macro completes.

The pdm_eval tag works similarly to pdm_include or pdm_macro. It inserts the text into the parser at the point of the tag, exactly as if the value of its variable had been coded in place of the tag.

pdm_eval has the following syntax:

```
<PDM_EVAL TEXT=PRE.name>
```

- **name**
  (Required) The name of the pre-processor variable whose value is to be inserted into the webengine's input.

PDM_FORM Start an HTML Form with a Session ID

<PDM_FORM> and </PDM_FORM> can be added to any web interface HTML template to create an HTML form including two hidden fields for the server variables SID (session ID) and FID (form ID). The optional OP operand creates an additional hidden field for one of the supported operations, as with the PDM_LINK tag. Except for the automatically-generated hidden fields, <PDM_FORM> and </PDM_FORM> are used in the same way as the standard HTML <form> and </form> tags (and generate these tags as part of their expansion).

PDM_FMT Format Text from a Server Variable

The <PDM_FMT> and </PDM_FMT> tags are used to format blocks of text inserted by server variables ($args.xxx) as directed by its arguments.

Note: <PDM_FMT> is ignored for literals, including $prop.xxx variables.

The following table describes these tags:

Property	Description
ESC_STYLE=**NONE** | **E** | C |	Specifies the escape type of the formatted text. Valid values are: **NONE** Default setting. Specifies that no special treatment be given to any character in the content body. **C** Give special treatment to the characters ', ", \, \r, `, and \n, which are meaningful in C

Property	Description
HTML | JS | JS2 | URL	programs. These characters will be escaped. **HTML**Give special treatment to the following characters, which are meaningful in HTML text: & becomes & ' becomes ' " becomes " < becomes < > becomes %gt; **JS**Give special treatment to the following characters, which are meaningful in JavaScript text: ' becomes %27 " becomes %22 / becomes %2F \ becomes %5C \r becomes %0D \n becomes %0A **JS2** Same as JS, but give no special treatment to the character, /, and give special treatment to two additional characters: - % becomes %25 - Line breaks are suffixed with %0A **URL** Translate all characters other than letters, digits, and '@*-_.#' to '%xx', where xx is the hexadecimal coding of the translated character.
JUSTIFY=LEFT | CENTER | RIGHT | **TRUNCATE**| WRAP | LIN	Specifies the justification of the formatted text. Valid values include: **TRUNCATE** Default setting. Eliminates HTML formatting by replacing '<' and '>' with < and > **Note:** For more information, see the following information about KEEPLINKS and KEEPTAGS. **LEFT|CENTER|RIGHT** Produces exactly WIDTH characters, truncated or padded with spaces as necessary, with any embedded new lines replaced by a single space, and the output text delimited by [set the pre variable for your book] and </pre> tags. The WIDTH argument must be specified as a positive integer. **WRAP** Same as LEFT, except that text wrapping honors word boundaries (line breaks are not placed within words). **LINE** Same as TRUNCATE, except that it also replaces all embedded line breaks with tags.
KEEPLINKS=YES| **NO**	If KEEPLINKS=YES is specified, the action of JUSTIFY=LINE or JUSTIFY=TRUNCATE is modified to preserve HTML anchor tags (Action:) while converting all other '<' and '>' characters. Mutually exclusive with KEEPTAGS.
KEEPNL=YES|**NO**	The normal action of PDM_FMT is to convert all embedded new lines and any following spaces to a single space. If KEEPNL=YES is specified, embedded new lines are preserved. This argument is ignored for JUSTIFY=LINE.
KEEPTAGS=YES| **NO**	If KEEPTAGS=YES is specified, the action of JUSTIFY=LINE or JUSTIFY=TRUNCATE is modified to preserve all HTML tags. Mutually exclusive with KEEPLINKS.
PAD=**YES**|NO	If PAD=NO is specified, PDM_FMT does not convert empty strings to a single space. This is the normal action when WIDTH is non-zero, or JUSTIFY is TRUNCATE or WRAP.

Property	Description
WIDTH= *nn*	When non-zero, specifies that the text should be formatted to exactly WIDTH characters.

<PDM_FMT> without WIDTH or JUSTIFY does no formatting on the enclosed text, but surrounds the text with [set the pre variable for your book]and </pre>.

For example, to produce a multi-line description, enter the following:

```
<PDM_FMT WIDTH=50 JUSTIFY=WRAP>$args.description</PDM_FMT>
```

To produce multi-column output, enter the following:

```
<PDM_FMT><PDM_FMT WIDTH=20 JUSTIFY=LEFT>$cst.last_name</PDM_FMT>
 <PDM_FMT WIDTH=20 JUSTIFY=LEFT>$cst.first_name</PDM_FMT>
  <PDM_FMT WIDTH=20 JUSTIFY=TRUNCATE>$cst.middle_name</PDM_FMT>
</PDM_FMT>
```

PDM_IF Conditional Processing

These tags are used to conditionally include text. <PDM_IF> blocks can be placed anywhere in an HTMPL file - in HTML, in JavaScript, and even within HTML tags. <PDM_IF> and <PDM_ELIF> (else if) both take a simple conditional clause as their properties rather than name-value pairs. If the clause is true, the text after the tag to the closing tag is included in the file; if the clause is false, the server discards the text between the tag and the closing tag. The closing tag can be <PDM_ELIF>, <PDM_ELSE>, or </PDM_IF>.

The <PDM_ELSE> and <PDM_ELIF> tags are optional. If both are specified, all <PDM_ELIF> tags must precede <PDM_ELSE>. There can be any number of <PDM_ELIF> tags between <PDM_IF> and <PDM_ELSE> (or </PDM_IF> if <PDM_ELSE> is omitted).

The syntax of the conditional in <PDM_IF> and <PDM_ELIF> is as follows:

- 0 is false; any other number is true
- "" is false; "*any-string*" is true
- "*value op value*" evaluates the left and right values against each other according to *op*. If both values consist of digits (optionally preceded by - or +), the comparisons are done numerically. Otherwise, they are done lexically (ASCII collation). Valid *op* values include:

op Value	Description
==	Equal to
!=	Not equal to
>=	Equal to or greater than (must be written as \>= or >=)
<	Less than (must be written as \< or <)
>	Greater than (must be written as \> or >)
<=	Equal to or less than (must be written as \<= or <=)

op Value	Description
&	Performs a bit-and of the left and right values. True if any bits are set; false if none are set.
%	Returns true if the left value is an even multiple of the right value, and false otherwise (useful for building two-dimensional tables).
:	Performs a byte-oriented pattern match like the UNIX grep command. It returns true if the left value contains the regular expression defined by the right value.

Example:

```
<PDM_IF $count \>= 10> . . .
<PDM_ELIF $count &lt; 5>  . . .
<PDM_ELSE> . . .
</PDM_IF>
```

There can be more than one conditional in a PDM_IF statement. Conditionals are separated by connectors, either && (and) or || (or). There is no precedence for either connector. The web engine examines a conditional from left to right until it reaches a connector. If the initial condition is true and the connector is ||, it considers the entire condition to be true without further evaluation. If the initial condition is false and the connector is &&, it considers the entire condition to be false without further evaluation. Otherwise, it considers the condition undetermined, and evaluates the conditional from after the connector.

PDM_INCLUDE Inserting from a Different File

The <PDM_INCLUDE> tag is used to insert text from a second file into an HTMPL file. The server replaces the <PDM_INCLUDE> tag with the contents of the second file.

Included files can contain <PDM_INCLUDE> tags. There is no limit to the depth of nesting.

The <PDM_INCLUDE> tag supports the following properties:

Property	Description
FILE=filename	(Required) Specifies the file to include. The web engine searches the directories used for HTMPL files, as defined in the current user's access type.
FIXUP=[**YES**|NO]	(Optional) Indicates whether the file should be interpreted by the web interface like a normal HTML template file, such as expanding variables beginning with dollar signs ($) and interpreting other CA SDM tags, such as PDM_LIST, and PDM_FORMAT. The value YES, indicates that the file should be treated as a regular HTML template file, and the value NO means that the included file should be treated as literal text. The default is YES. **Note:** For compatibility with previous releases, the values TRUE or 1 can be substituted for YES, and the values FALSE or 0 can be substituted for NO. These values are deprecated, and should not be used in new pages.
propname=value	Specifies that property propname should have the specified value. The property's value can be accessed within the included file by prefixing propname with $prop. For example, the following specification would allow the included file to reference $prop.menubar: <PDM_INCLUDE … menubar=no> Global properties can also be specified in the web.cfg configuration file. For information

Property	Description
	about web.cfg, see How to Configure the Web Interface (see page 884). **Note:** For compatibility with previous releases, property values specified on <PDM_INCLUDE> can be referenced without the preceding 'prop.', in the form $propname. This usage is deprecated and should not be used in new pages.

PDM_JSCRIPT Conditionally Include a JavaScript File

The <PDM_JSCRIPT> tag is used to conditionally include a JavaScript file on a form. This tag has two forms:

```
<PDM_JSCRIPT file=xxxx.js [include=yes|no]>
```

Pdm_jscript with file=xxx.js specifies that JavaScript file xxx.js is required by this form. The webengine adds the file to a list of JavaScript files required by the form. Processing of the tag occurs while the form is being parsed, and is not affected by pdm_if. That is, a pdm_jscript tag referencing a file adds that file to the list of JavaScript files if it occurs anywhere in the file or in an included file, or in a macro.

The optional argument *include=no* can be specified to instruct the webengine to ignore the tag. This argument provides conditional processing for the tag, and is primarily useful when the tag is invoked in a macro. For example, the dtlTextbox macro specifies the following:

```
<PDM_JSCRIPT file=spellcheck.js include=&{spellchk}>
```

This indicates that any form containing a dtlTextbox macro that specifies spellchk=yes requires the JavaScript file spellcheck.js.

The second form of the pdm_jscript tag is the following:

```
<PDM_JSCRIPT insert=here>
```

Pdm_jscript with insert=here requests the webengine to insert standard HTML <script> tags for all required JavaScript files. The webengine processes this form of the tag during the HTML generation phase, so that it is affected by pdm_if. A pdm_jscript tag with insert=here is part of std_head_include.htmpl, so it is present on virtually every form.

Note: The webengine inserts script tags only the first time it encounters pdm_jscript insert=here.

PDM_LINK Create a Hyperlink Invoking an HTMPL Operation

<PDM_LINK> and </PDM_LINK> can be added to any web interface HTML template to create links a link that invokes an HTMPL operation. The <PDM_LINK> tag generates the standard HTML <a href=... > tag and has similar arguments, except that it allows specification of a CA SDM operation in place of a URL.

The format is as follows, where *operation* is one of the supported operations (see page 1789):

```
<PDM_LINK OP=operation> ... </PDM_LINK>
```

Example:

```
<PDM_LINK OP=MENU> Menu </PDM_LINK>
<PDM_LINK OP=CREATE_NEW FACTORY=iss> Submit Issue </PDM_LINK>
<PDM_LINK OP=LOGOUT> Logout </PDM_LINK>
```

PDM_LIST Format a List of Database Rows

The <PDM_LIST> and </PDM_LIST> tags are used to delimit repeating sections of HTML for multi-record output. Everything between <PDM_LIST> and </PDM_LIST> is repeated once for each record to be output. There are two types of PDM_LISTs:

- Lists taken from an object attribute that implies a list. For example, the properties attribute of the request object is the list of properties associated with that request. This type of PDM_LIST always has a SOURCE property.
- Lists with an explicit where clause. This type of PDM_LIST always has a WHERE property.

An object attribute <PDM_LIST> takes the following properties:

Property	Description
ESC_STYLE=**NONE** | C | HTML | JS | JS2 | URL	Specifies the escape type of the formatted text. Valid values are: **NONE**Default setting. Specifies that no special treatment be given to any character in the content body. **C**Give special treatment to the characters ', “, \, \r, ', and \n, which are meaningful in C programs. These characters will be escaped. **HTML**Give special treatment to the following characters, which are meaningful in HTML text: & becomes &' becomes '" becomes "< becomes <> becomes %gt; **JS**Give special treatment to the following characters, which are meaningful in JavaScript text: ' becomes %27" becomes %22/ becomes %2F\ becomes %5C\r becomes %0D\n becomes %0A **JS2** Same as JS, but give no special treatment to the character, /, and give special treatment to two additional characters: - % becomes %25 - Line breaks are suffixed with %0A **URL** Translate all characters other than letters, digits, and '@*-_.#' to '%xx', where xx is the hexadecimal coding of the translated character.
LENGTH=*nn*	Specifies the number of rows of output (defaults to all).
PREFIX=*prefix*	Specifies the prefix on references to attributes from records in the list. These are referenced in the form *$prefix.attr_name* in the text between <PDM_LIST> and </PDM_LIST>. The PREFIX property is optional in an object variable list. If PREFIX is omitted, the value of SOURCE is also used for the prefix.

Property	Description
SEARCH_TYPE=DISPLAY|**GET_DOB**	Specifies the method the server should use to build the list form: DISPLAY specifies the server should issue a single query for the entire form GET_DOB specifies the server should issue separate queries for each row of the form The choice affects list performance, and depends on the complexity of the list (the number of joins required to display it) and the characteristics of your DBMS. GET_DOB has more predictable performance than DISPLAY, and is the default.
SORT=*index-name*	Specifies the index name to use for sorting. The default value of this argument is DEFAULT (which means the first sort index for the underlying factory).
SOURCE=*source*	Specifies the object variable defining this list. This field is required. Do not put a dollar sign ($) in front of *source* on the PDM_LIST statement itself. If the PREFIX property is not specified, *source* is also used as the prefix for references to attributes from records on the list, in references of the form *$source.attr_name*. When used in a reference, *source* does require a preceding dollar sign.
START=*n*	Specifies the first output row (defaults to zero).

Example:

```
<table border>
<tr>
<th>Child Change Order Number</th>
<th>Summary</th>
</tr>
<PDM_LIST SOURCE=args.children>
<tr>
[assign the value for TD in your book]$args.children.chg_ref_num</td>
[assign the value for TD in your book]$args.children.summary</td>
</tr>
</PDM_LIST>
</table>
```

Because no prefix was specified, references to attributes of the listed records are prefixed by $args.children, the source value.

A where clause PDM_LIST takes the following properties:

Property	Description
FACTORY=*name*	Specifies a class of object to be searched. This property is required.
LENGTH=*nn*	Specifies the number of rows of output (defaults to all).
ORDER_BY=*attr-name*	Specify the attribute name to sort by. It can contain the DESC (descending) or ASC (ascending) modifiers.
PREFIX=*prefix*	Specifies the prefix on references to attributes from records in the list. These are referenced in the form *$prefix.attr_name* in the text between <PDM_LIST> and </PDM_LIST>. The PREFIX property is required in a where clause list.

START=*n* *n*	Specifies the first output row (defaults to zero).
WHERE=*where-clause*	Specify the where clause for the search. It can contain (dotted) attributes. This property is required.

For example:

```
<table>
<tr>
<th>Child Change Order Number</th>
<th>Summary</th>
</tr>
<PDM_LIST PREFIX=list FACTORY=chg WHERE="status = 'OP'">
<tr>
[assign the value for TD in your book]$list.chg_ref_num</td>
[assign the value for TD in your book]$list.summary</td>
</tr>
</PDM_LIST>
</table>
```

PDM_NOTEBOOK Create a Notebook

Several of the forms in the CA SDM analyst interface use nested tabs (notebooks). Nested tabs display several sets of fields in the same physical area of the screen, with only one set visible at a time. The user selects the set of fields that is visible by clicking a named tab at the top of the notebook, or by pressing the access key combination Alt+*n*, where *n* is the number of the tab. An example of a form using a notebook is the Issue Detail (detail_iss.htmpl). We recommend that you use WSP to modify the contents of notebooks, or insert a notebook into a form that does not already contain one.

The following tag marks the end of a notebook:

```
<PDM_MACRO name=endNotebook>
```

PDM_PRAGMA Specify Server Information

The <PDM_PRAGMA> tag is used to specify information used by the web engine, such as form release and version. It does not generate any HTML code, and can be placed anywhere in a form. Possible arguments are:

Argument	Description
RELEASE=value	Specifies the CA SDM release number corresponding to this form. This value is “110” on all CA Service Desk Manager r11.0 forms. It is accessible within the form in the $prop.release variable.
SITEMOD=value	Specifies a site-defined string identifying the modifications applied to this form. It is accessible within the form in the $prop.sitemod variable.
VERSION=value	Specifies a CA Technologies-defined string identifying the version number of this form. It is accessible within the form in the $prop.version variable.

Argument	Description
OVERIDE=YES|**NO**	Specifies whether or not values in this PDM_PRAGMA statement override values in previous PDM_PRAGMA statements.

CA Technologies uses PDM_PRAGMA statements to document form versions. All CA Service Desk Manager r11.0 forms include the following PDM_PRAGMA statement:

```
<PDM_PRAGMA RELEASE=110>
```

In addition, the std_head.htmpl form includes the following JavaScript statement:

```
cfgFormRelease = "$prop.release" - 0;
```

The PDM_PRAGMA statement and the cfgFormRelease variable allows the CA SDM web interface to distinguish CA Service Desk Manager r11.0 forms from previous release forms. Releases prior to CA Service Desk Manager r6.0 did not support the PDM_PRAGMA statement.

Normally, only PDM_PRAGMA statements in the highest-level file of a form (that is, a file not brought in by PDM_INCLUDE) are used to set $prop.release, $prop.sitemod, and $prop.version. In addition, a PDM_PRAGMA statement will not override a non-empty value set by a previous PDM_PRAGMA statement. You can specify OVERRIDE=YES to specify that a PDM_PRAGMA statement can override previous PDM_PRAGMA statements, or that a PDM_PRAGMA statement in an included file can be used.

PDM_SCOREBOARD Build a Scoreboard Tree

The <PDM_SCOREBOARD> tag is used to generate the scoreboard shown on the left side of the main form. It takes the following property:

- **TARGET=*value***
  Specifies the name of the target frame for lists requested by clicking a node on the scoreboard. Lists are loaded into the target specified, which can be any value supported for the target attribute of a link. The default value is *_self* (the window containing the PDM_SCOREBOARD tag).

Any HTMPL form including a <PDM_SCOREBOARD> tag must also include the fldrtree.js JavaScript file. This file can be included with the following statement in <HEAD> section of the form:

```
<SCRIPT LANGUAGE="JavaScript" SRC="$CAisd/CAisd/fldrtree.js"></SCRIPT>
```

In addition, it is desirable to include a link with the name scoreboard_asof_data to display the effective date of the numbers in the tree. See the distributed file scoreboard.htmpl for an example of the use of this tag.

The queries included on the scoreboard are defined by the contents of the User_Query table (object name usq) for the current user. A record in this table defines each line on the tree (folder or node).

Initially, users have no entries in their User_Query table. A user with no User_Query entries receives the default set of scoreboard queries associated with their access type. A user with administrative authority can also customize the default scoreboard for an access type.

PDM_SET Set the Value of a Server Variable

The <PDM_SET> tag is used to assign a value to a server variable. It has the following syntax:

```
<PDM_SET arg.name[+]=value>
```

- **arg**
  (Required) Specifies the variable type, and must be arg for normal use.

  > **Note:** There is no $ character.

- **Name**
  (Required) Specifies the name of the variable.

- **+**
  (Optional) Specifies that the value should be appended to the existing value of the variable. There cannot be any spaces before or after.

- **=**
  (Required) Must be specified exactly as shown, with no spaces before or after.

- **value**
  (Required) Specifies the text to be assigned or appended to the variable.

The PDM_SET tag can also be used in the preprocessor phase to create or update a preprocessor variable.

PDM_TAB Create a Tab within a Notebook

The <PDM_MACRO name=startNotebook hdr=cng_nb> tag is used to define a notebook tab. We recommend that you use WSP to modify the contents of notebooks, or insert a notebook into a form that does not already contain one.

PDM_WSP Control WSP Preview

The <PDM_WSP> tag is used to control the WSP preview feature. It does not generate any HTML code, and can be placed anywhere in a form.

By default, WSP determines how to preview a form by examining the form name:

- For detail forms (names of the form detail_*factory*.htmpl), WSP displays the form in edit view, with data from the most recently created row of the appropriate table. If there is no data you are allowed to view in the table, WSP displays the form set up to create a row. WSP preview sessions are typically prohibited from updating the database. WSP displays forms in edit view to allow you to preview all features. However, CA SDM ignores a Save request from a read-only preview session. The web engine changes the text on the Save button to noSave as a visual reminder of this.

- For list forms (names of the form list_*factory*htmpl), WSP displays the form in list view, with the list displaying data from the most recently created row of the appropriate table. If there is no data you are allowed to view in the table, WSP displays the form in search view, with the filter open.

- For other forms, WSP displays the form with no database context.

You can change this default behavior by placing a PDM_WSP tag anywhere on the form. For example, you can display a notebook tab form on its associated detail form, or provide prerequisite arguments for forms normally invoked with an environment provided by another form. Possible arguments are the following:

Property	Description
FACTORY=*value*	Specifies the Object Engine factory used by this form.
PREVIEW=*name*.htmpl | *value* | no	Specifies the preview URL. This can be an HTMPL file name, in the form xxxx.htmpl; a CA SDM URL (used unaltered if it begins with “OP=”); or the keyword “no”, indicating the form cannot be previewed. A value not beginning OP= is modified by replacing a reference of the form {*factory*} or {*factory*:} with an ID or persistent ID (respectively) of the most-recently created row from the referenced factory that the current user is authorized to view.
WHERE=*value*	Specifies a where clause used to search for a representative row or rows to show on the previewed form.
MODE=*value*	Specifies the mode of the constructed URL. Can be the following: GENERAL. General format. Determine the mode by examining the preview argument: detail_xxxx.htmpl - READONLY list_xxxx.htmpl - LIST any other - GRONK READONLY. Detail file in read-only view. EDIT. Detail file in edit view. LIST. List file. GRONK. Unspecified file. In this situation, gronk the file.

Server Variables

This article contains the following topics:

CA SDM information is included in the HTML template using variables beginning with a dollar sign ($). Each page is created with some variables that are documented in the template file. These variables can be put on the page or used in conditional statements:

- Simple Variables

- Property Variables
- Environment Variables
- Business Object Variables
- List Variables

Simple Variables

Simple variables specify flags that are passed to the web page. To access a simple variable, use the variable name preceded by a dollar sign ($). This makes the value of the variable available. For example, two such variables are $CAisd and $cgi. Putting $CAisd in a template results in the substitution of the main CA SDM web server installation directory, whereas $cgi refers to the URL of the pdmweb.exe program. Simple variables are documented in the upper section of the HTMPL file that uses them.

The following shows a list of variables that can be used in all the HTMPL files:

- **$ACCESS.*group***
  The user access privilege object contains the privilege settings on the function group *group* for the current login user. For example, $ACCESS.admin holds the privilege value for the admin functional group. Valid privilege values are:
  - 0-NO ACCESS
  - 1-VIEW
  - 2-MODIFY

  This variable is not available in the login form.
- **$cgi**
  The URL of the pdmweb.exe program.
- **$cst**
  The data object of the current login user. This variable is not available in the login form. You can reference individual attributes of this object with the form $cst.*attrname*; for example, $cst. first_name.
- **$CAisd**
  The URL of main CA SDM web server installation directory.
- **$MachineName**
  The MachineName defined in the web.cfg file.
- **$ProductName**
  The product name defined in the NX.env file.
- **$SESSION**
  The session object saves all session variables including session ID ($SESSION.SID) and all variables defined in the web.cfg file.

- **$USER_STATE**
  User-defined state information.

Property Variables

Property variablesrepresent a property of the configuration file, web.cfg. You can access any entry in the web.cfg file (including user-defined entries) within an HTML template file by prefixing it with "$prop."

For example, one of the lines in web.cfg, which specifies the number of entries displayed in a single page on a list form is as follows:

```
ListPageLength 10
```

You can refer to this variable in an HTML template with the specification:

```
$prop.ListPageLength
```

If you use the <PDM_INCLUDE> special tag to incorporate another file into a template file, you can specify additional properties as attributes of the <PDM_INCLUDE> tag. You can reference these properties in the included file in the same way as web.cfg properties. A property specified as a <PDM_INCLUDE> attribute that has the same name as a web.cfg property overrides the web.cfg property within the included file.

For example, the following <PDM_INCLUDE> tag creates a property called $prop.menubar that can be referenced within the std_body.htmpl file:

```
<PDM_INCLUDE FILE=std_body.htmpl menubar=no>
```

Note: You can refer to configuration file property *xxx* in two ways: $prop.*xxx* or *$SESSION.xxx*. Both return the same value. However, the $prop.*xxx* syntax is preferred because it involves less server overhead.

In addition to properties from web.cfg, there are several predefined properties that can be accessed with $prop. These are:

- **$prop.browser**
  A string identifying the browser in use. This will be "IE" for Internet Explorer.

- **$prop.combo_name**
  A string containing the current user's name, in the form "last_name, first_name middle_name."

- **$prop.factory**
  A string containing the factory associated with the current form, such as "cr" for requests or "iss" for issues.

- **$prop.FID**
  A string containing the numeric form ID of the current form.

- **$prop.form_name**
  A string containing the name of the current HTML template, in the form *xxx*.htmpl.

- **$prop.form_name_1**
  A string containing the substring of the form name before the first underscore. For example, for the form detail_chg_edit.htmpl, form_name_1 would be “detail.”

- **$prop.form_name_2**
  A string containing the substring of the form name after the first underscore and before the last underscore (or dot). For example, for the form detail_chg_edit.htmpl, form_name_2 would be “chg.”

- **$prop.form_name_3**
  A string containing the substring of the form name after the last underscore and before the dot. For example, for the form detail_chg_edit.htmpl, form_name_3 would be “edit.” For the combination detail form, which has a file name of the form detail_*xxx*.htmpl, $prop. form_name_3 is set to the current view, either “ro” or “edit”.

- **$prop.release**
  A string containing the release level of the form. The PDM_PRAGMA statement contains more details on this property.

- **$prop.SID**
  A string containing the numeric session ID of the current session.

- **$prop.sitemod**
  A string containing the site-defined modification name of the form. The PDM_PRAGMA statement contains more details on this property.

- **$prop.user_type**
  A string containing “analyst,” “customer,” “employee,” or “guest.”

- **$prop.version**
  A string containing the version of the form. The PDM_PRAGMA statement contains more details on this property.

Environment Variables

Environment variablesrepresent an entry within the NX.env configuration file. You can reference any entry in NX.env within an HTMPL template file by prefixing it with “$env.”

For example, one of the lines in NX.env, which specifies the host name of the CA SDM server is as follows:

```
@NX_SERVER=hostname
```

You can refer to this variable within an HTMPL template file with the specification:

```
$env.NX_SERVER
```

Business Object Variables

Businessobject variablesrepresent a CA SDM object, such as an issue or a request. To access an object, you need to start with the variable name, followed by a period (.), followed by whatever attribute names you want to display. For example, on an issue where, by convention, the object is represented by the variable args, you can display the description, the open date, the assignee's phone number, the number of activities on the issue, and the description of the first activity, as shown by the following:

```
$args.description
$args.open_date
$args.assignee.phone_number
$args.act_log.length
$args.act_log.0.description
```

You can use braces to delimit the variable name if it is not surrounded by white space. For example, $foo bar and ${foo}bar are both valid. You can also use the variable args to access non-attribute values (for example, $args.KEEP.*name* as described in Supported Operations (see page 1789)).

It is possible that a non-attribute variable may not be defined. For example, it may be possible to get to a form from two different places, only one of which provides a value for $args.KEEP.foo. You can provide a default value for a $args reference with the following syntax, where the string after the colon is substituted for the reference if *variable* is undefined:

```
${args.variable:default}
```

- **Time Zone Date Variables**
  Time zone date variables are a special case of business object variables. They provide a means to convert universal dates (UTC) represented as integers to string dates adjusted for the time zone of the user's browser. The variable for representing integer dates is:

  ```
  $args.attr_name_INT_DATE
  ```

  Example: $args.open_date_INT_DATE

- **Factory Data Variables**
  Factory data variables are a special case of business object variables. A factory data variable is replaced by information about a referenced object. There are seven such variables available:

  - **$args.*attr_name*.COMMON_NAME**
    The common name (externally readable string) of the table referenced by the attribute. For example, on the Request Detail form, the value of $args.assignee.COMMON_NAME is the assignee's combo name (“last, first, middle”).

  - **$args.attr_name.COMMON_NAME_ATTR**
    The attribute name of the common name in the table referenced by the attribute. For example, on the Request Detail form, the value of $args.assignee.COMMON_NAME_ATTR is “combo_name”.

  - **$args.FACTORY_*attr_name***
    The name of the factory associated with the specified attribute. For example, on the Request Detail form, the value of $args.FACTORY_assignee is “agt”.

- **$args.LENGTH_*attr_name***
  The maximum length of the attribute. For example, on the Request Detail form, the value of $args.LENGTH_summary is 240.

- **$args.*attr_name*.REL_ATTR**
  The rel attr (foreign key) of the attribute. For example, on the Request Detail form, the value of $args.assignee.REL_ATTR is the value of the assignee's ID field.

- **$args.*attr_name*.REL_ATTR_ATTR**
  The attribute name of the rel_attr in the table referenced by the attribute. For example, on the Request Detail form, the value of $args.assignee.REL_ATTR_ATTR is “id”.

- **$args.REQUIRED_*attr_name***
  A string, either “0” or “1” indicating whether the referenced attribute is required.

- **$args.*attr_name*.SELECTIONS**
  A list of valid selections for *attr_name*. This value is an empty string if *attr_name* is not a reference to another table, or if the size of table referenced by *attr_name* exceeds the value of the configuration file property SelListCacheMax. Otherwise, the SELECTIONS variable is a string containing the common name and rel attr of all the entries in the referenced table. Successive values are separated by the string “@,@”, so the variable's value has the form: "cname1@,@rel_attr1@,@cname2@,@rel_attr2"

- **$args.*factory*_SEL_UNDER_LIMIT**
  A string, either “0” or “1”, indicating whether the current number of rows in the table corresponding to *factory* is less than the value of the configuration file property SelListCacheMax. This variable is deprecated in favor of the SELECTIONS variable, which should be used in all new forms.

Factory data variables containing a dotted reference (COMMON_NAME, REL_ATTR, and SELECTIONS) can be used with a dotted reference of any length. For example, on a Request Detail form $args.assignee.organization.COMMON_NAME is replaced by the external name of the assignee's organization.

List Variables

List variables are used to iterate through data. They are accessed using list tags as described in PDM_LIST: Format a List of Database Rows (see page 1779).

Supported Server Operations

This article contains the following topics:

The following operations are supported to let you integrate the CA SDM web pages with your web pages:

- **CREATE_NEW**
  Provides a generic interface to let the user create a row in a specified table. The object name must be specified, and by default a template named *detail_xxx*_edit.htmpl is used for object *xxx*. You can override the .htmpl file by specifying the HTMPL property.

  - **Required specifiers:**
    FACTORY=*object-name*

  - **Optional specifiers:**
    ALG_PRESET=*preset_expressionALG_PRESET_REL=preset_expression*CREATE_ALG=*activity_log_type*HTMPL=zdetailxxx*_factory*.htmplKEEP.*attr_name=value*PRESET=*preset_expression*PRESET_REL=*preset expression*SET.*attr_name=value*use_template=1 | 0 (0 is the default)

  Note: To use the HTMPL specifier with CREATE_NEW, the referenced form must have a name conforming to the naming convention zdetailxxx*_factory*.htmpl. The name must begin with the string zdetail, followed by any alphanumeric characters (including a null string), followed by an underscore and the factory name.

- **ENDSESSION or LOGOUT**
  Ends the current logged-in session. ENDSESSION is the preferred operation.

- **GENERIC_LIST**
  Provides a generic interface to allow the user to display a list from any table in the database. The object name must be specified, and by default a template named list*_xxx*.htmpl is used for object *xxx*. You can override the .htmpl file by specifying the HTMPL property.

  - **Required specifiers:**
    FACTORY=*object-name*KEEP.*attr_name=value*

- **DISPLAY_FORM**
  Provides a generic interface to let the user display any customized form.

  - **Required specifiers:**
    HTMPL=*htmpl_file*

  Note: DISPLAY_FORM replaces JUST_GRONK_IT. Existing implementations can continue to use JUST_GRONK_IT, which functions exactly like DISPLAY_FORM. DISPLAY_FORM is the preferred operation.

- **MENU**
  Displays the main menu page, which is defined in the web.cfg file in the Menu property.

  - **Optional specifiers:**
    HTMPL=*menufile*
    menufile is the name of an alternate main menu file.

- **PAGE_EXTENSION**
  Allows the webmaster to specify additional extensions to the interface.

  - **Required specifiers:**
    NAME=*html_file*
    html_file is one of the file names listed in the configuration file UserPageExtensions directive.

  - **Optional specifiers:**
    REQUIRES_LOGIN=1
    If present, a login page appears first if the user is not currently logged in. If omitted or set to zero, the file is shown without checking if the user is currently logged in.

- **RELOG**
  Displays the login page.

- **SEARCH**
  Provides a generic interface to allow the searching of any table in the database. This operation assumes that an appropriate search_*xxx*.htmpl has been created, where *xxx* is the *object-name*, as defined in the .maj files in the majic directory in bopcfg.

  Note: For more information, see CA Service Desk Manager Reference Commands (see page 3496). By default, the results of this search are displayed in list_*xxx*.htmpl, but this can be overridden by specifying the HTMPL property.

  - **Required specifiers:**
    FACTORY=*object-name*QBE.*op.attr_name=value*

  - **Optional specifiers:**
    ALG_PRESET=*preset_expression*ALG_PRESET_REL=*preset_expression*CREATE_ALG=*activity_log_type*HTMPL=*list_htmpl_file*KEEP.*attr_name=value*

- **SEC_REFRESH**
  Refreshes the user access information from the security subsystem. A hyperlink for this operation is provided to users who have MODIFY privileges (for the admin functional group) on the menu screen. After updating user access privileges with the security program, this operation provides a means to refresh access information. (This operation refreshes the security information for all users.)

  Note: Security refresh is an asynchronous process. When the security refresh is done, a message shows in the standard log file (stdlog).

- **SET_MENU**
  The behavior of this operation is the same as MENU when MENU is used with the HTMPL variable. The only difference is that this operation also sets the default menu form to the menu form specified with the HTMPL property.

  - **Required specifiers:**
    HTMPL=*htmpl_file*

Note: This operation overrides the MENU set in the web.cfg until the web service is restarted.

- **SHOW_DETAIL**
  Provides a generic interface to allow the user to display a read-only detail of a row in a specified table. The persistent ID name must be specified (from which the object name is inferred). By default, a template named detail_*xxx*_ro.htmpl is used for object *xxx*. The .htmpl file can be overridden by specifying the HTMPL property.

  - **Required specifiers:**
    PERSID=*persistent-id*

  - **Optional specifiers:**
    ALG_PRESET=*preset_expression*ALG_PRESET_REL=*preset_expression*CREATE_ALG=*activity_log_type*HTMPL=*readonly_detail_htmpl_file*

- **UPDATE**
  Provides a generic interface to editing any table. The ID and object name must be passed in and a detail form that the user can edit is displayed to the user. By default, the user has exclusive access to the record for two minutes, and is guaranteed to get changes into the database if they are submitted in this time.

  - **Required specifiers:**
    PERSID=*persistent-id* orSET.id=*id-of-row-to-update* FACTORY=*object-name*

  - **Optional specifiers:**
    NEXT_PERSID=*persistent-id* (of record to display after successful update)KEEP.*attr_name=value*KEY.*attr_name=value*HTMPL=zdetailxxx_*factory*.htmpl

Note: To use the HTMPL specifier with UPDATE, the referenced form must have a name conforming to the naming convention zdetailxxx_*factory*.htmpl. The name must begin with the string “zdetail”, followed by any alphanumeric characters (including a null string), followed by an underscore and the factory name.

Note: For information about web.cfg, see How to Configure the Web Interface (see page 884).

Operation Variables

This table lists the variables that can be set for each of the operations in the supported operations:

Variables	Description	Operations
ALG_PRESET ALG_PRESET_REL	Specifies values for one or more of the attributes of the activity log created as a result of the CREATE_ALG variable. If CREATE_ALG is not specified, ALG_PRESET and ALG_PRESET_REL are ignored.	CREATE_NEWSEARCHSHOW_DETAIL
CREATE_ALG	Specifies the activity log type of an activity log to be created as a side effect of the operation. Use the ALG_PRESET or ALG_PRESET variables to specify values for the attributes of the new activity log. The timing of creation of the activity log depends on the operation, as follows: **CREATE_NEW**The activity log is created when the new record is saved. If the new record is not saved, no activity log is created. **SEARCH**The activity log is created when a record is selected from the list form. If the record is viewed instead of selected (that is, the user explicitly selects the View command from the list form's mouse-over menu), no activity log is created. **SHOW_DETAIL**The activity log is created before the record is displayed.	CREATE_NEWSEARCHSHOW_DETAIL
FACTORY	Specifies the class of object to be searched, created, or updated. You can use any name specified as an OBJECT in the *.maj files in $NX_ROOT /bopcfg as listed in CA Service Desk Manager Reference Commands (see page 3496).	CREATE_NEWGENERIC_LISTSEARCHUPDATE
HTMPL	Allows the HTMPL author to override the default template naming convention and explicitly specify the HTMPL file to display, instead of the default template. **Note:** When the HTMPL specifier is used with CREATE_NEW or UPDATE, the name of the referenced form must conform to the naming convention zdetailxxx_factory.htmpl, where xxx are any characters, and *factory* is the factory name.	CREATE_NEWDISPLAY_FORMJUST_GRONK_ITMENUSEARCHSET_MENUSHOW_DETAIL UPDATE
KEEP.*name*	Specifies the value that can be saved and passed between pages.	CREATE_NEWGENERIC_LISTSEARCHUPDATE
KEY.*attr_name*	Similar to the SET.*attr_name*, except that this specifies a lookup on *attr_name*, which must be a reference to another table or object.	UPDATE
NEXT_PERSID	Specifies the persistent ID of the record to be displayed next.	UPDATE
PERSID	Specifies the persistent ID of a record to be displayed. You can specify this in either of the following ways: Directly, with a persistent ID consisting of a factory name, a colon (:), and a unique integer database ID. For example, PERSID=chg:1234, specifies the change order with database ID 1234. Indirectly, with a persistent ID consisting of a factory name, a colon (:), an attribute name, a second colon (:), and a value. This form of PERSID specifies the record of the specified factory that has an attribute of the specified value. For example, PERSID=chg:chg_ref_num:demo:3 specifies the change order with reference number demo:3.	SHOW_DETAILUPDATE
PRESET PRESET_REL	Specifies values for one or more of the attributes of the record created as a result of the CREATE_NEW variable. If CREATE_NEW is not specified, PRESET is ignored.	CREATE_NEW
		SEARCH

Variables	Description	Operations
QBE.*op*.*attr_name*	Specifies the values to use when performing a search. These values are identified using a QBE keyword, where *attr_name* identifies any attribute name on a ticket that can be set and *op* indicates to search where the attribute: EQ is equal to the value NE is not equal to the value GT is greater than the value LT is less than the value GE is greater than or equal to the value LE is less than or equal to the value NU is null NN is not null IN matches the SQL LIKE expression KY contains the text entered If you do not define any QBE variables, the standard search window is displayed.	
SET.*attr_name*	Specifies an attribute name to use when a ticket is created, where *attr_name* identifies any attribute in a ticket that can be set. The attribute names will vary depending on the underlying object. All objects and their attributes can be found in the *.maj files in the majic directory in bopcfg as listed in CA Service Desk Manager Reference Commands (see page 3496).	CREATE_NEWUPDATE
SET.*id*	Specifies the database ID of the row to be updated.	UPDATE
SKIPLIST	When set to 1, searches that result in 1 hit do not display the search result list. Instead, the read-only detail is displayed directly.	SEARCH
use_template	When set to 1, the SEARCH operation will return a list of templates. The returned template selected will be used in the CREATE_NEW operation to populate a new record. This variable is valid for change orders, issues, and requests.	CREATE_NEWSEARCH

Syntax of PRESET, PRESET_REL, ALG_PRESET, and ALG_PRESET_REL

The PRESET, PRESET_REL, ALG_PRESET and ALG_PRESET_REL keywords in the URL specify initial values for attributes of the ticket and its activity log, respectively. There are two possible formats:

- **[ALG_]PRESET=*attr*:*value***
  Indicates that the specified attribute of the ticket or activity log should be set to the specified value. For example, the following specification sets the description of the new ticket to “Hello:”

```
PRESET=description:Hello
```

- **[ALG_]PRESET_REL=attr:obj.relattr:testattr:value**
  Indicates that the specified attribute of the ticket or activity log should be set to a value copied from another database table. The value is copied from the *relattr* attribute of the *obj* whose *testattr* has the specified *value*. For example, the following specification sets the analyst attribute

of the new ticket to the ID of the contact with user ID xyz123:
PRESET_REL=analyst:cnt.id:userid:xyz123
When this format is used, the implied query must retrieve a unique record. If more than one contact has a user ID of xyz123 (or none), the example PRESET specification has no effect.

The PRESET, PRESET_REL, ALG_PRESET and ALG_PRESET_REL keywords can occur as many times as desired in a URL, allowing the setting of multiple attributes. Alternatively, a single keyword operand can specify multiple values separated by @@. If the '@@' separator is used, you cannot mix value formats for [ALG_]PRESET and [ALG_]PRESET_REL keywords. For example, the following example shows two different ways of specifying values for ticket description, summary and analyst:

```
PRESET=description:Hello+PRESET=summary:HelloThere+PRESET_REL=analyst:cnt.id:userid:
xyz123
PRESET=description:Hello@@summary:HelloThere+PRESET_REL=analyst:cnt.id:userid:xyz123
```

For requests, issues, incidents, problems, and change orders, both PRESET and PRESET_REL support a keyword attribute ASSET to link an object to an asset. The ASSET attribute updates the affected_resource attribute of a request, incident, or problem, or the asset LREL of an issue or change order.

Link Examples

The following link examples do not include the path to CA SDM. All CA SDM URLs begin with coding of the following form:

http://*hostname*[:*port*]/CAisd/pdmweb.exe

In this example, *hostname* is the name of your server and *port* (optional) is the port number if you are using Tomcat. This coding is shown as an ellipsis (...) in the following URL examples:

- To create a request with an affected end user with the userid tooda01, use the following example URL:

  ```
  ...?OP=CREATE_NEW+FACTORY=cr+PRESET_REL=customer:cnt.id:userid:tooda01
  ```

- To display a list of all requests assigned to userid tooda01, use the following example URL:

  ```
  ...?OP=SEARCH+FACTORY=cr+QBE.EQ.assignee.userid=tooda01
  ```

- To display the detail form for request 1234, use the following example URLs:

  ```
  ...?OP=SHOW_DETAIL+FACTORY=cr+PERSID=cr:ref_num:1234 (read-only view)

  ...?OP=UPDATE+FACTORY=cr+PERSID=cr:ref_num:1234 (update view)
  ```

Note: You can bypass the logon challenge by using Web Services for authentication. For information about the getBopsid() method, see CA Service Desk Manager Reference Commands (see page 3496).

Advanced Modifications

This article contains the following topics:

You must be aware of various aspects of modifying web pages if you elect to use tools other than Web Screen Painter to modify HTMPL, or if you have unusually complex customization requirements. However, we strongly recommend that you work with WSP to modify CA SDM web pages before trying any other approach. WSP is capable of doing almost any modification you need, and it automatically handles housekeeping issues, such as placing updates in the site mods directory, and distributing published files to all servers.

The Web Engine and Its Cache If you decide to create version any

When modifying web pages, it is helpful to understand the structure of the CA SDM web server. The web interface uses either a J2EE servlet container, such as Tomcat, or a standard HTTP server, such as Apache or Microsoft Internet Information Server (IIS). When a user requests a CA SDM web page, the HTTP server invokes the supplied program pdmweb.exe.

After it starts, pdmweb.exe sets up a connection with a CA SDM daemon (or Windows service) called the web engine. The web engine interprets the user's request. Most requests require the web engine to look up a template (HTMPL) file and translate it into standard HTML. Usually, the translation process requires the web engine to communicate with a CA SDM server to read or update the database, and include database information in the generated HTML. After the HTML is complete, the web engine sends it to pdmweb.exe, which in turn sends it back to the user's browser.

To maximize performance, the web engine typically reads each HTMPL file only once. After parsing the file and determining how to translate it to HTML, the web engine stores the parsed file in its cache, significantly reducing the processing time the next time the file is requested. While the cache is beneficial in a production environment, it can be inconvenient in development, as it means that changes to HTMPL files do not take effect until either the web engine is recycled or the pdm_webcache utility is used. In a development environment, you can avoid this behavior by specifying the configuration file property SuppressHtmplCache. However, we recommend that you do not suppress the HTMPL cache in a production environment because it severely impacts overall performance of the web engine.

The web pages served up by pdmweb.exe are generated by reading HTMPL files and using them to generate HTML. HTML template files are identified by a file suffix of .htmpl. You can modify these template files, and thereby modify the CA SDM web pages.

The pdm_webcache Utility

Use the pdm_webcache utility to remove one or more HTMPL forms from the web engine cache. This forces the web engine to fetch these forms from the disk the next time they are used, allowing changes to forms to take effect.

```
pdm_webcache [-f form-name] [-g form-group] [-i interface] [-p process] [-v]
```

- **-f *form-name***
  Specifies the name of the form to be removed from the cache, such as detail_cr.htmpl. You can use '%' (or '*') as a wildcard character to select more than one form. For example, the specification:
  -f detail%
  selects all detail forms.
  This argument is optional. If it is omitted, all forms in the cache are selected.

- **-g *form-group***
  Specifies the name of the form group to be removed from the cache, such as Analyst. You can use '%' (or '*') as a wildcard character to select more than one form group**.** For example, the specification:
  -g Anal%
  selects all form groups beginning with "Anal".
  This argument is optional. If it is omitted, all form groups in the cache are selected.

- **-i *interface***
  Specifies the name of the web interface to be removed from the cache, such as analyst, customer, or employee. You can use '%' (or '*') as a wildcard character. For example, the specification:
  -i a%
  selects the analyst interface.
  This argument is optional. If it is omitted, all interfaces in the cache are selected.

- **-p *process***
  Specifies the name of the web engine process whose cache is to be modified, such as web:local.
  This argument is optional. If it is omitted, all web engines are selected.

- **-v**
  Specifies verbose output. When this argument is specified, pdm_webcache lists the full name of every form removed from the cache, in the form:
  interface:*form-group*:*form-name*
  This argument is optional. If it is omitted, pdm_webcache reports only a count of forms removed from each web engine's the cache.

How to Modify HTML Templates

Typically, you can make two types of changes to the HTML templates:

- You can make modifications that will be visible to the user but will not be altered by the web interface prior to display. For example, you could add a GIF file for your company logo to the web interface pages (a “pass through”) by adding the reference to the appropriate template file or you could add JavaScript to your page to validate input. Any changes you make to the HTMPL file that are not contained within a PDM tag, as defined in the following, are passed unchanged in the HTML returned to the user.

- You can modify the replaceable sections of the templates. For example, you can add new application data to the request detail page.

Several kinds of template entries let you do the following:

- Display information from CA SDM to the user.

- Set up a query page.

- Create links to other CA SDM pages using link tags.

Files That Should Not be Modified

Certain HTMPL templates and JavaScript files contain information required by many CA SDM web forms. The information in these templates is both release dependent and critical to the successful operation of the CA SDM web interface. Therefore, these files are always replaced when a new version of CA SDM is released; changes made to them are not upgraded.

The templates affected by this restriction are as follows:

- **ahdtop.htmpl**
  Contains styles, scripts, and JavaScript variables used throughout the CA SDM web interface. This file is part of the main frameset of the web interface, and is always present during a session. All CA SDM forms have access to the JavaScript variable ahdtop that references the window containing ahdtop.htmpl.

- **menu_frames.htmpl**
  Defines the HTML frameset used by the CA SDM main form.

- **msg_cat.js**
  Contains the text of all messages used in CA SDM JavaScript files.

- **reports.htmpl**
  Contains data required for web reports.

- **std_body.htmpl**
  Contains standard information used at the beginning of the BODY section of most HTMPL templates.

- **std_footer.htmpl**
  Contains standard information used at the end of the BODY section of most HTMPL templates.

- **std_head.htmpl**
  Contains standard information used at the beginning of the HEAD section of almost all HTMPL templates.

- **styles.htmpl**
  Contains CSS styles used throughout the CA SDM web interface.

Although you cannot modify these files directly, you can add additional information to them. Each restricted file xxx.htmpl (except for menu_frames.htmpl and reports.htmpl) has a corresponding xxx_site.htmpl file that you can modify. For example, you can add additional information to ahdtop.htmpl by modifying ahdtop_site.htmpl, or add new messages by modifying msg_cat_site.js.

The xxx_site.htmpl file corresponding to each restricted file is loaded after the main file so you can override or change JavaScript in the main file. Use caution when adding information, as badly designed changes to these files can cause unexpected problems throughout the CA SDM web interface.

Guidelines for New HTMPL Files

You can add your own HTMPL files to the CA SDM web interface. Follow these guidelines to help ensure your HTMPL file works well with the rest of the CA SDM interface:

1. Include the following statement somewhere in the <HEAD> section of the file. This statement should follow the <TITLE> statement (if any). It defines several JavaScript global variables required by CA SDM web interface, and also registers your page with the CA SDM window manager:

   ```
   <PDM_INCLUDE FILE=std_head.htmpl>
   ```

2. Include the following attribute as part of the <BODY> tag of the file. This attribute helps the CA SDM window manager keep track of your page:

   ```
   onUnload="deregister_window()"
   ```

3. Include the following statement at the beginning of the <BODY> section of your file. The “menubar=no” argument is optional; if specified, it suppresses the CA SDM menu bar:

   ```
   <PDM_INCLUDE FILE=std_body.htmpl [menubar=no]>
   ```

4. Include the following statement at the end of the <BODY> section of your file.

   ```
   <PDM_INCLUDE FILE=std_footer.htmpl>
   ```

How to Add User Defined State Information

Many customers want to be able to embed their own state information in the CA SDM web pages, and have CA SDM pass the state information to all subsequent pages it serves up to the user's session. This information can be interrogated with conditional statements in the HTMPL files.

State information for a user's session is accomplished by setting the special attribute USER_STATE in your links or forms. After it is submitted into the CA SDM web engine, every page that is presented to the user will have the HTMPL variable USER_STATE available and set to the value last submitted for USER_STATE.

The following examples show how you might set up an entry into CA SDM from some other part of your site, such as from pages that are oriented to your sales force:

- Using a hyperlink

```
<a href="/CAisd/pdmweb.exe?USER_STATE=Sales">Service Desk</a>
```

- Using a form with a hidden field

```
<form action="http://yourhost.com/CAisd/pdmweb.exe">
<input type=hidden name=USER_STATE value=Sales>
```

Click the button for the Service Desk

```
<input type=submit>
</form>
```

Then you can modify your HTMPL forms based on the state information:

```
<PDM_IF "$USER_STATE" == "Sales">
```

custom information for sales audience

```
<PDM_ELIF "$USER_STATE" == "Engineering">
```

custom information for engineers

```
<PDM_ELSE>
```

information for everyone else

```
</PDM_IF>
```

How to Directly Create a Request from a Template

It is possible to create a Request directly from a Template using an URL.

Example

```
http://machinename/CAisd/pdmweb.exe?FACTORY=cr+OP=CREATE NEW+PERSID=cr:
3106+use_template=1
```

where cr:3106 is the persid of the template.

Directories Used by Your HTTP Server

The default installation of CA SDM defines two virtual directories to your HTTP server:

- The CAisd virtual directory points to the following directory in your CA SDM installation:
  1. In Windows: *installation-directory*\bopcfg\www\wwwroot
  2. In UNIX: $NX_ROOT/bopcfg/www/wwwroot
- The CAisd/sitemods virtual directory points to the following directory in your CA SDM installation:

1. In Windows: *installation-directory*\site\mods\www\wwwroot
2. In UNIX: $NX_ROOT/site/mods/www/wwwroot

Subdirectories under these virtual directories are:

Subdirectory	Stores
css	Style sheets
help	Web interface help
html	HTML files
img	Graphic files
scripts	JavaScript
sitemods	Site-defined modifications

If you decide to create versions of any of the files in the css, html, img, or scripts directories, we strongly recommend that you do not update the file in /CAisd. Instead, store the file in the appropriate subdirectory of /CAisd/sitemods. For example, if you decide to modify a style sheet in /CAisd/css, store your modified version in /CAisd/sitemods/css. When the web engine parses an HTMPL file, it automatically modifies file names beginning with $CAisd to point to sitemods if the file exists in a subdirectory of sitemods.

Using the /CAisd/sitemods directory has these advantages:

- It allows you to keep a record of the distributed files you have changed.
- It gives you easy access to the original version in case there is a question or a problem.
- It makes the process of installing maintenance or a new release easier, since CA SDM installation never places anything in the /CAisd/sitemods directory.

Note: There is no /CAisd/sitemods/help subdirectory. Because the help data is in standard HTML files (not HTMPL templates), the web engine cannot dynamically change file references. If you need to modify help, you must make your changes in /CAisd/help.

The HTML subdirectory contains a few heavily used files that do not need to be processed by the web engine and can improve performance when cached on the browser. If you create version of any of these files, carefully check the file for references to other modified files. Because there is no web engine processing, you must manually insert a reference to sitemods where appropriate.

Download PDF Attachments

When you download and try to view a PDF attachment in CA SDM, the PDF file may not display correctly, or a blank window may appear after you upgrade to Adobe Acrobat release 7.0 or 8.0. With CA SDM, you can display the PDF file correctly by completing the following steps:

1. Set the *forceDecompressOnDownload* parameter to YES in $NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\web.xml.

   Note: On Linux, $NX_ROOT is /opt/CAisd

2. Restart the CA SDM services.

Edit in List Modification

This article contains the following topics:

Several list forms, such as the Request and Issue lists, include an Edit in List button. When this button is available and a result set is displayed, the user can click Edit in List to replace the search filter with a small edit form. The edit form allows the user to update records directly on the list form. The user can even update everything selected in the list by placing the desired new data in the edit form and clicking Change All.

Editing list data involves no communication with the server until the user clicks Save. When the user clicks Save, all the updates (marked by yellow highlights on the form) are sent to the server, which applies all the changes in a single operation, returning a status message and redisplaying the list.

You can modify this feature by controlling whether the Edit in List button is available on a particular list form, and by controlling the fields that appear in the edit form displayed when the user clicks Edit in List.

To place an Edit in List button on a list form, including the following statement somewhere in the <HEAD> section of the form:

```
<SCRIPT LANGUAGE="JavaScript" SRC=$CAisd/CAisd/list_edit.js></SCRIPT>
```

Simply adding this statement puts the button on the form. However, the button is disabled unless JavaScript statements specifying the contents of the edit form are also included in the form. These statements must be placed immediately prior to the results set specification, and have the following format:

Statements	Comments
startListEdit(_search_filter);	Specify exactly as shown
listEditStartRow();	Specify exactly as shown
listEditField("attr"[, "hdr"]);	Specify zero or more
listEditReadonly("attr[", "hdr"]);	Specify zero or more

Statements	Comments
endListEdit();	Specify exactly as shown

The endListEdit() statement must be followed by the ResultSet() statement that begins the results set. You specify the fields in the edit form and their sequence on the form by coding one or more listEditReadonly() or listEditField() statements.

startListEdit(_search_filter)

This statement begins the list edit form. It must be coded exactly as *startListEdit(_search_filter);*.

listEditStartRow()

This statement begins a new row of fields on the list edit form. It must be coded exactly as *listEditStartRow();*. You must place a listEditStartRow() statement immediately after the startListEdit() statement. You can optionally include additional listEditStartRow() statements among the listEditField() and listEditReadonly() statements that specify the fields on the form.

listEditField(attr_name ,hdr)

This statement specifies an attribute to be included on the list edit form.

- **attr_name**
  Specifies the name of the attribute to be included in the edit form (including dots, if appropriate). All attributes specified for a list edit form must also be in the results set. The *attr_name* specified must be identical to that specified in the rs.showData() or rs.showDataWithLink() that adds the attribute to the results set.
  The attribute appears on the edit form in the same format that it appears in the search filter. If the attribute is not in the search filter, it is edited in a 20-character text box.
  attr_name is a required argument.

- **hdr**
  Specifies the text of the header on the field in the edit form. This argument is optional; if omitted, the header text is taken from the search filter. If hdr is omitted and the attribute is not in the search filter entry for attr_name, the header text defaults to the attribute name surrounded by question marks.

listEditReadonly(attr_name ,hdr)

This statement specifies a non-editable attribute to be included on the list edit form. Its arguments have the same significance as those for listEditField().

endListEdit()

This statement ends the list edit form. It must be coded exactly as *endListEdit();*.

Integrating with Your Own Web Pages

This article contains the following topics:

You can integrate the CA SDM web interface functionality with your web pages to present a seamless interface for your users.

Note: The web engine, which is the executable that acts as the gateway between the web server and the CA SDM server, allows multiple simultaneous connections from a given user. More than one frame at a time can have an open connection to the CA SDM web engine process.

You can integrate the web interfaces in the following ways:

- By creating links from any of your web pages to the appropriate CA SDM web page without having to go through the web interface menu page.
- By adding HTML forms to your web pages that collect input and perform supported operations directly, without displaying any CA SDM web data entry pages.
- By creating web form groups that can be used to associate HTML web-based forms to users through their access type. Similar to the form groups used by the administrative interface, web form groups can be used to customize your HTML pages.

Linking to CA SDM Functions

You can link directly to major CA SDM functions without displaying the main page. You typically do this by accessing the pop-up window for the new window containing the CA SDM information. You can also replace your web page with the CA SDM page.

In both cases, the product displays the requested page in the same way that the user sees it in a typical session, but without the main page and scoreboard. If you are an analyst, display the main page and scoreboard by selecting File, Restore Scoreboard, which is available only on pages displayed by bypassing the main page.

To create a link that bypasses the main page, specify a URL of the following form:

```
http://hostname[:port]/CAisd/pdmweb.exe?OP=operation+var=value+...
```

In this example URL, *hostname* is the web server host computer; *port* is the port number (typically 8080) required only if you are using Tomcat as your http server; *operation* is one of the supported operations, and *var=value* is one or more of the variables allowed with the operation.

For example, a link that loads the form for creating a request can be specified as the following:

```
<A HREF=http://hostname/CAisd/pdmweb.exe?OP=CREATE_NEW+FACTORY=cr>Define Request</A>
```

Posting Forms to CA SDM

You can also access CA SDM functionality by adding HTML forms to your web pages that refer to supported operations (see page 1789). If the form is submitted with sufficient information to perform the operation, such as creating a request, the operation is performed without displaying a form to collect additional input.

When you add an HTML form to your web page:

- The ACTION for the form is the URL for pdmweb.exe.
- The METHOD is POST.
- Either the name of the SUBMIT button should be one of the supported operations, or you should have a hidden field named OP whose value is one of the supported operations (see page 1789).

For example, to create an HTML form that loads the page for creating a request, specify the following code:

```
<FORM ACTION=/CAisdCAisd/pdmweb.exe METHOD=POST>
<INPUT type=HIDDEN NAME=FACTORY VALUE=iss>
.
.
.
<INPUT type=SUBMIT NAME=CREATE_NEW VALUE=" OK ">
</FORM>
```

JavaScript Modification

This article contains the following topics:

The CA SDM web interface makes extensive use of JavaScript and includes a number of JavaScript files in the /CAisd/scripts directory. If you decide to modify any of these script files, place the modified version in /CAisd/sitemods/scripts, as described in Directories Used by Your HTTP Server (see page 1800).

For performance reasons, the JavaScript files delivered in the /CAisd/scripts directory are compressed, with comments and unnecessary white space removed. This compression can make them difficult to read. You can find uncompressed versions of all JavaScript files in one of the following directories:

- (UNIX) $NX_ROOT/sdk/scripts
- (Windows) $NX_ROOT/sdk/scripts

If possible, avoid creating modified versions of entire JavaScript files, because each file contains a number of functions and you may only want to modify one function. In most cases, you can override individual functions by placing a modified version in the JavaScript file sitemods.js. We strongly recommend that you take this approach when modifying JavaScript.

sitemods.js

A skeleton *sitemods.js* file is distributed with CA SDM. All distributed HTMPL files include this file at the end of their <head> section, making it the last JavaScript file loaded. Because it is the last file, any functions defined in it override functions with the same name included earlier. This lets you provide your own version of a distributed JavaScript function without directly modifying distributed code.

This approach is not effective for functions invoked at load time in the <head> section, such as those in menubar.js and ahdmenus.js.

However, you can modify most JavaScript functions by completing the following steps:

1. Place a modified version of the function in sitemods.js.
2. Store the updated copy of sitemods.js in CAisd/site/mods/www/wwwroot/scripts.

Modifying Context Menus

A number of forms within CA SDM use context menus, accessed by right-clicking an object. Using the Web Screen Painter, you can modify context menus to add, remove, or modify their items.

Note: For more information about adding menu items, see the *Web Screen Painter Help*.

Updating and Creating Change Orders as Employee User

By default, a user can only view change orders from the Employee web interface. You can enable creating and updating change orders by employees:

Follow these steps:

1. Sign on to the web as the Administrator, and select the Administration tab.
2. Select Access Type from the Security menu.
   The Access Type List appears.
3. Select the Employee link to display the Employee Access Type Detail window.
4. Set the Change Orders to "modify" under the Function Access tab and save.
5. Click the Back button to return to the Administration tab, and then select Data Partitions, Data Partition List.
6. Click Employee to display the Data Partition Detail window. On the Constraints List portion of the window, review the Type column for following Change_Request Tables:
   - Pre-Update
   - Create

7. For each Table that you want to edit, click the Table name to display that table's Data Partition Constraint Detail window.

8. Click the Edit button.

9. Edit the constraint as follows:
   change "id = 1" to "affected_contact = @root.id".

10. Click Save.

Now when you login to the web interface as an employee user, the *Create Change Order* link appears.

Add a "Closed Change Orders" link to the Employee Scoreboard

You can use the product to add a Closed Changes node option to the Employee web interface scoreboard.

Follow these steps:

1. Log in to the product as an Administrator.

2. Click the Service Desk tab.

3. Select File, Customize Scoreboard.
   The Customize Scoreboard dialog appears.

4. Click the Role option and select Employee in the drop-down list.

5. Under Add New Node, click the Node's Stored Query link.
   The Stored Query List dialog appears.

6. Search and select Closed Changes from the Stored Query list. This is typically displayed as code CHGUBIN7.

7. Specify a location for the new node by selecting an item in the scoreboard tree on the left.

8. Click Add New Node.
   The new node named Closed Changes is added to the scoreboard tree.

9. Click Finished.

Download Attachments

When you download an attachment in CA SDM, it automatically displays the attachment in the browser window without prompting for a response from you. This action can be dangerous if a virus is associated with the attachment.

With CA SDM, you can force a save-as dialog that prompts you to respond if you want to save the attachment on the disk or open it. Saving an attachment can be a secure method because you can save the attachment on the disk and scan it before you can actually open it. You also have the option to force the save-as dialog only on certain attachment types.

You can force the save-as dialog to appear through the web.xml servlet configuration file. The web.xml file is located at the following paths:

Windows: $NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\web.xml

Linux: $NX_ROOT is "/opt/CAisd"

Free-Form Modification of Detail Forms

This article contains the following topics:

The topics in this section describe how to perform free-form modification of Detail Forms.

Using JavaScript on Detail Forms

Use WSP to add your own fields to a detail form, or rearrange or change edit characteristics of fields provided on the form by default. However, sometimes you want to modify a form beyond simply adding new fields to a grid. There are a number of a JavaScript functions provided with CA SDM to make it easy to merge your own modifications into a combination detail form and give it any appearance you want. These functions are summarized as follows:

- You can place any HTML whatsoever prior to the DetailForm() statement or after the endDetail() statement without affecting the operation of the detail form at all.

- You can use the detailEndTable() function to close the table that lays out detail form elements in a grid. After you have done this task, you can lay out your own HTML in any desired format. In this case, your HTML is inside the detail form, and any form fields within it are submitted to the web engine when the user clicks Save. You can use the detailNextID() function to generate ID fields for your HTML elements that allow them to participate in mouse-less navigation of the detail form. You can see several examples of this technique in the notebook tabs, such as xx_alg_tab.htmpl.

- You can follow your own HTML with a dtlStartRow macro to restart standard detail form formatting. This starts a second grid, whose fields will not necessarily be aligned with the first. This technique is used in every notebook tab.

- If you want to insert a custom element at the end of a row, you can use the detailWriteRow() function to write out the contents of a row without closing it. You can see an example of this technique in the code that generates the "24 Hour" button in detail_cr.htmpl and detail_iss.htmpl.

- If you want to explicitly specify the contents of an element in a row without closing out the table that lays out the grid, you can use the detailRowHdr() function to specify the header text and the detailSetRowData() function to specify the data text. You can see an example of this technique in the code that generates the timer field in detail_cr.htmpl and detail_iss.htmpl.

- If you provide a function to validate a field's value (normally in an event handler), and want its results reported during browser-side validation (so that an erroneous field is redrawn with a thick red border, and an error message appears in a yellow band at the top of the form), use the function detailReportValidation(). You can see an example of this in the validate_duration() function used to validate the duration fields in xx_candp_tab.htmpl. The validate_duration() function is in the file val_type.js.

- If you want review the HTML generated for a detail form, you can use functions docWrite() and docWriteln() in place of the standard functions document.write() and document.writeln(). Then if you invoke the function holdHTMLText() anywhere in the <HEAD> section of your form, CA SDM will pop up a debugging form containing a TEXTAREA with all of the HTML generated for the form, which you can review or copy and paste into a validation tool.

While you are composing your modifications, remember that the combination detail form is displayed in both a read-only and an edit view. If your modifications apply specifically to one view or the other, you can test the current view in one of two ways:

- In JavaScript, the expression _dtl.edit is true in the edit view and false in the read-only view.

- In either JavaScript or open HTML, the statements:

```
<PDM_IF "$prop.form_name_3" == "edit">

</PDM_IF>
```

(Used only in the edit view)

or

```
<PDM_IF "$prop.form_name_3" == "ro">
```

(Used only in the read-only view)

```
</PDM_IF>
```

Used to bracket code intended only for the edit or read-only view, respectively.

detailEndTable()

This function closes the HTML table that lays out the detail form elements in a grid. It has no arguments.

You can start a new grid with the dtlStartRow() macro. However, elements in a new grid are not necessarily aligned with elements in a previous grid.

detailNextID(colspan, lastelement)

This function returns a string of the form:

```
" ID=df_nn_nn TABINDEX=n onFocus=func onBlur=func"
```

Inserting this string into an HTML element causes the element to follow the conventions of CA SDM mouse-less navigation, including accessibility with the arrow keys and turning pale yellow when focused. The returned string begins with a space and ends with no space.

- **colspan**
  Specifies the number of columns in the grid occupied by the element. This argument is optional; it defaults to one if not provided. If omitted, the element is assumed to occupy one column of the grid. This affects arrow key behavior. The *colspan* argument can be omitted even if the *lastelement* argument is provided.

- **lastelement**
  A Boolean value specifying whether the element for which the ID being generated is the last one in its row. If omitted, the element is assumed to be followed by other elements. This affects arrow key behavior.

detailNextLinkID()

This function returns a string of the form:

```
" ID=dflnk_nn_nn TABINDEX=0 onFocus=func onBlur=func"
```

Inserting this string into an HTML element defining a link element causes the element to follow the conventions of CA SDM mouse-less navigation, including accessibility with the up arrow key from the base element and turning pale yellow when focused. The returned string begins with a space and ends with no space.

This function takes no arguments.

detailReportValidation(field, has_error, emsg)

This function reports the result of external field validation. If validation is reported to have failed, the field is redrawn with a thick red border and the error message provided is shown in a yellow band at the top of the form. The user is not permitted to save the record until a subsequent call to detailReportValidation() reports the field as error-free.

The detailReportValidation() function is functional only for fields registered for browser-side validation. All fields created with detail form macros are automatically registered for validation. You can register other fields with the detailSetValidateFunction().

- **field**
  (Required) Specifies the form element object containing the field. The easiest way to obtain this is to pass this argument to the event handler performing the validation. Another way is to use the standard JavaScript function document.getElementById().

- **has_error**
  (Required) A Boolean or integer value specifying whether the field is in error. Setting a field in error prevents the user from saving the record, causes the field to be highlighted with a thick red border, and places the error message supplied as the third argument in a yellow band at the top of the form. Setting a field as not in error reverses these changes.

- **emsg**
  A text string specifying the message to display in the yellow band at the top of the detail form when the *has_error* flag is set. This argument is required if *has_error* is set.

detailSetValidate(hdrtext, is_required, maxsize)

This function specifies that the most recent field created with an ID supplied by detailNextID() is subject to browser-side validation. Validation for required fields and for fields with a maximum size is automatic. Other forms of validation may be provided through JavaScript functions or event handlers calling detailReportValidation().

You should call detailSetValidate() only for form fields you have defined yourself whose ID was created by detailNextID(). The detailSetValidate() function must be called immediately after creating a field that you want validated. It is unnecessary (and will caused unexpected results) to call detailSetValidate() for fields created by detail form macros.

- **hdrtext**
  (Required) Specifies a string used to identify the field in error messages.

- **is_required**
  (Required) A Boolean or integer value specifying whether the field is required. CA SDM automatically verifies that all required fields are provided whenever the user attempts to save a record.

- **maxsize**
  An integer specifying the maximum length of data allowed for the field. CA SDM automatically verifies that all fields with a *maxsize* value have a length within limits whenever the user attempts to save a record. This argument is required. To suppress *maxsize* validation, specify a value of 0.

detailRowHdr(hdrtext, colspan, is_required)

This function stores text for the header (TH) element of an item in the grid. The text is not actually written to the form until a detailWriteRow() function or dtlStartRow macro is invoked.

- **hdrtext**
  Specifies the text in the header element. This argument is required.

- **colspan**
  Specifies the number of columns in the grid occupied by the element. This argument is optional; it defaults to one if not provided. If omitted, the element is assumed to occupy one column of the grid. This affects arrow key behavior. The *colspan* argument must be provided if the *is_required* argument is provided.

- **is_required**
  Specifies whether the *hdrtext* should be displayed in the style corresponding to a required field. The argument can be a Boolean, a number, or a string. A number or a string is interpreted as false if zero and true otherwise. This argument is optional; if omitted, the *hdrtext* is styled as a non-required field.

detailSetRowData(text)

This function stores HTML text for the data (TD) element of an item in the grid. The text is not actually written to the form until a detailWriteRow() function or dtlStartRow macro is invoked. The single argument is the HTML text of the element to be stored.

detailWriteRow()

This function writes the HTML stored for the current row. This creates two HTML table rows, one for the header (TH) elements and one for the data (TD) elements. The function also writes the [assign the value for TD in your book] tag that begins a new data element. The TD tag is automatically closed by the dtlStartRow macro, so it is unnecessary (and incorrect) to provide the [assign the value for TD in your book] tags in HTML text that follows detailWriteRow(). This function has no arguments.

Create a Quick Close Ticket With Preset Options

In the Quick Profile View, you can create a Quick Close ticket, for example, a Quick Close Incident. Add a preset string to the URL when you create a Quick Close ticket to add a description, a summary, or other field information automatically.

Follow these steps:

1. Copy the ahdtop_site.htmpl file from NX_ROOT/bopcfg/www/htmpl/default to NX_ROOT/site /mods/htmpl/www/default.

2. Edit the ahdtop_site.htmpl file to add the appropriate variable (depending on the type of Quick Close ticket) with the preset string.

   - Quick Close Incident -- var quick_close_preset_in
   - Quick Close Problem -- var quick_close_preset_pr
   - Quick Close Request -- var quick_close_preset_cr
   - Quick Close Issue -- var quick_close_preset_iss

   For example, the following string sets the description to HelloIncident and summary to HelloIncidentSummary for a Quick Close Incident.

   ```
   var quick_close_preset_in = "PRESET=description:HelloIncident@@summary:
   HelloIncidentSummary";
   ```

3. Log in to CA SDM.

4. Select View, Quick Profile in the Service Desk tab.
   The Quick Profile Contact Search page appears.

5. Complete one or more of the search fields for the contact, and click Search.
   The Quick Profile Contact List populates with those contacts that match your search criteria.

6. Select a contact.
   The right pane displays the information for that contact.

7. Click Quick Close.
   The ticket is created with the preset information.

Looking Up Information in Reference Tables

Input fields on a detail form editing a database record are namedSET.attr_name. When the record is saved, data from SET fields are copied directly to the underlying record. Thus, an input field for an attribute that references another table should contain the REL_ATTR (foreign key) of that table. This is normally the id, persistent_id, or code of the reference record.

Users do not directly provide REL_ATTR values, and the SET fields for attributes referencing another table are hidden. The visible field on the form is named KEY.*attr_name*, and it contains the common name of the referenced record. A common name must be converted into a REL_ATTR to update the record. There are several times when this might be done:

- For fields with a drop-down list, the SET value is provided directly by the drop-down.
- For fields with a lookup when the user clicks the lookup and selects an item, the SET value is copied from the selected item.
- For fields with a lookup where the user provides a partial key that uniquely identifies the record and then clicks the label, the browser requests the SET value from the server and copies both it and the full key back to the form.
- If the Autofill configuration file property is provided or defaulted, and the user both provides a partial key that uniquely identifies the record and clicks Notebook to exit the field, the browser requests the SET value from the server and copies both it and the full key back to the form.

Otherwise, when the record is saved with a KEY value and no SET value, the web engine resolves the value during the save. If any KEY values cannot be resolved to a unique SET value, the save is prevented, and the edit form is redisplayed.

If a form has been redisplayed as a result of a save that failed due to a lookup resolution failure, the following variables are available in the HTMPL for each attribute field for which a lookup was performed:

- **LIST_*attr***
  Contains all the matches found. Typically this is specified as the right-hand side of the SOURCE= field in a <PDM_SELECT> statement.
- **FLAGS_*attr***
  This is set to one of the following values:
  - **0**
    Display initial search field.
  - **1**
    More than one and fewer than MaxSelectList were found (typically a <PDM_SELECT> list would be displayed in this case).
  - **2**
    No matches were found.

- **3**
  Too many matches were found (more than MaxSelectList).

- **SEARCH_STATUS_*attrstring***
  Contains the TooManyMatches text string from the web.cfg file.

Specifying Lookups on Contacts

When specifying a contact (last name, first name, middle name) in an editable form, you can delimit the contact name with commas (,) or blank spaces, but not both. Commas are preferable because names often have embedded spaces, which cause problems.

Since a combination of commas and blank spaces is not allowed, the presence of commas implies that all parts of the name are comma-separated; if no commas are present, names are delimited by spaces.

Since the information is eventually passed to an SQL query, the percent symbol (%) serves as a wildcard character. For example, 'P%, J%' would match 'Public, John', 'Penxa, Jane', and any other names whose last name begins with P and first name begins with J. (Case-sensitivity depends on the underlying database.) Similarly, 'P% J%' would bring up the same names.

However, 'P%, Jon D' would not bring up all contacts with a first name of Jon, a middle initial of D, and a last name beginning with P, because the presence of one comma means all delimiters are commas. Therefore, the last name would be looked up as 'P%' and the first name would be looked up as 'Jon D'. To avoid this error, specify 'P%, Jon, D' instead.

Understanding List Forms

The following information provides background information about the internals of CA SDM list forms. We recommend that you use the Web Screen Painter Design View to modify these forms.

CA SDM list forms are defined with the following macros (invoked with the PDM_MACRO tag):

- **lsStart**
  Begins a list

- **lsCol**
  Defines a column in a list

- **lsWrite**
  Inserts text into the pdm_list part of a list

- **lsEnd**
  Ends a list

The general form of a list using these macros is the following:

```
<pdm_macro name=lsStart>
<pdm_macro name=lsCol hdr=hdr1 attr=attr1>
<pdm_macro name=lsCol hdr=hdr1 attr=attr1>
<pdm_macro name=lsEnd>
```

This results in text similar to the following example in the output HTML:

```
var rs = new Resultset();    From lsStart
rs.startList(); From lsStart
rs.header("hdr1"); From lsCol
rs.setData("attr1","options"); From lsCol
rs.header("hdr2"); From lsCol
rs.setData("attr2","options"); From lsCol
<PDM_LIST SOURCE=list> From lsEnd
rs.data(attr1) From lsCol/lsEnd
rs.data(attr2) From lsCol/lsEnd
</PDM_LIST> From lsEnd
```

Note: There are two distinct sections to the output list: the setup section before the <PDM_LIST> tag, and the actual list between the <PDM_LIST> and </PDM_LIST> tags. The lsCol macro makes use of preprocessor variables and the <PDM_SET> tag to output data to both sections of the list. The entire list section of the list is created by a <PDM_EVAL> tag generated by the lsEnd macro.

To insert your own JavaScript in the setup section of the list, simply include it where needed. Use the lsWrite macro to insert your own code into the list section of the list.

The lsWrite Macro

The lsWrite macro specifies text for the list section of a list (the portion between the <pdm_list> and the </pdm_list> tags). Text specified for the text argument of this macro is deferred, and not written to the output HTML until the lsEnd macro.

lsWrite [both=no|yes]

text=”xxx”

- **both**
  Specifies that the text operand is to be written both immediately to the output HTML and to the deferred text buffer. This can be useful to output JavaScript to conditionally bypass both the setup and the list information output by a subsequent lsCol macro. Optional; defaults to no.

- **text**
  Specifies the text generated by this macro. Text specified is deferred until the lsEnd macro.

It is often desirable to include pdm tags and references to form variables in the text output by an lsWrite macro. To prevent these from being interpreted by the web engine during parsing of the lsWrite macro itself, follow these syntax rules:

- If the lsWrite macro generates a pdm_tag, omit the surrounding “<” and “>” delimiters of the tag. For example, to insert a <pdm_else> statement into the list section of the list, code:

  ```
  <PDM_MACRO NAME=lsWrite text="pdm_else">
  ```

  The web engine automatically inserts the “<” and “>” before producing the text when it detects that the first four characters are “pdm_” (or “PDM_”).

- If the lsWrite macro generates a reference to a form variable, code an @ character in place of the $ character that designates the variable. For example, to generate a reference to the list variable $list.persistent_id, code:

```
<PDM_MACRO NAME=lsWrite text="@list.persistent_id">
```

  The web engine automatically converts the "@" to "$" before producing the text. To produce a literal @ sign, precede it with a backslash.

Web Engine PreProcessing

This article contains the following topics:

The web engine goes through two phases when processing an HTMPL file:

- The preprocessing phase, when it reads the HTMPL file and any referenced files (including files referenced by PDM_INCLUDE and PDM_MACRO tags). The output from preprocessing is an entry in the web engine's internal cache.

- The generation phase, where it reads the form from its cache and generates HTML. The output from generation is HTML delivered to the browser.

The pre-processing phase is typically done once for each form in the lifetime of the web engine. The generation phase is done each time a form is requested.

You can use the PDM_SET and PDM_EVAL tags during the preprocessor phase to generate and store information, such as HTML text, that the web engine can use in the generation phase.

Preprocessor Variables

Preprocessor variables begin with the string "$PRE.". They are created and updated with the PDM_SET (see page 1783) tag. This tag has the following syntax when used with a preprocessor variable:

```
<PDM_SET PRE.name[+]=value>
```

This tag assigns or updates a preprocessor variable, creating it if necessary. It is processed when the web engine encounters it while reading a form. Only the invariant PDM_IF statements affect PDM_SET of a preprocessor variable; others are ignored.

Invariant PDM_IF Detection

When parsing a form, the web engine detects invariant PDM_IF statements. An invariant PDM_IF is one whose argument consists entirely of literals, environment variables, constant properties, and preprocessor variables. When the web engine detects an invariant PDM_IF, it evaluates its condition immediately. This has the following effects:

- PDM_SET and PDM_EVAL tags that are bypassed by an invariant PDM_IF are ignored. All other pdm_eval tags and PDM_SET tags referencing preprocessor variables are executed when processed, even if they are within a non-invariant PDM_IF.

- Form variable references bypassed by an invariant PDM_IF are ignored, and their value is not fetched when the form is used. You can use this technique to improve the performance of a form. For example, if a form contains the following, the web engine fetches the value of $args.def before it displays the form:

```
<PDM_IF "$env.NX_OTB_MARKET == "itil" && "$args.a" == 1>

<h1>This is form $args.def</h1>

</PDM_IF>
```

  However, if the following segment has been written, the web engine determines that the first PDM_IF is invariant, and retrieves the value of $args.def only if $NX_OTB_MARKET is “itil”.

```
<PDM_IF "$env.NX_OTB_MARKET == "itil">

<PDM_IF "$args.a" == 1>

<h1>This is form $args.def</h1>

</PDM_IF>

</PDM_IF>
```

PDM_EVAL Insert Text from a Preprocessor Variable

The PDM_EVAL tag inserts the value of a preprocessor variable into the input to the web engine parser. If used inside a macro, its effect is deferred until the macro completes.

The PDM_EVAL tag works similarly to PDM_INCLUDE or PDM_MACRO. It inserts the text into the parser at the point of the tag, exactly as if the value of its variable had been coded in place of the tag.

PDM_EVAL has the following syntax:

```
<PDM_EVAL text=PRE.name>
```

where PRE.name specifies the name of the preprocessor variable whose value is to be inserted into the web engine's input

Execution of the PDM_EVAL tag can be controlled by invariant PDM_IF statements.

Important! On UNIX, the LIBPATH needs to be set before running the utility. Use pdm_task to perform this task. For example, before running the utility, input "pdm_task pdm_eval".

Event Log Data Storage Modification

The system environment variable *@NX_EVENT_LOG_EXCLUDE*, which is set in the *NX.env* file and requires a restart of the CA SDM services, lets you control the amount of data that is stored in the event log (event_log table). This variable lets you store only the events you want to track, report on, and use as part of the Recent Activity that can be launched as a button from the Quick Profile page.

In this variable, commas separate list items (for example, *@NX_EVENT_LOG_EXCLUDE = FAQ, KD_OPEN*). For example, if you use the LOGIN,LOGOUT events from the following table (@NX_EVENT_LOG_EXCLUDE value of LOGIN,LOGOUT), the product does not record login and logout events.

Refer to the following information when modifying data to store in the event log using this variable:

Event	Enum	By	Sets	Comments
LOGIN	1	CA SDM		Specifies that the User logs in to the system.
LOGOUT	2	CA SDM	numdata1	Specifies that the User logs out, where numdata1=logout reason:**0** -- normal**1** -- timeout**2** -- abnormal
CR_CREATE	3	CA SDM	sd_ob_type, sd_obj_id, kd, numdata1	Indicates that the User creates a request, where numdata1=id of affected end user.
ISS_CREATE	4	CA SDM	sd_ob_type, sd_obj_id, kd, numdata1	Indicates that the User creates a change order, where numdata1=id of the affected end user.
CHG_CREATE	5	CA SDM	sd_ob_type, sd_obj_id, kd, numdata1	Indicates that the User creates an issue, where numdata1=id of the affected end user.
EMAIL	6	Knowledge Management	kd	Specifies that the Analyst emails a document.
LINK	7	Knowledge Management	kd, sd_obj_type, sd_obj_id	Indicates that the User accepts a solution, and links it to a ticket.
UNLINK	8	CA SDM	sd_id, sd_obj_type, sd_obj_id	Specifies that the User unlinks a solution from a ticket.
SEARCH	9	Knowledge Management	numdata1,	Indicates that the User searches knowledge, where numdata1=CI_ASKED_QUES id.
FAQ	10		numdata1	Indicates a FAQ search, where numdata1=O_INDEXES id (category).

Event	Enum	By	Sets	Comments
		Knowledge Management		
DT_NAVIGATE	11	Knowledge Management	kd,numdata1, textdata1	Indicates that the User navigates a decision tree, where numdata1=ES_NODES ID textdata1=path.
KD_BOOKMARK	12	Knowledge Management	kd	Indicates that the User bookmarks a KD.
KD_COMMENT	13	Knowledge Management	kd, numdata1	Indicates that the User adds a comment to a KD, where numdata1=O_COMMENTS id.
KD_CREATE	14	Knowledge Management	sd_ob_type, sd_obj_id, kd	Specifies that a User creates a document. CA SDM IDs are used when a KD is created using submit knowledge from a request or an issue.
KD_OPEN	15	Knowledge Management	kd, numdata1	Indicates that a User opens a KD, where numdata1=BU_TRANS ID.
KD_RATE	16	Knowledge Management		Indicates that a User rates a KD, where numdata1=BU_TRANS ID.
KD_NEW	17	Knowledge Management	numdata1	Specifies that a User clicks on the New Documents folder in the Knowledge tab.
NX_ATTACH_AUDIT_TO_NEW_TICKET	18	CA SDM		When a User opens a new ticket, all events for the current session appear by default on the Event Log tab of the ticket. **0** -- Only events relevant to the ticket appear on the Event Log tab. **1** -- All events for the current session appear on the Event Log tab of the ticket.
TICK_OPEN	19	CA SDM		Indicates that the ticket was viewed.
TICK_SEARCH	20	CA SDM		Indicates the user who searched for tickets and links the number of searches.
KD_PRNT	21	Knowledge Management	kd	Indicates the knowledge document was printed.

Print CA SDM Web Pages

CA SDM uses background graphics to format its buttons and notebook tabs. The default setting for many browsers is *not* to print these background images. Therefore, if you select File, Print on either the browser menu or the CA SDM menu, the printed page shows only the corners of the buttons or tabs.

You can print CA SDM web pages on Internet Explorer.

Follow these steps:

1. Select Tools, Internet options.
   The Internet Options dialog appears.

2. Select the Advanced tab.

3. Scroll down to the Printing heading, and select the Print Background Colors and Images option.
   The printed CA SDM web pages include background graphics.

You can print CA SDM web pages on Firefox.

Follow these steps:

1. Select File, Page Setup.

2. Select the Format & Options tab.

3. Select the Print Background (color & images) check box.
   The printed CA SDM web pages include background graphics.

Modify CA Business Intelligence Reports

This article contains the following topics:

The following reports are shipped with CA Service Management Release 14.1:

- (For CA SDM) Crystal Reports and Web intelligence reports

- (For CA Service Catalog and CA Asset Portfolio Management) Web Intelligence reports

Before you modify the reports, ensure that you have followed these prerequisites:

- Installed Crystal Reports 2013 Designer on the machine where CA Business Intelligence Release 4.1 SP3 Client Tools are installed.

- Completed CA Business Intelligence Configuration for CA SDM using the CA Service Management Installer.

Important! Please do not modify OOTB Universe and Reports. Always make a copy, modify the copy and save it outside the CA Reports folder.

Modify Crystal Reports

Follow these steps:

1. Open the Crystal Reports 2013 Designer on the machine where it is installed.
2. Log in to the BusinessObjects Repository.
3. Navigate to the Folder structure in the Repository Explorer and open the Target Report that you want to modify.
4. Click Database Menu, Database Expert Edit Query.
5. Make the necessary modifications.
6. Create or update formulas, if required.
7. Click File, Save As. Provide a New Report Name and save it outside of the CA Reports folder.

Modifying Web Intelligence Reports

Follow these steps:

1. Open the Web Intelligence Rich Client on the machine where CA Business Intelligence Client Tools are installed.
2. Log in to the BusinessObjects Repository.
3. Navigate to the Folder structure in the Repository Explorer and open the Target Report that you want to modify
4. Click Design, Structure.
5. Click Data Access, Edit.
6. Make the necessary modifications.
7. Create or update variables, if required.
8. Click File, Save As. Provide a New Report Name and save it outside of the CA Reports folder.

At the end of this topic, you have successfully modified the reports.

CA Business Intelligence Infrastructure

CA Business Intelligence (CA BI) is an enterprise reporting infrastructure that enables you to create, maintain, store, schedule, and distribute reports for CA SDM users and roles. BusinessObjects Enterprise XI, Release 2 and its associated tools, coupled with BusinessObjects Crystal Reports 2013 are the backbone of the architecture. BusinessObjects Enterprise tools are contained in a CA SDM created package, merging CA SDM reporting essentials into an industry leading business intelligence framework.

Note: Although Crystal reports are delivered as the primary component of CA BI, the report creation and maintenance tool, Crystal Reports 2013, is not delivered. Crystal Reports 2013 is a separately licensed product that can be purchased from BusinessObjects and used in conjunction with CA BI.

Reporting Components

Following are the primary components included in the CA Business Intelligence infrastructure:

- **CA SDM** Database/ Domsrvr / ODBC Driver -- Report data is stored in a SQL Server or Oracle CA SDM database. BusinessObjects reporting applications (Crystal Reports and Web Intelligence) access the database using an ODBC driver that connects directly with the CA SDM object engine (domsrvr). All CA SDM security, including data partition and tenancy restrictions, is automatically applied to reports.
- **Central Management Server** -- The Central Management Server (CMS) is the central repository that stores all objects used in every reporting process.
- **Central Management Console** -- The Central Management Console (CMC) is the main administrative facility for BusinessObjects. It provides access to all BusinessObjects administration functions. Using the CMC, you can deploy reports and assign user access and folder permissions for Business Intelligence Launch Pad.
- **BusinessObjects Universe** -- The universe provides a business representation of a data warehouse or transactional database. It describes the classes (tables) and objects (columns) which are used in reports. The CA SDM universe is installed and configured during the installation. At the completion of the installation, the universe connection is assigned to various groups and users in CA SDM.
  - **Universe Design Tool** -- It is a tool in BusinessObjects Enterprise that lets you modify the CA SDM Universe, which is a metalayer between CA SDM schema, and BusinessObjects reporting tools. The Import/Export Wizard facilitates object population or extraction within the CMS.
- **Default Predefined Reports** -- Predefined reports are web-based CA SDM and Knowledge Management reports developed with either BusinessObjects Web Intelligence (WebI) or Crystal Reports. The reports can be used as models for defining site-specific reports.

- **Business Intelligence Launch Pad** -- Business Intelligence Launch Pad is a web interface that allows authorized CA SDM users to interact with web-based predefined reports by viewing, running, and scheduling report types including, but not limited to, WebI and Crystal Reports. Reports are contained in folders in the public section in Business Intelligence Launch Pad.

- **Ad Hoc Reports** -- Ad hoc reports are created and administered from Business Intelligence Launch Pad using a WebI plugin-based interface. This tool is intended for users who want to create basic reports easily without writing queries.

Development Environment

This article contains the following topics:

Updating the CA Business Intelligence infrastructure with CA SDM schema changes is an administrative function. An administrator who is promoting modified schema into the reports must set up the environment, apart from their production environment.

Some of the tools used by CA Business Intelligence require a Windows-based architecture. This means that installations of Linux/UNIX must configure CA Business Intelligence on a Windows computer to interact with the Linux/UNIX production environment CA Business Intelligence installation. If you are using Windows servers in production, you should configure an additional Windows computer for your development environment.

Tools

Updating the CA Business Intelligence infrastructure with CA SDM schema changes is an administrative function. To promote modified schema changes into the reports, you must include the following tools in your development environment:

- **Universe Design Tool**
  This full client Windows tool is installed on the CA Business Intelligence production server as part of the base CA Business Intelligence installation for windows. When the CA Business Intelligence server is a non-Windows architecture, or when login access to the production CA Business Intelligence application server is undesirable, you must create a separate CA Business Intelligence installation on a Windows (development) server. A development CA Business Intelligence server installation allows you to access the production CA Business Intelligence objects remotely, no matter the architecture of the CA Business Intelligence production server installation.

- **BusinessObjects Web Intelligence**
  This web-based report creation tool is used for modifying and creating Web Intelligence (WebI) reports. You can access the WebI tool through the Business Intelligence Launch Pad interface. Administrative permissions for the WebI and Business Intelligence Launch Pad tools are available within CA Business Intelligence, specifically using the BusinessObjects Central Management Console (CMC) tool.

- **CA SDM ODBC Driver**
  Provided with the CA Business Intelligence installation is the CA SDM ODBC Driver. This component enables WebI and Crystal Reports to access CA SDM data while enforcing data

partition security. The ODBC Driver is installed as part of the base CA Business Intelligence installation on the CA Business Intelligence application server. It is also available as a client installation so that it can be used on a computer not running CA Business Intelligence along with the Crystal Reports XI client.

Note: For information on defining data partitions security for your reporting environment, see the Set Up Data Partitions Security for Reporting (see page 3212) section.

How to Create a Development Environment

To create a development environment, do the following:

1. Secure a server with a supported Windows operating system.
2. Install and configure CA SDM.
3. Install and configure CA Business Intelligence.
4. Change the default ODBC DSN Name from casd_xxxxx to casd_yyyyy where yyyyy is exactly the same as the DSN on the production implementation.

   Important! Regardless of the actual connection properties, the DSN name must be identical on the development and production implementations.

5. (Optional) Install and configure Crystal Reports XI.

   Note: It is not required to install Crystal Reports on the same computer as CA Business Intelligence. Crystal Reports can be installed on a different computer, as long as the CA SDM ODBC Driver is also installed on the Crystal Reports computer , and the DSN Name is modified to be identical to the production implementation, regardless of the actual connection properties. For more information about installing an individual copy of the CA SDM ODBC driver, separate from the CA Business Intelligence installation, see your ODBC Driver documentation.

6. Create the Framework (see page).

Framework

After the tools are available in your development environment, the next step is to create a framework that will allow schema changes to be preserved through product upgrades.

Important! Do not modify the default development CA SDM universe installed with CA Business Intelligence. Otherwise, your schema changes may be overwritten during patch and upgrade processes. Modifying the CA SDM universe will eventually result in lost schema changes within the CA Business Intelligence infrastructure.

The BusinessObjects universe is the metalayer that describes the schema within the CA Business Intelligence infrastructure. Instead of changing the CA supplied universe, you can create a customer-specific universe linked to the CA SDM universe. Using this approach, you can maintain local schema changes with minimal effort during the upgrade process, and CA SDM will be able to provide upgrades to the base universe.

CA SDM customers familiar with BusinessObjects universe documentation will be aware of other documented procedures available from BusinessObjects that allow tying universes together. The process discussed here, however, is the only process that is supported by CA for maintaining customer modifications.

The default universe is named "CA SDM" and it is stored in the "CA Universes" folder within the Central Management Console (CMC). This default universe is the "kernel" universe in a structure where universes are linked.

The CA SDM universe can be named anything you choose. The name will be displayed to report writers when they are building reports, so make sure the name is meaningful. The customer universe is the "derived" universe in a structure where universes are linked.

Within this framework, any number of derived universes can be maintained, but only one is required for maintaining schema changes. Multiple derived universes may be used for ease of maintenance or security requirements, but such decisions are solely at the discretion of your production support needs.

In any multiple derived universe environment, ensure that you do the following:

- Maintain the z_ naming convention for the universe file name on all universes.
- Use the CA SDM connection, then store the universe in the CA Customer Universe folder.
- Do not delete the link to the kernel universe.

Create a Framework for Promoting Schema Changes to CA Business Intelligence

Use the Universe Design Tool to create a framework for promoting schema changes to CA Business Intelligence.

Follow these steps:

1. Open the Universe Design Tool.
   Select File, New from the Universe Design Tool menu.
   The Universe Parameters window appears.

2. Click the Definition tab and enter a meaningful name for this universe in the Name field.

3. (Optional) Enter a description in the Description field.

4. Select CA SDM from the Connection drop-down list.

5. Click the Add Link button on the Links tab.
   The Universe to Link dialog appears.

6. Expand the CA Universes folder and complete these tasks:

   a. Open the CA Service Desk.unv file. The Universe to Link dialog closes and the CA SDM universe appears on the Links tab.

   b. Click OK to close the Universe Parameters dialog.

   Universe Design Tool may take a few minutes to process the link and create the derived universe.

7. After the derived universe is created, perform these tasks:

   a. Modify the following parameter(s) as appropriate.

      - Select Parameters from the File menu.
      - Click the Parameter Tab.
      - Specify ANSI92 = YES.

   b. Click the Controls tab and set the following fields to a value appropriate to your implementation, then click OK to save the values and close the parameter dialog:

      - Limit size of result set
      - Limit execution time
      - Limit size of long text objects (minimum of 4000).

   c. Define hierarchies. Note that customer hierarchies are not imported.

      - Select Tools, Hierarchies.
      - Multi-select all custom hierarchies, then click the Add arrow button. All hierarchies are moved to the right side.

8. From the Universe Design Tool menu, click File, Save.
   The Save As dialog appears.

9. In the File Name field, select any descriptive file name, and proceed the file name with "z_". For example, a universe named "ACME Anvil Co" might default to: "ACME_Anvil_Co.unv." Change this file name to "z_ACME_Anvil_Co.unv" before saving.

10. Export the derived universe to the CMS as follows:

    a. Select File, Export from the Universe Design Tool menu.

b. From Domain field drop-down list, select <Browse>, then locate and select CA Customer Universes.

c. Click OK to export the universe to the local CMS
The Universe Successfully Exported dialog appears.

The framework now exists to promote custom schema changes throughout CA Business Intelligence.

11. Log into Business Intelligence Launch Pad as an administrative user and do the following:

a. Select Public Folders.

b. From the Business Intelligence Launch Pad toolbar, click New, Folder.

c. In the Folder Name field, provide a description meaningful to report users, such as "Organization Name Reports."

d. Click OK to see the folder created under Public Folders.

This creates the minimum framework to use and store reports by your organization. Any number of subfolders and objects can be added to this folder structure.

Reports and Folder Structures

This article contains the following topics:

Included with the CA BI installation are several Crystal Report XI and WebI report objects. The reports are contained in the following CA SDM folder: CA Reports\CA SDM.

Important! Do not modify the CA SDM universe and report objects contained in the CA SDM folder structure.

Consider the following information about reports and the folder structures:

- The steps for creating a framework explain how to add a folder in the Business Intelligence Launch Pad public section, which is specific to the end user. Within this folder, a user can create additional subfolders and report objects.

- In an implementation where each user is authorized access to CA BI by their unique CA SDM login ID, users can save reports for personal use within the My Folders section. BusinessObjects enforces security on this folder by showing these objects only to the logged in user.

- In an implementation where all users have a single reporting user ID for accessing CA BI, the My Folders section is available to all users.

Create a Web Intelligence Report

Use CA Business Intelligence to create a Web Intelligence report.

Follow these steps:

1. From the CA SDM Reports tab, click the Business Intelligence Launch Pad button.
   The Business Intelligence Launch Pad home page appears.
2. Click New, Web Intelligence Document from the menu bar.
3. Select the derived universe that you created when you defined your development framework.
   The Web Intelligence report creation tool appears.

   Note: Save your document at regular intervals. If the connection session times out, your report modifications will be lost. For information on how to increase the Web Intelligence connection session time-out value, see Change the Web Intelligence Session Time-Out (see page 3263).

4. From the Web Intelligence toolbar, select Save, Save as.
   The Save Document dialog appears.
5. In the General section, specify a meaningful name for this report in the Title field.
6. In the Location section, select the appropriate folder.
7. (Optional) modify the properties as desired.
8. Click OK to save the report.
   The report appears in the specified folder and is available to all report users.

Modify a Web Intelligence Report

Use CA Business Intelligence to modify a report that was delivered in the CA Reports\CA Service Desk folder structure.

Follow these steps:

1. From the CA SDM Reports tab, click the Business Intelligence Launch Pad button.
   The Business Intelligence Launch Pad home page appears.
2. In the left pane, navigate the CA Reports folder structure, and open the desired Web Intelligence report.
3. Click the name of the report so that the report runs and displays a result.

4. From the Web Intelligence toolbar, select Document, Save as.
   The Save Document window appears.

5. In the Location section, select the appropriate folder.

6. Click OK to save the report in the new location.

7. Select Document, Edit.

8. Click Edit Query (the name of the universe CA SDM appears on the Data tab).

9. Click the Properties tab. If necessary, click the down-facing arrows next to the Universe, so that the CA SDM text is displayed with an ellipse (…).

10. Click the ellipse (...) button to display the Universe dialog.
    The Other Available Universes window appears.

11. Select the name of your universe and click OK.
    Web Intelligence will automatically map all known fields from the CA SDM universe to your universe and display the Change Source dialog. Green check boxes appear next to each mapped field. If all fields are mapped correctly, click OK to confirm the change. If any fields are displayed with a red "X", click the ellipse (...) button next to the field name, and select the appropriate field.

12. From the Web Intelligence toobar, click Edit Report, and select the Properties tab.

13. Expand the General node.

14. Click the ellipse (...) button next to the Document Properties value.
    The Document Properties dialog appears.

15. In the Document Options section, select the Refresh on Open check box.

16. Click Save and then close Web Intelligence.
    The report is associated with the appropriate universe and can be modified as needed.

Create a Crystal Report

Use Crystal Reports to save a report in the CA Business Intelligence Universe.

Follow these steps:

1. Launch Crystal Reports XI.

2. Select File, New, Blank Report.
   The Database Expert dialog appears.

3. Expand the Create new Connection node and click Universes.
   The Business Objects Enterprise dialog appears.

4. Log on to BusinessObjects Enterprise using your administrator credentials.

5. Navigate to the folder containing the derived universe.

6. Select the derived universe and click Open.
   The Business Objects Query Panel dialog appears.

7. In the Universe tree structure, drag and drop the appropriate attributes into the Select and Filter sections of the Query panel.

8. When the query building process is complete, the standard Crystal Reports designer tool is presented.

9. Build and run the report.

   Note: For more information about building and running reports, see Crystal Reports documentation.

10. Save the report in the Business Objects Enterprise repository as follows:

    a. Select File, Save as.

    b. In the Save As dialog, select Enterprise.

    c. Navigate to the folder created when you defined your development framework, and save the new report in BusinessObjects Enterprise.

    The new report is now available in the enterprise, and can be modified as needed.

Modify a Crystal Report

Use Crystal Reports to modify a report in the CA Business Intelligence Universe.

Follow these steps:

1. Open Crystal Reports XI.

2. Select File, New, Blank Report.
   The database expert dialog displays.

3. Click to expand Create new Connection.
   Click Universes.
   The Business Objects Enterprise dialog displays.

4. Log on to Business Objects Enterprise as administrator.

5. Click to navigate the folder housing the derived universe and click to select the derived universe.
   Click Open.
   The Business Objects Query Panel dialog displays.

6. Navigate the universe tree structure to find, drag, and drop attributes to the select and filter portions of the query panel.
   When the query building process is complete, the report writer is presented with the standard Crystal Reports designer tool.

7. Build and run the report as per Crystal Reports instructions.

8. When ready, save the report to the Business Objects Enterprise repository.

   a. Choose File, Save as
      The Save as dialog displays.

   b. On the left side of the save as dialog, click the Enterprise icon.

   c. Navigate the folder structure starting with the customer-specific folder created earlier in this document and click Save to save this report in Business Objects Enterprise.

9. The new report is now available in the enterprise, and can be modified as needed.

Schema Changes to the Infrastructure

This article contains the following topics:

After the CA BI development environment is established and schema changes have been published to CA SDM using the documented process for customizing schema data, the schema changes are ready to be promoted through the CA BI infrastructure. You can make the new schema available for report creation and modification.

Add Schema Changes to Derived Universe

Promoting schema changes into the CA BI infrastructure is as straight-forward as adding the new schema object to the derived universe.

Note: Before you begin, verify that the appropriate steps have already been completed, and the new schema objects have been added to the CA SDM flexible schema.

Follow these steps:

1. Open the BusinessObjects Designer, and import the derived universe to a local file system as follows:

   a. Select File, Import from the Designer menu.
      The Universe Successfully Imported dialog appears.

   b. Click OK.

2. Refresh the structure of the derived universe as follows:

   - Select View, Refresh Structure from the Designer menu.
     The following questions appear:

     - "Do you want to refresh the out of date columns in selected tables?" Click OK.

     > **Note**: If the message "No update needed" appears, it means the CA SDM object layer has not been appropriately updated with the new schema. Review the steps for publishing schema changes to CA SDM.

   - "Refresh structure: The structure has been successfully modified." Click OK.

   New columns appear in the universe structure on the right side of the window, making new object(s) available for use within the derived universe.
   The objects are available to the CA BI tools after they are moved from the right pane to the left pane. When you add objects to the left pane, make sure that you follow the common schema modifications (see page 1833) standards.

3. Drag and drop the new object(s) to the desired location in the left pane.

4. Click Save.

5. Select File, Export from the Designer menu.
   The Universe Successfully Exported dialog appears.

6. Click OK.
   Changes added to the derived universe schema are exported to the local CMS.

7. From the Designer menu, select Tools, Check Integrity.

   a. In the dialog that appears, select the Parse Objects check box. (Do not change other settings.)

   b. Click OK. The integrity check is started.

   > **Note**: No parse errors should be reported. If errors are found, modify your objects in the left pane so that they do not produce parse errors.

8. Click OK to close the dialog.

9. Export the derived universe to the CMS as follows:

   a. Select File, Export from the Designer menu.

   b. From Domain field drop-down list, select <Browse>, and then locate and select CA Customer Universes.

c. Click OK to export the universe to the local CMS.

The Universe Successfully Exported dialog appears.

10. Save your changes and export the CA SDM universe.
The changes are now available in your CA BI reporting environment, including Web Intelligence and Crystal Reports.

Common Schema Modifications

You can implement schema modifications in the Universe. To familiarize you with the process, the following table lists the common schema modifications that you might encounter.

When a field type is defined in Web Screen Painter as...	Follow these rules when using the field in the Universe: Right click the attribute and select...
INTEGER	Object Properties, Definition Tab, Type = Number
STRING	Object Properties, Definition Tab, Type = Character
DATE	Object Properties, Definition Tab, Type = Date Object Format, Number Tab: Choose category "Date/Time"; Choose Format mm/dd/yyyy hh:mm:ss AM/PM
DURATION	Object Properties, Definition Tab, Type = Number; Object Properties, Definition Tab, Select = PdmSeconds(object.attr)
SREL	Create a CA SDM attribute alias.
BREL	Not Applicable
QREL	Not Applicable
DERIVED	Use an appropriate data type and object format for the value stored in the derived field, if desired. The Derived field can produce any result, so there is not a specific standard to follow.
Special Case: Local This is not a data type defined within Web Screen Painter, but instead a data type used by the universe sometimes to indicate an unsupported data type.	The Local field is displayed in the right pane of the universe with type "L". These fields can be dragged, but not dropped into a class on the right universe pane. Most often, fields data types such as binary, are not supported by the Universe. However, they can be added to the left pane of the universe by creating an object and placing the PdmString (object. attribute) in the "SELECT" window of the Edit Properties dialog.

Legacy Reports Modification

CA SDM lets you modify legacy reports or design your own reports. You can:

- Modify legacy Summary, Detail, and Analysis reports to contain exactly the information you need, such as additional fields.

- Produce a new report with any information available from the database in a format that is useful to you.
- Pass arguments of variable information into the report by including command line arguments. Arguments can be values or expressions, such as the current value of a field or an SQL WHERE clause expression.
- Generate reports at the command line, from a script file, or from a menu option.

Follow these steps:

1. Design the report:
   - Decide what data you want to include in the report.
   - Create a report template that contains SQL-like queries, expressions, and functions to manipulate data, and statements to format the data for the printed page.
2. Generate the report from:
   - The command line
   - A CA SDM menu option
   - A script file

Note: If you have a third-party database system you can use its report generating tools to create reports with data from the CA SDM database. CA SDM provides several database views that simplify the process of creating modified reports using third-party database systems. See the documentation for your database system for information about reporting on databases. For more information about database views, see the *Reporting (see page 3180)* section.

Modify Crystal Reports

Before you can display any of these reports, the following conditions apply:

- You must make the Crystal reports available to the Crystal Report Selector by copying them to the Crystal directory: $NX_ROOT/bopcfg/rpt.
- Your database client must be up and running, with connectivity established to the database server running on the same or another computer. If you are using a CA SDM Client to run your Crystal or Access reports you need to have installed a database client for the specific database and have established connectivity with the database server in order to run these reports.

After creating any custom Crystal reports, perform the following:

1. Copy custom Crystal reports to the following crystal directory:

```
$NX_ROOT/bopcfg/rpt
```

2. Add the file names of custom Crystal reports to the following configuration file:

```
crystal.cfg
```

You can then access the Crystal reports by clicking Start on the taskbar, and then choosing Reporting, Service Desk Reporting (Crystal Reports) from the CA SDM menu (accessible from the Programs menu). The Service Desk Reporting (Crystal) window appears.

Important! CA SDM clients cannot be upgraded. Therefore, if you create and use Crystal reports on the CA SDM Server and you plan to upgrade your version of CA SDM, you need to copy all custom reports to a different location so you will not lose them. Following the upgrade, copy the reports back to the $NX_ROOT/bopcfg/rpt Crystal directory and modify the crystal.config file to make them accessible from the Report Selector.

Custom Report Design

This article contains the following topics:

To design a custom report, you must have a basic understanding of the following concepts:

- Writing SQL queries.
- Programming, especially in C.
- Creating special programs or script files that you may need to execute before you execute the report template program. For example, you may want to create a program that prompts the user to enter an argument, such as the conditions for a WHERE clause.

Note: Before you create a custom report, be sure to check if the report you need is already provided. CA SDM provides a wide variety of Crystal and Microsoft Access reports, and runtime versions of these products to let you run the reports. For more information about reports, see the Reporting Using CA Service Desk Manager (see page 3180) section.

Selecting Information for the Report

To help you select data from the CA SDM database for customized reports, see CA Service Desk Manager Reference Commands (see page 3496). It lists database tables, fields, descriptions, and other database information.

How to Create a Report Template

A report template is a file that, when executed by a CA SDM report program, generates a report of a particular design. A report template contains variable expressions, functions, and statements that define how the data is fetched, calculated, and printed.

To create a report template, create a file containing the following types of report statements:

- **Block statements**
  Defines the CA SDM database tables from which data will be fetched and the actions that are to be performed on the fetched data.

- **Layout statements**
  Defines how the data variables and literal text display on the report output.

Note: Store all your .rpt files in a new directory, $NX_ROOT/site/mods/rpt (UNIX) or *installation-directory*\site\mods\rpt (Windows). This directory preserves them when you upgrade to a new release of CA SDM.

Block Statements

Block statements provide the report template with its framework. They define the data to be manipulated and control the execution of the report. Block statements begin with a name that must be unique throughout the report template. They then have the following two sections:

- **Data query section**
  Contains SQL SELECT, WHERE, and SORT clauses to define which data is fetched from the database.

- **Output program section**
  Defines the actions that are to be performed on the fetched data. It contains variable declarations, functions, and other block statements, including nested statements, which can be used to create conditional reports. It can also contain layout statements, which format and print the data as ASCII text.

A simplified version of the syntax of a block statement that shows the relationship between the two sections follows:

```
BLOCK blockname ("SELECT clause", "WHERE clause")
   SORT clause {output program statements}
```

The BLOCK (see page 1847) in the Reference section discusses the detailed version of the syntax, along with a description of each clause and parameter.

Layout Statements in Report Templates

Layout statements define how variables and literal text will appear on the report output:

- You can use the PAGE HEADER and PAGE FOOTER statements to place information at the top and bottom of each report page.
- You can nest HEADER, HEADER2, FOOTER, and PRINT statements within the braces section of the parent BLOCK statement to create titles and summary totals for the various *reporting sections* (parts of the report output).

  Note: When nesting, be careful not to confuse the braces used in layout statements with the braces that encompass the nested statements within a parent BLOCK statement.

- You can include literal text to create labels and line drawing characters to enhance the appearance of the report.

The layout statements are as follows:

- **PAGE HEADER**
  Places information at the top of each report page. It is placed outside the BLOCK statement.
- **PAGE FOOTER**
  Places information at the bottom of each report page. It is placed outside the BLOCK statement.
- **HEADER**
  Places information at the top of each reporting section. It is placed inside the BLOCK statement.
- **HEADER2**
  Places continuation header information at the top of each succeeding page of a reporting section, if that reporting section extends over multiple pages. It is placed inside the BLOCK statement.
- **FOOTER**
  Places information at the bottom of each reporting section. It is placed inside the BLOCK statement.
- **PRINT**
  Places the data in a reporting section. It is placed inside the BLOCK statement.

You can also use the following predefined variables in layout statements:

- CT prints the current time
- CD prints the current date
- PG prints the page number
- **Data Fields**
  Specifies any variable in a layout statement that results in a piece of data when you generate the report. Use the following guidelines when placing fields in your report template:

- Enclose data fields in square brackets ([ ]).
- The field's square brackets define its print space on each line of output. This space is the number of characters delimited by the square brackets, including the brackets. If the output of a variable is longer than the print space, the output is truncated. To ensure that the field has enough print space, you can add trailing spaces between the variable name and the closing bracket. For example, these trailing spaces allow for contacts with long names:

```
[contact          ]
```

- For output that is less than one line, the field can be closed with a greater than right angle bracket (>). This extends the print space to the right margin. For example, the right angle bracket used in a HEADER statement allows the current date to print without being truncated:

```
[CD               >
```

Note: When the field is more than one line and the variable is flagged as MULTILINE, the right angle bracket (>) acts exactly the same as the right square bracket (]). If the print statement for a MULTILINE variable is closed with the right angle bracket (>), characters wrap on white space to stay within the field defined by the left bracket ([) and the right angle bracket (>). Also, if the variable is not MULTILINE, the right angle bracket (>) causes all the data to be displayed on the current line regardless of its length.

- A field in a layout statement can refer to a previously defined variable or a column name.
- To reference a variable or column name in another block statement, use the following syntax:

```
blockname::column | variable-name
```

- **Literal Text**
  Literal text allows you to include supplementary information in your report. It will appear on the report output exactly as specified in the template. To include literal text in a layout statement, place it on any line after the opening brace ({) and before the closing brace (}). Do not enclose it in quotes or square brackets.
  In this example, "ACME Company" and "Page: " are interpreted as literal text by the CA SDM report program:

```
PAGE HEADER {

               ACME Company          Page: [PG]

}
```

Variable Expressions in Report Templates

Every value that you want to appear on the report output can be assigned to a variable. Variable expressions let you:

- Manipulate CA SDM data

- Use functions to perform calculations on fetched values

The following example creates a variable named *desc* to reference the contents of the chg_desc field in the Change Order window. The MULTILINE flag allows the variable to print in its entirety over multiple lines:

```
desc = description MULTILINE;
```

The following example prints the description. The output will be as long as the length defined in the brackets. If you want a longer description to appear, increase the number of spaces in the brackets.

```
PRINT { [desc  ]                                  }
```

Example Report Template

The following Affected Contact Report template shows how to create a report template. It produces a report that lists open change orders with the same affected contact:

```
PAGE HEADER {
                                                        As Of: [CD>
                                                               [CT>
}
PAGE FOOTER {
                          Page: [PG>
}
BLOCK chg ("SELECT \
        chg_ref_num, description, priority, \
        status, category, assignee \
      FROM Change_Request",
    "WHERE #Change_Request.status = 'OP' \
AND #Change_Request.requestor = #ca_contact.id \
AND #ca_contact.last_name = ? \
AND #ca_contact.first_name = ? \
AND #ca_contact.middle_name = ? " , $1, $2, $3)
{
    BLOCK st ("SELECT sym FROM Change_Status",
            "WHERE code = ? ", chg::status) {}
    BLOCK (strlen(category)) cat ("SELECT sym FROM Change_Category",
                    "WHERE code = ? ", chg::category) {}
HEADER {
        OPEN CHANGE ORDERS WITH SAME REQUESTOR/FROM CONTACT
CHANGE ORDER Summary          Pri   Status    Category          Assignee
}
HEADER2 {
CHANGE ORDER Summary          Pri   Status    Category          Assignee
-------------------------------------------------------------------------
}
    num = chg_ref_num;
    desc = description MULTILINE;
    pr = deref (priority);
    stat = st::sym;
    catgry = cat::sym;
    asgn = deref (assignee);
```

```
PRINT {
[num      ] [desc            ][pr ] [stat    ] [catgry          ] [asgn ]
}
}
```

- **Page Header**
  Specifies what to print on the top of each page of the report. CD and CT are predefined variables that give the current date and time. They will appear in the header on the top of each page. Each of these fields ends with an angle bracket, which allows the field to expand towards the right margin. Because “As Of:” is outside of a field and because it is on a line after the opening brace, it will appear as literal text on the report output.

```
PAGE HEADER {                              As Of:  [CD>

                                                   [CT>

}
```

- **Page Footer**
  Includes the page number with “Page: ” as literal text.

```
PAGE FOOTER {

                                Page: [PG>

}
```

> **Note:** Since PAGE HEADER and PAGE FOOTER statements produce global headers and footers, they are not included in a BLOCK statement.

- **Reporting Section**
  Creates a reporting section for the main BLOCK statement, along with its nested statements. A reporting section is usually only part of the data in the report, but this report has only one reporting section. The unique name of this block is chg.
  The SELECT clause selects the columns to be included in the data for the report FROM three tables, but only where conditions specified by the WHERE clause are met.
  The last three AND expressions in the WHERE clause contain question marks, which act as argument placeholders that take the values of the $1, $2, and $3 arguments, in order. Thus $1 is for ca_contact.last_name, $2 is for ca_contact.first_name, and $3 is for ca_contact.middle_name. The $1, $2, and $3 arguments obtain the values of command line arguments.

```
BLOCK chg ("SELECT \

...",

"WHERE \

...\

AND #ca_contact.last_name = ? \

AND #ca_contact.first_name = ? \

AND #ca_contact.middle_name = ? ", $1, $2, $3)
```

- **Reporting Section Headers**
  Specifies that the opening brace starts the output program part of the BLOCK statement: its statements tell what to do with the data fetched by the SELECT and WHERE clauses. This example has nested HEADER and HEADER2 statements that will apply to this reporting section only. HEADER2 prints only if the report output is on multiple pages.

```
{

   ...

   HEADER {

            OPEN CHANGE ORDERS WITH SAME REQUESTOR/FROM CONTACT

CHANGE ORDER Summary           Pri    Status  Category  Assignee

}

   HEADER2 {

CHANGE ORDER Summary           Pri    Status  Category  Assignee

------------------------------------------------------------------

}
```

- **Variable Assignments**
  Specifies variable expressions that act on the data specified by the SELECT clauses. They assign variables to the values of columns and to the results of expressions. These variables match the fields in the PRINT statement that follows.
  The MULTILINE flag on the *desc* variable causes them to print or display on multiple lines rather than being truncated. The deref function is used to return the string expression contained in the referenced columns.

```
num = chg_ref_num;

desc = description MULTILINE;

pr = deref (priority);

stat = st::sym;

catgry = cat::sym;

asgn = deref (assignee);
```

- **Printing**
  Contains the fields to be printed. This statement could have also included literal text of lines that could enhance the appearance of the report. The final ending brace matches the opening brace of the output program section of the BLOCK statement.

```
PRINT {

[num ] [desc         ] [pr]  [stat] [catgry] [asgn         ]


}

}
```

Report Template Reference

You can use variable expressions, functions, and statements in a report template.

This section contains the following articles:

Variable Expressions

This article contains the following topics:

Variable expressions define the data to be printed or displayed in a report template. They are placed in a layout or block statement.

Variable Expression Syntax

Syntax refers to the rules governing the formation of statements in a programming language. The structure of this string is as follows:

```
variable-name = expression [flags]
```

Variable Expression Flags

Flags format the result of a variable expression. Use these flags to format text fields:

- **MULTILINE**
  Displays on multiple lines rather than truncating.

- **RIGHT**
  Right justifies.

Use these flags to format numeric fields:

- **BLANKZERO**
  Functions as null-value fields, which do not print a zero.

- **BOOL**
  Converts zero to no or non-zero to yes.

- **REAL**
  Displays as floating point (default is integer).

- **ZEROFILL**
  Shows leading or trailing zeros

Use these flags to format date and time fields:

- **DATE**
  Shows only date portion of date/time.

- **DAYS**
  Displays durations with days.

- **HOURS**
  Displays durations with hours.

- **MINUTES**
  Displays durations with minutes.

- **SECONDS**
  Displays durations with seconds.

- **TIME**
  Shows only time portion of date/time.

Variable Expression Example

The following line displays a Variable Expression example:

```
desc = description MULTILINE
```

Variable Expression Remarks

Variable names must be unique within a BLOCK statement and must not duplicate any column in the SELECT clause for the block. The same variable name can be used in different BLOCK statements but it cannot be repeated within a BLOCK statement.

Follow these syntax rules when including expressions in your report template:

- Use any valid C expression.

- Do not enclose variable or column names in quotes.

- Enclose string constants in single or double quotes.

- You can refer to a nested block, but only if it contains exactly one row.

- To include a column name that is the same as a keyword, precede the column name with a backslash (\). For example, ALIAS is a keyword and \alias is a column name.
- Use the dollar sign ($) to reference environment variables, such as $name, and to reference command line arguments, such as $*n*, where *n* is the position of the argument on the command line.
- To specify the number of command line arguments, use $#. For example, the following expression means that if the number of command line arguments is greater than one, use the additional argument as an argument; otherwise, set the value of the argument to an empty string. The report template itself is considered a command line argument. Therefore, the number of arguments is at least one.

```
$# > 1 ? $1 : "
```

- Use ## to concatenate two strings, for example:

```
title = "This is the " ## "first line. "

long_name = fn

irst_name ## last_name
```

- The following casts are supported:
  - (number)
  - (string)
  - (date_time)
  - (duration)
- To reference a variable or column name in another block, precede the name with its block name and two colons. For example:

```
blockname::column | variable-name
```

Report Template Functions

The following functions can be used in your report template:

- **is_null (*expr*)**
  This function returns true if the expression is null.

```
false = 0

true = is_null (false)
```

- **sqrt (*expr*)**
  This function calculates the square root of the expression.

```
nine = 9

three = sqrt (nine)
```

- **pow (*expr1, expr2*)**
  This function raises *expr1* to the power *expr2.*

```
two = 2

three = 3

eight = pow (two,three)
```

- **log (*expr, expr*)**
  This function calculates the natural log of the expression.

```
ten = 10

result = log (ten)
```

- **catname (*expr*, *expr*, *expr*)**
  This concatenates three strings representing a contact name into a string with commas, according to rules in the field format file.

```
last = "Murphy"

first = "Fred"

middle = "P"

contact_name=catname (last, first, middle)
```

- **strlen (*string*)**
  This function returns the length of the string.

```
buffer = "A thirty character long string"

thirty = strlen(buffer)
```

- **strindex *(string, pattern [, start_index]*)**
  This function returns the index of the first pattern match, or the next pattern match after the start_index, in the string. Returns -1 if there is no match.

```
buffer = "A thirty character long string"

zero = strindex(buffer, " [A-Z] ")

two = strindex(buffer, " [a-z] ")
```

- **substr (*string, pattern [, length]*)**
  This function returns the portion of the string after the first pattern match. It length is defined, it limits the length of the output string. Returns a string of zero length, if there is no match.

```
buffer = "A thirty character long string"

last_word = substr(buffer, " [a-z]*$ ")

first_capital_letter = substr(buffer, " [A-Z] ",

    1)
```

- **substr *(string, index [, length]*)**
  This function returns the portion of the string after the index. Its length is defined and limits the length of the output string. Returns a string of zero length, if there is no match.

```
buffer = "Summary: The network card displays a

    code of ... "

summary = substr(buffer, 9)

30_char_summary = strindex(buffer, 9, 30)
```

The remaining functions (pseudofunctions) perform on a block of data rather than on variable expressions. These functions are usually placed in a BLOCK statement to get information about a nested BLOCK statement's data.

- **count (*block-name*)**
  Returns the number of rows in the block specified in the BLOCK statement. The block-name must be a simple string.

```
BLOCK sample ("SELECT id  FROM Contact") {

entries = count (sample)

}
```

- **sum (*block-name, expr*)**
  Executes the expression for each row of the specified block and sums the result.

```
BLOCK sample ("SELECT actual_cost, est_cost FROM Change_Request") {

difference = sum (sample, est_cost-actual_cost)

}
```

- **average (*block-name*, *expr*)**
  Executes the expression for each row of the block and returns the average of the result.

```
BLOCK sample ("SELECT actual_cost, est_cost FROM Change_Request"){

avg_difference = average (sample, est_cost-actual_cost)

}
```

- **prev (*expr*)**
  Returns the previous value of the expression. This function should be used with caution so its value does not overwrite the latest value by accident.

- **downtime *(sla_schedule, expr1, expr2 [, delay-block, expr, expr]*)**
  Invokes an SLA downtime calculation. The first argument must be a string that identifies a workshift. The other arguments are start and end times:
  expr1 is the start date/time of the event
  expr2 is the end date/time of the event
  In this example, the wrkshft BLOCK fetches the work shift schedule, the evt_dly BLOCK statement fetches the delays and the downtime function uses these records to calculate the downtime.
  BLOCK attevt ("SELECT start_time, fire_time, event_tmpl, obj_id FROM Attached_Events")

```
{
BLOCK evt ("SELECT persid, sym, work_shift FROM Events ", "WHERE persid = ?", attevt::event_tmpl) {}
BLOCK wrkshft ("SELECT sched FROM Bop_Workshift", "WHERE persid = ?", evt::work_shift) {}

BLOCK evt_dly ("SELECT start_time, stop_time FROM Event_Delay", "WHERE obj_id = ?", attevt::obj_id) {}
total_downtime = downtime(wrkshft::sched,
attevt::start_time,  attevt::fire_time,
evt_dly,
evt_dly::start_time, evt_dly::stop_time);
}
```

- **deref (*column-name*)**
  Returns the string representation of the pointer by performing an automatic lookup in the appropriate table.

```
BLOCK chg ("SELECT organization FROM Change_Request") {
org = deref (organization)
}
```

Because this pseudofunction involves lookups, it is valid only if it is the only thing in the expression. For example, this is valid:

```
model = deref (nr_model)
This is not valid:
model = "model"  ## deref (nr_model)
```

Note: Forward references to variables or blocks are not allowed.

Report Template BLOCK Statements

This article contains the following topics:

Block statements define the database tables from which data will be fetched, and can include actions to perform on the fetched data.

Block Statement Syntax

Syntax refers to the rules governing the formation of statements in a programming language. The structure of this string for BLOCK is as follows:

```
BLOCK blockname (
       "SELECT [ALIAS,] field_name[, field_name ...]
       FROM table_name[, table_name ...] "
       [,"WHERE where_clause"][, arguments,] )
       [SORT "sort clause"]
{
output program statements
}
```

Block Statement Parameters

- ***blockname***
  Identifies the block. Each *blockname* must be unique.

- **SELECT clause**
  Follows the *blockname* and is delimited by double quotes. Lists the columns to be fetched, followed by the keyword FROM, followed by the tables from which the columns are to be fetched. It is required. Here is an example with three tables specified:

  ```
  "SELECT open_date, chg_ref_num \

  last_name, first_name \

  FROM Change_Request, \

  ca_contact"
  ```

  You cannot include an SQL alias, such as:

  ```
  "SELECT open_date As OpenDate"
  ```

- **WHERE clause**
  (Optional) Follows the SELECT clause and further qualifies the information selected. It may be a string constant or an expression evaluating to a string. If the WHERE clause is an empty string, all records are returned. WHERE clauses can contain replacement arguments (which refer to variables or command line arguments) using the syntax of a question mark (?). The following WHERE clause could follow the previous SELECT clause:

  ```
  "WHERE #Change_Request.open_date >= ? \

  AND #Change_Request.active_flag = 1 \

  AND #ca_contact.last_name = ? ", $1
  ```

  Note: The WHERE clause must be separate from the SELECT clause because the WHERE clause can be an expression evaluating to a string, whereas the SELECT clause is exclusively a string constant. This gives you more flexibility and data manipulation capabilities in producing your report.

- **SORT clause**
  (Optional) Follows the SELECT and WHERE clauses and sorts the fetched rows of data. The SORT clause is formatted like the SQL ORDER BY clause. Here is an example:

```
SORT "open_date"
```

- **Output program statements**
  Controls execution of the report. Before the data query, the HEADER statement, if included, prints the heater test for the block. The data query then runs. If data is returned, each statement executes in the order written, with one exception. Block functions, like sum and average, behave as thought they were at the end of the output program. In fact, their values are not stable until execution begins on the next data record.

Important! The output program depends on the success of the data query. If no data is returned from the query, then, except for the HEADER statement, the output program will not execute.

Block Statement Example

This BLOCK statement assumes that an argument will be passed that holds an integer equal to the change order priority. The WHERE clause first checks the number of arguments passed ($#). If one is present, it is used to evaluate the expression to produce the WHERE clause; otherwise a null WHERE clause is substituted (" ").

```
BLOCK chg ("SELECT priority FROM Change_Request",
$# > 1 ? "WHERE priority =" ## $1 :  "") {}
```

Footer Statement Example

The following lines display a Footer Statement example:

```
FOOTER {
     Summary Information:
             Total Failures:  [Fail_count >
             Total Downtime:  [Downtime >
}
```

Block Statement Remarks

HEADER, HEADER2, FOOTER, PRINT and variable expressions can be placed in the braces. Any statement will be executed for each row selected.

Note: PAGE HEADER and PAGE FOOTER statements cannot be placed in a BLOCK statement.

Report Template FOOTER Statements

This article contains the following topics:

This layout statement places information at the bottom of a reporting section.

Footer Statement Syntax

Syntax refers to the rules governing the formation of statements in a programming language. The structure of this string for FOOTER is as follows:

```
FOOTER {parameters}
```

Footer Statement Parameters

The parameters are as follows:

- **CD**
  A predefined variable used to display the current date.
- **CT**
  A predefined variable used to display the current time.
- **PG**
  A predefined variable used to display the current page number.
- **column | variable-name**
  This field can be a variable from an earlier variable expression or a reference to a column in the SQL clause of a BLOCK statement.
- **literal-text**
  Any text that is not a predefined variable or a column or variable name is interpreted as literal text. Literal text that you include in the FOOTER statement appears in the exact horizontal location where you enter it.

Footer Statement Remarks

FOOTER statements are printed at the bottom of a reporting section. A typical use might be to present summary information or statistics. You can include a FOOTER statement in a BLOCK statement.

A field's content occupies the exact space delineated by the square brackets. Any excess characters are truncated. However, you can close a field with an angle bracket (>) to permit its content to expand in its entirety towards the right margin.

To reference a variable or column name in another BLOCK statement, use the following syntax:

```
blockname::column | variable-name
```

HEADER

This article contains the following topics:

This layout statement places information at the top of a reporting section.

Header Statement Syntax

Syntax refers to the rules governing the formation of statements in a programming language. The structure of this string for HEADER is as follows:

```
HEADER {parameters}
```

Header Statement Parameters

For a list and explanation of the valid parameters for this statement, see Report Template PAGE HEADER Statements (see page 1853).

Header Statement Example

The following lines display a Header Statement example:

```
HEADER {
                 Contact Summary Report
     Contact Name   Contact Alias   Organization
}
```

Header Statement Remarks

HEADERS are printed at the beginning of a reporting section and can be included in a BLOCK statement. HEADERS are typically used to present section and/or column headings.

A field's content occupies the exact space delineated by the square brackets. Any excess characters are truncated. However, you can close a field with an angle bracket (>) to permit its content to expand in its entirety towards the right margin.

Note: If the print statement for a MULTILINE variable is closed with the right angle bracket (>), characters wrap on white space to stay within the field defined by the left bracket ([) and the right angle bracket (>). Also, if the variable is not MULTILINE, the right angle bracket (>) causes all the data to be displayed on the current line regardless of its length.

To reference a variable or column name in another BLOCK statement, use the following syntax:

```
blockname::column | variable-name
```

Report Template HEADER2 Statements

This article contains the following topics:

This layout statement places continuation HEADER information at the top of each succeeding page of a reporting section, if that reporting section extends over multiple pages.

Header2 Statement Syntax

Syntax refers to the rules governing the formation of statements in a programming language. The structure of this string for HEADER2 is as follows:

```
HEADER2{parameters}
```

Header2 Statement Parameters

For a list and explanation of the valid parameters for this statement, see Report Template HEADER2 Statements (see page 1851).

Header2 Statement Example

```
HEADER2 {
   Contact Summary Report (continued)
   Contact Name   Contact Alias   Organization
}
```

Header2 Statement Remarks

A HEADER2 statement can be included in a BLOCK statement.

A field's content occupies the exact space delineated by the square brackets. Any excess characters are truncated. However, you can close a field with an angle bracket (>) to permit its content to expand in its entirety towards the right margin.

To reference a variable or column name in another BLOCK statement, use the following syntax:

```
blockname::column | variable-name
```

Report Template PAGE FOOTER Statements

This article contains the following topics:

This layout statement places information at the bottom of each report page.

Page Footer Statement Syntax

```
PAGE FOOTER {parameters}
```

Page Footer Statement Parameters

With the exception that you cannot use column and variable names, the parameters for this statement are the same as those for FOOTER. For a list and explanation of the valid parameters for this statement, see Report Template PAGE FOOTER Statements (see page 1852).

Parameters for a Page Footer Statement Example

```
PAGE FOOTER {
                Page Number: [PG>
}
```

Parameters for a Page Footer Statement Remarks

A field's content occupies the exact space delineated by the square brackets. Any excess characters are truncated. However, you can close a field with an angle bracket (>) to permit its content to expand in its entirety towards the right margin.

To reference a variable or column name in another BLOCK statement, use the following syntax:

```
blockname::column | variable-name
```

Report Template PAGE HEADER Statements

This article contains the following topics:

This layout statement places information at the top of each report page.

Page Header Statement Syntax

Syntax refers to the rules governing the formation of statements in a programming language. The structure of this string for PAGE HEADER is as follows:

```
PAGE HEADER {parameters}
```

Page Header Statement Parameters

With the exception that you cannot use column and variable names, the parameters for this statement are the same as those for FOOTER. For a list and explanation of the valid parameters for this statement, see Report Template PAGE FOOTER Statements (see page 1852).

Page Header Statement Example

```
PAGE HEADER {
   Date of Report:  [CD>
   Time of Report:  [CT>
}
```

Page Header Statement Remarks

PAGE HEADERS are printed at the top of every report page. They can be defined at any point within the report template file, but they cannot be included within a BLOCK statement.

A field's content occupies the exact space delineated by the square brackets. Any excess characters are truncated. However, you can close a field with an angle bracket (>) to permit its content to expand in its entirety towards the right margin.

To reference a variable or column name in another BLOCK statement, use the following syntax:

```
blockname::column | variable-name
```

Report Template PRINT Statements

This article contains the following topics:

This layout statement places data in a reporting section.

Print Statement Syntax

Syntax refers to the rules governing the formation of statements in a programming language. The structure of this string for PRINT is as follows:

```
PRINT {parameters}
```

Print Statement Parameters

Refer FOOTER (see page 1849) for a list and explanation of the valid parameters for this statement.

Print Statement Example

```
PRINT {
[num ] [desc          ] [pr]  [stat] [catgry] [asgn              ]
}
```

Print Statement Remarks

Place PRINT where you want the data for a reporting section to appear in the report. You can include a PRINT statement in a BLOCK statement.

A field's content occupies the exact space delineated by the square brackets. Any excess characters are truncated. However, you can close a field with an angle bracket (>) to permit its content to expand in its entirety towards the right margin.

> **Note:** If the print statement for a MULTILINE variable is closed with the right angle bracket (>), characters wrap on white space to stay within the field defined by the left bracket ([) and the right angle bracket (>). Also, if the variable is not MULTILINE, the right angle bracket (>) causes all the data to be displayed on the current line regardless of its length.

To reference a variable or column name in another BLOCK statement, use the following syntax:

```
blockname::column | variable-name
```

Web Services Management

This article contains the following topics:

Web Services are a set of data exchange standards that enable communication between products, even if they are on different operating environments. This ability is analogous to browsing the Web on a personal computer -- all remote websites are accessible regardless of whether they are hosted on Solaris, AIX, Windows, and so on. In the same manner, Web Services allow products to communicate over HTTP to various servers regardless of operating environment. For example, a Microsoft Office product can communicate with a program on a UNIX server, and a Java Server Page can access a server hosted on a Windows server. This platform-neutral communication allows for powerful integrations.

The Web Services take advantage of this technology, allowing almost any product to access CA SDM and Knowledge Management. Web Services clients can create tickets, update assets, search the knowledge base, and so forth.

> **Important!** For additional information on web services, see the CA SDM Reference (see page 3496).

CA SDM Components

CA SDM provides the installation files for this version of the J2EE Web Services in the following directory:

```
<NX_ROOT>/sdk/websvc/R11
```

Note: <NX_ROOT> specifies the root installation path for CA SDM.

Web Service Options

These options control the web service session:

- **rest_webservice_access_duration**
  Specifies the number of hours that the REST Web Service Access Key remains active before expiration. The Access Key timeout is not based on inactivity time, but it is based on duration time since the Access Key creation. After the Access Key meets the specified duration, the Access Key ends regardless of whether it is being used.
  Optionally, the REST client can also provide the Access Key duration time for the specific Access Key during the Access Key request. To provide the duration value, set it directly on the expiration_date attribute of the rest_access resource, as part of the POST request payload.
  Valid Range: 1-8760 hours
  Defaut: 168

- **rest_webservice_disable_basic_auth**
  Disables Basic Authentication in REST Web Services.
  Default: No

- **rest_webservice_list_max_length**
  Specifies the maximum number of rows that a REST Web Service query returns.
  Default: 500

- **rest_webservice_list_page_length**
  Specifies the default number of rows that a REST Web Service query returns per page.
  Valid Range: 1-500
  Default: 25

- **rest_webservice_resources_to_expose**
  Specifies the list of Majic factories (resources) that CA SDM exposes through REST Web Services. This option overrides the default behavior. By default, CA SDM exposes all factories through REST Web Services.
  If you do not enter values in this option, the default behavior exposes any Majic factory that does not have the REST_OPERATIONS property set to NONE. By default, no Majic fatory has this property set to NONE.
  Use the REST_OPERATIONS property to set the specific HTTP CRUD (CREATE, READ, UPDATE, DELETE) methods for CA SDM to expose on a given Majic factory.
  Default: rest_access
  Example: rest_access, cnt, grp, cr, crs, pri, alg, urg, imp, pcat, org

- **hmac_algorithm**
  Specifies the algorithm that you use to compute the signature for Custom/Secret Key Auhentication in REST Web Services.
  Default: HmacSHA1

- **string_to_sign_fields**
  Specifies the fields that you use to compute the signature for Custom/Secret Key Authentication in REST Web Services, in addition to the default REQUEST_METHOD, REQUEST_URI, and QUERY_STRING fields.
  Default: blank

- **webservice_domsrvr**
  Specifies the name of the object engine that SOAP web services use. If not installed, SOAP web services use "domsrvr".
  The value of the option must be a string beginning with the characters "domsrvr:"

- **webservice_session_timeout**
  Sets the timeout value (in minutes) for SOAP Web Service sessions. When the time between successive web method calls is greater than the value specified, the session ID is marked expired. The session is then no longer valid.
  To prevent sessions from expiring due to activity, set the value for this option to 0. Other methods, such as logoff routines, can still invalid sessions.

Note: These options require restarting the CA SDM server.

Web Services Installation

Depending on your configuration type, CA SDM installs web services for the following servers:

- Conventional: Both primary and secondary servers. For web service clients to use a URL on a secondary server, you add a web engine to the secondary server

- Advanced Availability: Application server

Web services use the default object manager that is installed on the CA SDM server. To use any other object manager, install and set the *webservice_domsrvr* option in Options Manager.

Note: For information about adding and configuring object managers, web directors, and web engines, see the *Configuring (see page 819)*. For information about installing and setting the *webservice_domsrvr* option, see the Options Manager (see page 1303) section.

How to Activate Design-Time

The CA SDM Web Services includes a method stub configuration feature for developers in the Java version. When activated, the Web Services ignores the CA SDM server and returns simulated data for method calls so that Web Services calls can be made without running a CA SDM server.

Follow these steps:

1. Edit deploy.wsdd to uncomment the sections for “design_mode_stubs”.
2. Reverse the deployment and redeploy the server.
3. Restart the application server.
   The design-time feature is activated.

Note: The design-time feature applies to CA SDM Web Services methods only.

Web Services Security

When you deploy web services, understand the important security considerations. The default configuration when using HTTP is insecure, as it is for all information in web service calls sent between the client and the server in plain text over the network using the HTTP protocol. This includes not only application data, such as ticket descriptions and contact names, but also web service session identifiers (SID). Depending upon the web service application login methods used, it can include passwords.

We recommand that Administrators deploying web services review this information carefully, and to take additional configuration steps at the application and network levels to secure their web service environment.

Important! The default web service configuration used with HTTP is insecure and vulnerable to security threats, which can include password discovery, session fixation, and data spying, among others.

There are three interrelated key security considerations in deploying Web Services:

- What (application level) access authentication schemes should this deployment support?
- What additional networking level security features does this deployment require?
- How will these requirements be enforced through web service configuration options?

The following describes each security feature:

- **Web Service Application Level Authentication Schemes** -- To access Web Services, a web service client application must be authenticated with the web service application. Web Services provides two schemes of access authentication. The first is by username/password, and the other is by Public Key Infrastructure (PKI) technology. Both work with the Access Control and Management component in Web Services, using access policy. Access authentication and access management are the most important security features of Web Services.
  Authentication with username/password methods may be disabled using the following security configuration command:

`disable_user_logon`

Before enabling this option, the administrator needs to determine if each web service client for which an enterprise is requesting Web Services access, can actually provide support for the alternative authentication method, which is the PKI-based login method. The key advantage to the PKI technology is that Web Services client applications do not require *maintained* system user accounts, that is; the maintenance, storage, and transmission of their passwords.

- **Networking Level Security Configuration** -- In both authentication schemes, username/password and Public Key Infrastructure (PKI), notice that the session identifier returned from the specific login method (as well as all subsequent information), are transmitted in plain text when using HTTP. Furthermore, if the username/password authentication scheme is used, the password is sent unprotected (in plain text) from the web service client application to the Web Services. During product development, the W3C did not have recommended standards for web services security. Subsequently, WS-Security is not used by these Web Services implementations to provide a security context. Instead, point-to-point transport layer security (SSL/TLS) and other network level security mechanisms (for example, IPSec), are recommended to protect the otherwise plain text transmission of the application-level authentication exchange(s), and subsequent session identification and data.

  Important! We recommend using SSL (or https) when deploying Web Services to protect the application-level authentication exchanges and subsequent transmissions of session identification and data.

- **Web Service Configuration** -- To allow administrators to enforce communications protocol-level security at the level of the Web Services application, the following two security configuration commands are supported:

  `require_secure_logon`

  This security feature requires you to use SSL (or https) for calling the Login() and LoginService() methods. This feature also provides a handy method for protecting the username and password, while avoiding the overhead of SSL for the rest of the web services.

  Important! If you use the require_secure_logon command, the Web Services application will not confirm that communications protocol-level security is enforced for methods other than Login() and LoginService(). Unless other precautions are taken, the other Web Services methods may be invoked insecurely, causing greater vulnerability to security threats.

  `require_secure_connection`

  This security feature requires you to use SSL to access any part of the web service. If https is required but not used, then a SOAP Fault with code UDS_SECURE_CHANNEL_REQUIRED is returned.

Note: For information about how to configure SSL, see your J2EE Servlet Container documentation.

Use the Web Services

The information in this section provides you with the fundamentals for using the CA SDM Web Services. Example code using the Web Services exists in the following CA SDM installation directory:

```
<NX_ROOT>/samples/sdk/websvc/java
```

The sample code is written in Java using Apache Axis for SOAP messaging.

Logins

Before any Web Services method can be used, a SID (session ID) must be obtained from one of these methods: login(), loginService(), and loginServiceManaged(). The first two methods require a username and password that are validated exactly the same as the CA SDM web interface; the contact's Access Type specifies the validation method. The third method requires a public/private key pair, where login request encrypted with the private key can only be decrypted through the public key, and vice versa.

How to Perform Common Tasks

The Web Services provides a flexible and powerful API into CA SDM, but it requires some knowledge of the object structure used by the product as follows:

1. Familiarize yourself with the information about objects and attributes in CA Service Desk Manager Reference Commands (see page 3496).
   This guide lists the attributes of each object in the system, which is essential because many of the Web Services methods require attribute names.

2. Review the Web Services methods, especially generic ones. For example, if your application must display all the activity logs for a request, first identify how the activity logs relate to the request.
   The CA Service Desk Manager Reference Commands (see page 3496) section shows that the request object has two lists of Activity Logs: The act_log (which shows only noninternal logs), and act_log_all (which lists all activity logs).

3. Identify which Web Services methods you require. To get lists attached to an object, use getRelatedList() or getRelatedListValues().

Default Handles

Some default data provided by the product is frequently used. Instead of looking up handles for these objects, some of the commonly used ones are listed in the following tables.

Note: While the handles do not change the legible symbols may be edited.

Contact Type (Object name: ctp)

Handle	Note
ctp:2307	The “Analyst” type
ctp:2310	The “Customer” type
ctp:2305	The “Employee” type
ctp:2308	The “Group” type

Impact (Object name: imp)

Handle	Note
imp:1605	Impact ‘None’
imp:1600	Low impact ‘5’
imp:1601	Medium-low impact ‘4’
imp:1602	Medium impact ‘3’
imp 1603	Medium-high impact ‘2’
imp:1604	High impact ‘1’

Priority (object name: pri)

Handle	Note
pri:505	Unassigned priority ‘None’
pri:500	Low priority ‘5’
pri:501	Medium-low priority ‘4’
pri:502	Medium priority ‘3’
pri:503	Medium-high priority ‘2’
pri:504	High priority ‘1’

Severity (object name: sev)

Handle	Note
sev:800	Low severity ‘1’
sev:801	Medium-low severity ‘2’
sev:802	Medium severity ‘3’
sev:803	Medium-high severity ‘4’`
sev:804	High severity ‘5’

Call Request Type (object name: crt)

Handle	Note
crt:180	Request
crt:181	Problem

Handle	Note
crt:182	Incident

Query for Requests, Issues, or Change Orders Assigned to a Contact

One of the most common operations is retrieving the active requests assigned to an analyst (assignee). You can use one of several methods, such as doQuery() (to get a list reference), or doSelect() (to get the values immediately). Assuming the assignee's handle is already known, the where clause to use is as follows:

```
assignee.id = U'<assigneeID>' AND active = 1
```

In this where clause, <assigneeID> is the id portion of a contact handle, value, such as "555A043EDDB36D4F97524F2496B35E75".

This where clause works for requests, change orders and issues because they all have the 'assignee' and 'active' attributes, and they mean the same thing for all three object types. The 'active = 1' portion of the where clause restricts the search to active requests.

The Active Flag

Most CA SDM objects have a field called 'active' or 'delete_flag'. This is actually an SREL pointer to the Active_Boolean_Table object or Boolean_Table object. Consider adding these fields to your queries to filter objects marked as Inactive by the system administrator. For querying purposes, search for 'delete_flag = 0' to find active records and 'delete_flag = 1' for inactive records. For example, the following pseudo-code demonstrates using doSelect() to retrieve values for all active Request Status objects:

```
doSelect(SID, "crs", "delete_flag = 0", -1, new String[0]);
```

To set an object to active or inactive, you need to pass the handle of the Boolean object representing either true or false. These handles do not change, so you can safely hard-code them. These are listed as follows:

Active_Boolean_Table	Boolean_Table
actbool:4551 = 'Active'	bool:200 = 'False'
actbool:4552 = 'Inactive'	bool:201 = 'True'

Retrieve Related List Length

When requesting attribute values from an object, such as with getObjectValues(), you can get the length of a related list by requesting the following attribute:

```
 "<listName>.length"
```

For example, to get the number of Activity Logs for a certain request, pass the following to getObjectValues():

```
"act_log_all.length"
```

Note: This is the only way you can use list names in these types of methods.

Access Control and Management

This article contains the following topics:

To minimize the potential problem of web services ticket flooding and to maintain the stability of the CA SDM server, this version of CA SDM Web Services uses an Access Control and Management system. It works primarily to handle the excessive service activities initiated by trusted user applications that can result from programming errors or exceptions. It also works as a barrier for controlling access to CA SDM Web Services from malicious attackers. An administrator of a web service application is able to create and define an access policy in CA SDM that controls access to CA SDM Web Services from a web service application.

Note: A default access policy with a code of DEFAULT is provided. The default access policy contains no access restrictions and is only applied to sessions authenticated through username and password.

Define an Access Policy

To create any SOAP web services access policy, an administrator defines an access policy.

Follow these steps:

1. Click the Administration tab.
2. In the tree on the left, click SOAP Web Services Policy, Policies.
   The SOAP Web Services Access Policy List page appears.
3. Click Create New.
   The Create New SOAP Web Services Access Policy dialog appears.
4. Enter the information for the new access policy:

Note: The defaultvalue of -1 in any operation counter indicates that no restrictions apply to the corresponding operation. A value of 0 (zero) indicates that the corresponding operation is not allowed.

- **Symbol**
  (Required) Identifies a symbolic name of the access policy.
- **Code**
  (Required) Indicates the unique text that identifies this access policy.
- **Status**
  (Required) Identifies the status of an access policy. An inactive policy is not used.
- **Proxy Contact**
  Identifies the contact to use for all web services operations and CA SDM security.
- **Default**
  Identifies the default policy. Set this policy as the default policy. Only one active default policy is allowed to exist. Creating a default policy automatically sets the current default policy to a nondefault status.
- **Has Key**
  (Read-Only) indicates whether a public key has been associated with this policy. This field is updated when a public key is associated with a policy through the pdm_pki utility.
- **Allow Impersonate**
  Identifies the allow impersonate permission. When you set this field, the policyholder can invoke the impersonate() web services method and create a web services session in the name of the user to be impersonated. Additional access authentication is not performed when creating the session. However, only when the access_level of the new access type for the user is less than or equal to the grant_level of the proxy access type for the user can this method be successfully called.
- **Description**
  Indicates the detailed description of this access policy.
- **Ticket Creation**
  Indicates the number of ticket (call request, change order, and issue) insertion operations allowed per hour.
- **Object Creation**
  Indicates the number of CA SDM object (other than ticket object) insertion operations allowed per hour.
- **Object Updates**
  Indicates the number of CA SDM object update operations allowed per hour.
- **Attachments**
  Indicates the number of attachment-related operations allowed per hour.

- **Data Queries**
  Indicates the number of data query operations allowed per hour.

- **Knowledge**
  Indicates the number of knowledge-related operations allowed per hour.

5. Click Save.
   The SOAP web services policy is defined.

Web Services Methods by Category

Each CA SDM Web Services method belongs to a specific category. The following lists each category and their corresponding methods:

- Ticket Creation
- Object Creation
- Object Updates
- Attachments
- Data Queries
- Knowledge

When an access policy is updated by CA SDM, Web Services dynamically updates the corresponding policy information. Active Web Services sessions controlled under this policy remain controlled with configurations in the policy. New Web Services sessions for this policy to manage and control, take the latest configurations in effect.

Note: For information about each method, see the CA Service Desk Manager Reference Commands (see page 3496) section.

Define an Error Type

Error types are assigned when creating tickets and an access policy defines one set of these error types. A CA SDM Web Services user application may use low-level web methods to create a ticket (request, change order or issue), specifying one of these types to categorize the error addressed in the ticket. Error types can be used only with the high-level createTicket() method. Low-level methods, such as createRequest(), do not use error types.

Web Services Error Types

CA SDM Web Services also provides a defined set of default error types, which are created for *every* policy. These default types, designated as *internal* error types, can be deactivated, but cannot be deleted. In the product, you can use the Web Services Access Policy Detail page to see the default error types provided when a new policy is created.

The following information describes each internal error type:

- **ACCESS_ERROR**
  Indicates that the system failed to connect to or find a resource, such as a file, website, and so on.
- **EXCEPTION_FATAL**
  Indicates that the application is shutting down unexpectedly.
- **EXCEPTION_RUNTIME**
  Indicates that the application code encountered an exception.
- **LOGIN_ERROR**
  Indicates that the operator failed to gain access to the application.

Additional Error Types

The administrator of an access policy can add additional error types as described in the following information:

Error Type	Description
Ticket Template	Identifies a template of a Incident or Error, issue, or change order that you use to create a ticket when this error type is reported. **Note:** The owning policy's contact is used as the end user. The Ticket Type and Ticket Template Name define the ticket template.
Default	Indicates if this error type is the default for the policy. Only one default is allowed per policy. **Note:** A new default error type overwrites the existing default error type associated with the policy.
Active	Represents an active error type. **Note:** An inactive type does not create tickets.
Internal	Identifies the field as read-only, which indicates whether this error type is an internal, default error type.
Symbol	Indicates the symbolic name of the error type.
Code	Identifies the unique text identifier of the error type.
Description	Describes the detailed description of the error type.
Duplicate Handling	Defines the action to take when the product detects that an identical ticket already exists.
Return Data	Identifies the user-defined return message you can specify for the web method "createTicket()" to return to client applications. Return data might be used for indicating an action the application should take (Application Data Return), or a message (User Data Return) to display to the end user.

Duplicate Ticket Handling

The Web Service Access Policy can detect and handle duplicate tickets, which is helpful for preventing ticket flooding. A ticket created with the potential of being a duplicate applies if all of the following conditions are true:

- At least one ticket of the same type (cr, iss, or chg) already exists and is ACTIVE.
- The existing ticket was created by the web service.
- The existing ticket was created with the same Policy and Error Type as the ticket being created.
- The “create date” of the existing ticket is within a specified threshold (for example, it was opened less than 2 days ago).

  Note: The create date field is configured using the Maximum time interval for searching duplicates.

- The duplicate ID matches the one provided by users when invoking the createTicket() method.

Users can also assist in preventing duplicates by classifying tickets as being unique or different, based on criteria known to the user. To do this, add an optional string parameter to the createTicket Web Services call. If duplicate handling is on, the string parameter is inspected after other duplicate handling criteria match to determine whether this is a unique or duplicate call to this method.

Duplicate Ticket Results

If the create ticket action results in a duplicate, the existing Error Type may be configured to do one of the following:

Reconfigured Error Type	Results
Create the New Ticket and Ignore Duplicates	A new ticket handle and number are returned (default).
Do Not Create a New Ticket; Add an Activity Log to the Existing Duplicate Instead	The ticket handle and existing ticket number are returned.
Do Not Create a New ticket; Add an Entry to the CA SDM Standard Log Instead	A ticket handle and existing ticket number are returned.
Create a New Ticket and Attach it as a Child to the Duplicate	A new ticket handle and number are returned.

Simplified Web Services Access

CA SDM Web Services provides an abbreviated set of high-level web services methods that are simplified versions of existing web services methods. The majority of users applications do not have to completely rely on a large set of web services methods before requesting service desk services

through CA SDM Web Services. Working closely with user-defined access policies and using default parameters defined in the policies, this set of high-level web services methods can function with little knowledge of the CA SDM object schema. Also, the high-level methods cover a common set of CA SDM functionalities that most service-aware applications need.

The following describes the use of these high-level web services methods:

- **createTicket (SID, Description, Error_Type, Userid, Asset, DuplicationID)**
  You must specify an error type for the reported error if you use this method. The error type should contain the ticket template appropriate for the ticket you want to create. It should define the action to take in the case of a duplicate ticket, specify the data outputs, and finally, it must be associated to the access policy that is defined for the user application.
  When this method is invoked, CA SDM Web Services locates the current access policy and the error type required for the ticket creation. The following shows the sequence that CA SDM Web Services uses for locating the proper error type:

  - If a specific error type code is provided as input and it matches a error type that is associated to the policy, this error type is used, regardless of whether it is internal.
  - If an error type is not specified or the previous step fails to locate an error type, the default error type is used if there is one defined for the policy.
  - If a default error type is not defined for the policy or the previous step fails, the default error type defined for internal error types is used.

  After an error type is defined, CA SDM Web Services uses it to create a ticket. The proxy user defined in the access policy is used for the ticket creation if the userid is empty, and asset information is added to the ticket (if the input is not empty). After the ticket is created, CA SDM Web Services returns both user data and application data, as specified by the error type.

- **closeTicket (SID, Description, TicketHandle)**
  Users can call this function to close an open ticket. It simply sets the status of an open ticket to ‘close’ and adds the input description to the activity log.

- **logComment (SID, TicketHandle, Comment, Internal_Flag)**
  Adds an entry with the input comment to the activity log for the open ticket.

- **getPolicyInfo (SID)**
  Lets users obtain the policy information that controls the current web services session. You can use this information as an indicator of server capacity for this user application. Users may want to adjust their web services calls to fit into the capacity.

By having this set of simplified Web Services APIs, a majority of users are spared the tremendous effort of understanding the complete set of web services API and CA SDM schema. Using them simplifies and accelerates the process of creating service-aware enabled applications for these users.

CA SDM Objects

This article contains the following topics:

CA SDM treats each entity, such as a contact or an issue, as an *object*. These high-level objects are defined in majic (.maj) and mod (.mod) files on the CA SDM server in the following directory:

```
/bopcfg/majic
```

Customized objects are defined in the following directory:

```
/site/mods/majic
```

Objects are essentially high-level wrappers around a database table.

An object's type (sometimes referred to as *factory*) defines the object. For example, request objects belong to the 'cr' type. Each object's type is defined by the "OBJECT" declaration in a majic file.

Note: All objects shipped with CA SDM are enumerated in the CA Service Desk Manager Reference Commands (see page 3496) section.

An object has *attributes*, which are essentially columns in a database table (do not confuse these with XML attributes). Web Services offers many methods to retrieve values for attributes. Many methods require you to name attributes for setting or retrieving values. You must use the attribute name assigned in the majic or mod file that defines the object, which can be different from the actual database name. Client sites can add additional attributes as a customization.

Note: For a list of all the attributes for each object, see the CA Service Desk Manager Reference Commands (see page 3496) section.

Web Services uniquely identifies an object by its *handle,* which is a string value of the form *objectType:ID*, where *objectType* is the object's type (factory) name, and ID is a unique value. The ID value matches that of the 'id' attribute found in every CA SDM object. Because the 'id' attribute is almost always indexed in the DBMS, using the ID portion of the object handle is especially valuable for forming efficient queries. Each object, regardless of its type, stores this value in an object attribute named "persistent_id".

Note: In prior releases, the ID portion of the handle was always a string of integers. In CA Service Desk r11.0 and later, the ID portion may also be the string representation of a UUID, typically 32 characters.

The following information lists the object and factory names of the entities that use UUIDs:

Object Name	Factory Name
Contact	cnt

Object Name	Factory Name
Asset	nr
Organization	org
Location	loc
Company/Vendor	ca_cmpny
Model	mfrmod

Handles are *persistent;* a handle representing a particular object is always unique for its lifetime, even across database migrations. Clients may want to take advantage of this persistence when working with fairly static objects, for example, Status or Contact Types.

Object handles are the key to using CA SDM Web Services. Many methods, especially those that update data, require handles. Most methods that return object data also include the object's handle.

System Updates and Caching

Web Services caches information for object types. Type information is not cached until the type is referenced for the first time, and will cause a small delay.

To avoid any server or caching delays, you may want to run a primer client to activate the Web Services and cache the most popular object type information. The easiest way to cache the object type information is to perform repeated calls to GetObjectTypeInformation(). The object types to consider for this technique could be one of the following:

Object Type	Definition
cr	Request
chg	Change Order
iss	Issue
cnt	Contact
nr	Asset
prp	Property (for Change and Issue)
prptpl	Property Template (for Change and Issue)
cr_prp	Request Property
cr_prptpl	Request Property Template
cr_wf	Classic Workflow (Request/Incident/Problem)

Add any additional object types your client code references.

Categories and Properties

The request, change order and issue objects all have a category field, which is used to classify the nature of the ticket. A category may have property objects, which are attached to the ticket when the category is assigned. Some of these may be marked *required*, which means a value must be supplied before the ticket can be saved (applies to both insert and update operations).

CA SDM Web Services automatically supplies default values for any ticket created with the Web Services. The default value (currently, “-“) is obtained from the CA SDM localized message catalog.

If you need to set property values at creation time, there are three ticket creation methods: createChangeOrder, createIssue, and createRequest. Each has a parameter with which you can pass in values for any properties. To discover which properties will be attached, you must find out the properties associated with the category you intend to assign to the ticket. The easiest method to use is getPropertyInfoForCategory().

Note: For more information about the getPropertyInfoForCategory(), see the CA Service Desk Manager Reference Commands (see page 3496) section.

To identify the valid values for a property, first find the property validation rule for the appropriate property template. To do this, request the validation_rule attribute when calling the getPropertyInfoForCategory method. Then, retrieve the associated validation_type for that rule. If the type is dropdown, you can then use the getRelatedList method to retrieve the values associated with the rule, using the "values" BREL attribute in the prpval_rule object.

Note: For more information, see the CA Service Desk Manager Reference Commands (see page 3496) section.

To set property values after an update operation with updateObject(), you must query the property list after the update. getRelatedList() can help with this task.

Validation of property values through Web Service methods is not currently supported. For example, to assign property values to a validation rule with a validation type of drop-down option, you would have to write additional code to create property values while creating the drop-down option validation rule. Do not attach a property value to a check box validation rule.

Note: For more information about property validation rules, see the Define a Category or Area (see page 1054). For information about creating property validation rules through the CA SDM interface, see Create Property Validation Rules in Setting Up Category or Area (see page 1050) section.

XML Object Returns

Many of the Web Services methods return an XML representation of CA SDM objects. The Web Services uses a standard XML structure beginning with the following root element:

```
<UDSObject>
```

The format of the XML representation is described in the following table:

XML Element	Type	Description
<UDSObject>	N/A	Identifies the root node.
<Handle>	String	Identifies the object's handle.
<Attributes>	Sequence	Identifies the attribute values. This holds zero or more elements for the object's attribute values.
<*attrName0* DataType = *"typeEnum"*>	String	Identifies the *AttrName0,* which is an object attribute name as defined in the CA SDM majic (.maj) or mod (.mod) file. This name may use dot-notation depending on the web method used. The element's value is the attribute's value. An empty element indicates a null/empty value for this object's attribute. The DataType attribute is an integer indicating the attribute's data type in the CA SDM environment.

For example, a call to getObjectValues() can return information illustrated by the following:

```
<UDSObject>
    <Handle>cnt:555A043EDDB36D4F97524F2496B35E75</Handle>
    <Attributes>
        <Attribute DataType="2003">
            <AttrName>first_name</AttrName>
            <AttrValue>first name</AttrValue>
            <DisplayValue>Yaakov</DisplayValue>
        </Attribute>
        <Attribute DataType="2005">
            <AttrName>organization</AttrName>
                <AttrValue>342</AttrValue>
        <DisplayValue>Accounting Crew</DisplayValue>
    </Attribute>
</Attributes>
    <Lists>        <List name="mylist1">
            <UDSObject>...</UDSObject>
            <UDSObject>...</UDSObject>
        </List>
    </Lists>
</UDSObject>
```

Some methods, such as doSelect(), return a sequence of <UDSObject> elements contained inside a <UDSObjectList> element.

The <Lists> section holds zero or more <List> nodes. A <List> node holds zero or more <UDSObject> nodes. <List> elements are generally returned only when a specific request for list values is made.

When you want to return a list of values related to a specific object, you should use the *getRelatedListValues* method.

If a request is made just for a list with no attribute name, such as actlog, then the entire <UDSObject> is returned in the <List> section.

Specialized methods, like getDocument(), can of course be different. When a request is made for an attribute, the database value is returned. For SREL attributes, this may not be so useful. Requesting the assignee attribute of a Request returns an integer because the Contact REL_ATTR (foreign key) is its ID. For CA Service Desk r11.0, the return data for attributes includes elements for the DBMS and common name value of SREL references.

ITIL Methodology

This article contains the following topics:

By default, the Web Services fully support the ITIL methodology. CA SDM ITIL features let you take advantage of the ITIL methodology.

Incident or Problem Creation

CA SDM supports ITIL methodology so that incidents and problems can be created using the CA SDM Web Services. Both incidents and problems are held in the cr (Call_Req) object. Its *type* attribute distinguishes the record as an incident, problem, or request. To create an incident, problem, or request, call createRequest and specify the appropriate value for the type attribute.

The type attribute is a pointer (SREL) to the crt (Call_Req_Type) object, so you must pass a handle as the value.

The following code examples illustrate how to create an incident or problem by passing the correct crt object handle to the createRequest method. Setting the *type* attribute in the name-value pair that is passed as a parameter to createRequest, creates the tickets:

Example: Syntax for a Problem

```
attrVals = {"summary", "A new problem", "description", "new problem", "type", "crt:
181", "catagory", "pcat:40002"}
USPSD.createRequest(SID, creatorHandle, attrVals, template, new String[0], new String
[0])
```

Note: All the workflow tasks that are attached to a category are available for a problem. The workflow task is selected on the configuration of CA Process Automation or Classic workflow.

Example: Syntax for an Incident

```
attrVals = {"summary", "A new incident", "description", "new incident", "type", "crt:
182", "catagory", "pcat:40002"}
USPSD.createRequest(SID, creatorHandle, attrVals, template, new String[0], new String
[0])
```

Note: All the workflow tasks that are attached to a category are available for an incident. The workflow task is selected on the configuration of CA Process Automation or Classic workflow.

Query for Incidents or Problems

To retrieve incidents or problems, include the *type* attribute of the cr object in the where clause. The following example illustrates a where clause for retrieving all active Incidents. This where clause could be used with methods that perform queries for 'cr' objects, such as doSelect and doQuery:

```
type.id = 182 AND active = 1
```

The '182' is the ID portion of the handle representing Incident types.

Note: For more information, see the crt (Call_Req_Type) objects table illustrated in Default Handles (see page 1860). For more information about forming proper queries, see WHERE Clause (see page 1719).

Attach an Incident to a Problem

You can associate one or more incidents to a problem. The problem attribute of an incident relates the incident to a problem.

Example: Associate an Incident to a Problem

This example demonstrates how to relate a newly created incident to an existing problem.

To associate the incident to the problem, use UpdateObject to set the problem attribute of the incident. The following example code sets the problem attribute to the handle of an existing problem ticket:

```
attributeValues = {"problem", "cr:12346"}
USPSD.UpdateObject(SID, incidentHandle, attributeValues, new String [0])
```

Attach a Problem to a Change Order

Incidents and problems can be linked to change orders with the attachChangeToRequest method. The following example code uses this method to simultaneously create a change order and attach it to a problem. In the example, "cr:12347" is the object handle of the problem -- it passes a blank handle for the fourth parameter, which causes the method to create a change:

```
UPSPSD.attachChangeToRequest(SID, creatorHandle, "cr:12347", "", new String[0],
"activity description")
```

Change Order Creation

CA SDM supports ITIL methodology so that a Change Order can be created using the CA SDM Web Services. Change Order are held in the chg (Change_Request) object. To create an change order, call createRequest and specify the appropriate value for the type attribute. The following code examples illustrate how to create a change order:

Example: Syntax for a Change Order

```
attrVals = {"summary", "A new change order", "description", "new change order","
catagory", "chgcat:400002"}
USPSD.createChangeOrder(SID,creatorHandle,attrVals,template,new String[0], new String
[0])
```

Issue Creation

CA SDM supports ITIL methodology so that an Issue can be created using the CA SDM Web Services. Issue are held in the iss (Issue) object. To create an Issue, call createRequest and specify the appropriate value for the type attribute. The following code examples illustrate how to create an change order:

Example: Syntax for Issue

```
attrVals = {"summary", "A new Issue", "description", "new Issue", "catagory", "isscat:
400002"}
USPSD. createIssue(SID,creatorHandle,attrVals,template,new String[0], new String[0])
```

Configuration Items

ITIL methodology uses the term *configuration item* (CI) to refer to hardware, software, and other IT resources. This term refers to the “nr” object stored in the CA Technologies-owned resource database table. All methods that use *asset* objects also work with CIs. This is only a difference in terminology.

Public Key Infrastructure (PKI) Authentication

This article contains the following topics:

If you plan to use the PKI authentication, realize that the content of the login request is encrypted with a private key that can only be decrypted by its matching public key. The response of the login request is returned as plain text.

Generally, each application accessing CA SDM Web Services is assigned with a policy. CA SDM Web Services stores detailed information about a policy, along with the public key of a digital certificate. An application, as the policy holder, uses the private key of the digital certificate and the policy code (as policy identifier) to assemble a login request.

loginServiceManaged (Policy, Encrypted_Policy)

CA SDM Web Services performs the user authentication by locating the policy through the plain text policy code, retrieving the policy holder's public key associated with the policy, decrypting the encrypted policy code, matching the decrypted content with the policy code, and finally, opening a session with a back-end server. The plain text session ID (SID) is returned and can be used for subsequent method invocations. Only the policyholder holds the private key that matches the policy' s associated public key stored in CA SDM.

All subsequent web services calls must include the returned session ID (SID). The Proxy contact specified in the policy is responsible for all web services activities initiated in this session. All function group security and data partition is enforced for the proxy contact.

Important! The Encrypted_Policy parameter should be in the BASE64 text format. The user application must perform proper conversion from the binary format.

Policy is a required field. When you define it, use plain text policy code as defined in a policy. Encrypted_Policy (the digital signature of the policy code encrypted with the policy holder's private key) is required. When you define Encrypted_Policy, use the algorithm SHA1 with RSA to obtain the digital signature.

Implement loginServiceManaged in Java

The following shows how to generate Certificates and then use these generated Certificates to access the CA SDM web services.

In the following example, the login process completes using the CA SDM Certificate and then performs two common web services calls. The getBopsid() web services method call allows you to obtain a token that is linked to a specific user. This token can be used to login to the CA SDM web interface as the linked user without being prompted for a password. This allows seamless integration to be enabled between different applications.

Important! The generated BOPSID token expires after 30 seconds, so it must be used promptly.

Important! There is a known issue when using the 1.4 version of the AXIS tool. For more information, see the *Release Notes*.

Follow these steps:

1. Generate the stub classes with AIXS Tool WSDL2Java. For more information, see the Generating Stub Classes with AXIS Tool WSDL2Java section from the PKI_loginServiceManaged_JAVA_steps file. Find the file in the following location:

```
$NX_ROOT/samples/sdk/websvc/java/test1_pki
```

2. Start the CA SDM service.

3. Run pdm_pki -p DEFAULT.
   DEFAULT.p12 is created in the current directory. This policy will have the password equal to the policy name (in this case DEFAULT).

   Note: This command will also add the Certificate's public key to the field pub_key field (public_key attribute) in the sapolicy table/object.

4. Log in to CA SDM.

5. Select SOAP Web Services Policy, Policies on the Administration tab.
   The SOAP Web Services Access Policy List page opens.

6. Click DEFAULT.
   The SOAP Web Services Access Policy Detail page opens.

7. Complete the Proxy Contact field (in this example, ServiceDesk) and confirm that the DEFAULT policy record Has Key field displays "Yes."

8. Copy DEFAULT.p12 (from the directory where command pdm_pki is executed), the JSP file called *pkilogin.jsp* and the HTML file called *pkilogin.htm* (from the $NX_ROOT/samples/sdk /websvc/java/test1_pki directory) to the following directory:

   ```
   $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/axis
   ```

9. Open the HTML form (from the axis directory). For example, http://localhost:8080/axis /pkilogin.htm
   Complete the appropriate fields.

   Note: The Directory field identifies the location of the Certificate file. Modify the path to the correct location.

10. Click Log me in!
    The results page opens.

11. Click the BOPSID URL.

    Important! Click this immediately! The BOPSID has a limited life token of about 30 seconds.

The format of a URL using a BOPSID is as follows:
http://<server name>:CA Portal/CAisd/pdmweb.exe?BOPSID=<BOPSID value>

Note: In order to use the loginServiceManaged method for a Java client program running on AIX, you may need to replace a pair of security policy files within your JAVA_HOME. Go to http://www.ibm.com (http://www.ibm.com) and search for "developerworks java technology security information AIX". In the "developerWorks : Java technology : Security" document, follow the link to "IBM SDK Policy files". Download the unrestricted policy files, local_policy.jar and US_export_policy.jar. Use these files to replace the original files in your JAVA_HOME/lib/security directory."

Configuration for the PKI Authentication Type

To configure for PKI authentication, you must first create an access policy. The process flow is as follows:

- **Create an Access Policy**
  The administrator performs this task using the product (Web Interface only), and as part of the process, needs to assign a unique text code to each access policy.

- **Obtain a Digital Certificate with a Public/Private Key Pair and Associate it with the Access Policy**
  For PKI access authentication, a user application needs to obtain a digital certificate that contains both a public key and private key pair. An administrator can obtain the digital certificate through third-party Certificate Authority (CA) or security products that support digital certificates. CA SDM also provides a server-side utility that can generate a digital certificate. It is located in <NX_ROOT> /bin directory as follows:

```
pdm_pki  - p policy_code [ - l certificate file] [ - f] [-h]
```

  - **-p**
    Identifies a unique policy code.

  - **-f**
    Allows the utility to replace the existing public key with a new public key.

  - **-l**
    Loads the public key stored in a X509 V3 certificate.

  - **-h**
    Displays help on the command line window.

  If you obtain a digital certificate through a third-party, CA Technologies, or security products, import it to where the CA SDM server is located, and then associate it to an access policy. The administrator of the user application should obtain a digital certificate file that includes the content of an X509 V3 certificate in DER/ASN.1 format.
  In addition, the certificate should contain only the public key of the public/private key pair. Using the - l option, the administrator should invoke the pdm_pki utility to load the certificate. The utility then loads the certificate, extracts the public key, converts the public key to BASE64 text format, and saves it with the access policy specified by the policy code.

When a digital certificate is generated by the pdm_pki utility, the administrator invokes the command in CA SDM without the - l option. The utility then generates a public and private key pair (keys are RSA1024 bit keys). The public key is converted to BASE64 text format where it is stored along with the access policy specified by the policy code. An X509 V3 certificate is also created to hold the public key along with other information (the default pass phase is set as the policy code). Finally, the X509 V3 certificate is packaged with the private key to a standard portable certificate format of PKCS12. It is then saved in a file with a file name of *policy_code*.p12, depending on the policy code supplied. This file can then be exported to clients.

Note: If an access policy has already been associated with a public key of a certificate, users need to specify the - f option when calling the pdm_pki command in order to overwrite the existing public key with a new public key.

Login to Web Services

The following describes the process flow for logging in to Web Services configured with PKI authentication:

Process	Description
Load the Digital Certificate and Extract the Private Key	The digital certificate must be stored in secure storage on the user side, where it can be retrieved and used for logging in to Web Services. Example of secure storages include the following: Windows Certificate Store Java Certificate Store (managed by java_keytool utility) Certificate store (created by other CA Technologies security products). A user application should be able to load the digital certificate and extract the private key using appropriate APIs, depending on user environments.
Create a Digital Signature of the Plain Text Policy Code with the Private Key	After the private key is extracted from the digital certificate, it can be used to generate a digital signature of policy code. Creating a digital signature encrypts a digest of a text with a private key. The digest algorithm must be standard SHA1, and the encryption algorithm should be RSA. Also, the binary digital signature should be converted to BASE64 text format before it can be used for logging in to Web Services. Depending on user environments, appropriate API calls should be used to archive this information.
Invoke the Web Service Call	A user application should invoke the Web Services method loginServiceManaged(), along with the plain text policy code and the BASE64 text formatted digital signature of the policy code.
Obtain the Returned SID	If the access request is authenticated, a plain text SID is automatically returned.

After a SID is generated, it establishes a successful binding between a Web Service session and an access policy. The user application can invoke other web services methods with this SID, and all of its access to Web Services becomes controlled and managed by this access policy.

Session and Authorization

A successful validation returns a SID that is associated with the validated username, whether it is the user name supplied for login or the proxy contact specified in a policy. Because of this process, each CA SDM user is assigned security rights that you may want enforced in your web service application.

For example, a specific user may have a Data Partition restricting which Requests the user can view. When using a SID for the user to get Request information, the CA SDM system ensures the data partition is enforced.

Function Group security is also applied. For example, a user may not have access to the Call Manager function group. Invoking any web services methods, such as viewing or creating Requests, is denied because access is denied to the Call Manager function group.

When your application is finished doing work for a user, call the Logout() method to invalidate the SID.

Each SID expires after a period of inactivity. That is, a SID expires if the interval between method calls is greater than a certain timeout value. The timeout interval is set in Options Manager and is specified by the following CA SDM option:

```
'webservice_session_timeout'
```

If this value is set to zero (0), a SID never times out. If this option is missing or not set, the default is one hour. If a Web Service method is called with an expired SID, a Fault is returned with an error code of UDS_SESSION_TIMEOUT the first time it is referenced, and UDS_BAD_SESSION each time thereafter.

To keep a SID active, call any web service method before the time out is reached. To keep the SID active without working the server, call serverStatus().

Tips for SOAP Web Services Clients

This article contains the following topics:

The samples directory of the CA SDM installation provides a sample Java client application for Web Services. This sample assists developers with web services client application development.

Many of the Web Services methods require arrays as input parameters. For example, the method createIssue() permits an empty array for propertyValues. Sometimes these arrays are optional, but the service requires an empty array for a successful pass. When you use Visual Studio .NET to access Web Services, specify an empty array with one of the following arrays:

- **C# language**

```
String[] emptyArray = new string[0];
```

- **Visual Basic .NET**

```
Dim emptyArray As String() = {}
```

- **Java**

```
ArrayOfString attr = new ArrayOfString();
attr.setString(new String[0]);
ArrayOfString is a proprietary class.
```

You can then pass emptyArray to array parameters that accept empty arrays.

Note: The CA SDM Web Services use the Apache implementation of standards established by the World Wide Web Consortium (W3C). Ideally, a client on any type of operating environment can access the services, but vendor implementations vary. Many programming environments provide a tool to generate proxy classes from a Web Services Description Language (WSDL) description.

Java Clients

The TableOfContents.doc in $NX_ROOT/samples/sdk/websvc lists several Java sample programs.

Each sample program contains notes on how it can be compiled and run using the script files run_java_test_bat.txt (Windows) and run_java_test_sh.txt (UNIX). These scripts demonstrate how to use org.apache.axis.wsdl.WSDL2Java to generate the CA SDM web services client-side stub files.

The - w parameter is required to properly generate the stub files when using Axis 1.4. Running WSDL2Java as shown will generate the stub files in subdirectory com/ca/www/UnicenterServicePlus /ServiceDesk. The following files are generated:

- ArrayOfInt.java
- ArrayOfString.java
- ListResult.java
- USD_WebService.java
- USD_WebServiceLocator.java
- USD_WebServiceSoap.java
- USD_WebServiceSoapSoapBindingStub.java.

Import these classes with the following statement:

```
import com.ca.www.UnicenterServicePlus.ServiceDesk.*;
```

Many Web Service methods have parameters of type ArrayOfString, a proprietary class. For example, the createRequest() method's attrVals, propertyValues and attributes parameters are all ArrayOfString parameters.

To set the values in an ArrayOfString variable, instantiate the variable and then use setString() as follows:

```
ArrayOfString attrVals = new ArrayOfString();
attrVals.setString(new String[]{"customer", customerHandle, "description",
"description text"});
```

To set it to empty

```
attrVals.setString(new String[0]);
```

Use a variable of type ListResult, another proprietary class, as the return value from the List methods: doQuery(), getRelatedList(), getNotificationsForContact(), getPendingChangeTaskListForContact() and getPendingIssueTaskListForContact(). A ListResult contains listHandle and listLength elements, which can be retrieved using getListHandle() and getListLength() as shown in this example:

```
ListResult doQueryResult = new ListResult();
doQueryResult = USPSD.doQuery(sid, "iss", "active = 1");
int listHandle = doQueryResult.getListHandle();
int listLength = doQueryResult.getListLength();
```

The getListValues() method uses the listHandle, retrieving the values from a subset of the list.

The Handles parameter of the freeListHandles() method is an ArrayOfInt, another proprietary class. Call freeListHandles() using the listHandle taken from a ListResult:

```
ArrayOfInt handleList = new ArrayOfInt();
handleList.setInteger(new java.lang.Integer []{ new java.lang.Integer(listHandle) });
USPSD.freeListHandles(sid, handleList);
```

Some methods have pass by reference parameters of type javax.xml.rpc.holders.StringHolder. For example, createRequest() has two parameters of this type, NewRequestHandle and NewRequestNumber.

```
StringHolder NewRequestNumber = new StringHolder();
StringHolder NewRequestHandle = new StringHolder();
String result;
result = USPSD.createRequest(sid, creatorHandle, attrVals, propertyValues, template,
attributes, NewRequestHandle, NewRequestNumber);
```

The Request's handle and reference number (ref_num) can then be obtained from NewRequestHandle.value and NewRequestNumber.value respectively.

SOAP Web Services Configuration

You can configure the CA SDM SOAP Web Services with entries in special web configuration files. The following table summarizes the names and descriptions of the configuration options:

Option Name	Description
design_mode_stubs	Sets the Web Service *to design mode* (CA SDM only).
require_secure_logon	Requires the login() and loginService() web methods to be called with a secure protocol, such as https.
require_secure_connection	Requires that every web method be called with a secure protocol.
disable_user_logon	Disables both login() and loginService() web methods, so only loginServiceManaged() can be used to log in.

CA SDM adds protection to the integrity of the running Tomcat server by verifying the length of the attribute values that pass to Web Service methods. By default, web service calls return an Axis Fault if the length of an attribute exceeds 900,000 bytes.

You set the following parameters in the deploy.wsdd file:

- **fatal_max_string_length**
  Sets the length of the largest attribute value that a web service method accepts.
  Default: 900,000 bytes

- **validate_parameters**
  Sets whether the attribute value length checking is performed. Set the parameter to 0 to turn off the validation.
  Default: 1 (on)

- **exception_methods**
  Displays a comma-delimited list of Web Service methods that are exempt from the attribute value length validation.

Redeploy the Web Services

New configuration settings take effect when you redeploy CA SDM Web Services. Complete the following steps to redeploy the Web Services:

1. Open a command prompt and set the CLASSPATH environment variable to include the required Axis jar files, which are supplied in <NX_ROOT>/java/lib.
   For example, to set it on Windows, execute the following command:

   ```
   set AXISHOME=%NX_ROOT%\java\lib
   set classpath= %AXISHOME%\axis.jar;%AXISHOME%\jaxrpc.jar;%AXISHOME%\saaj.jar;%
   AXISHOME%\commons-logging.jar;%AXISHOME%\commons-discovery.jar;%AXISHOME%
   \wsdl4j.jar;%AXISHOME%\log4j-1.2.8.jar;%classpath%;
   ```

2. Modify the directory to <NX_ROOT>/sdk/websvc/R11 and execute the following commands:

   ```
   java org.apache.axis.client.AdminClient undeploy.wsdd
   ```

```
java org.apache.axis.client.AdminClient deploy.wsdd
```

3. Recycle Tomcat by recycling the CA SDM service. You can avoid shutting down the entire CA SDM system by recycling Tomcat by simply using the following commands:

   ```
   pdm_tomcat_nxd  - c stop
   pdm_tomcat_nxd  - c start
   ```

   The Web Service is redeployed.

4. Verify that the service deployed by viewing the Axis services listing page at the following default URL:

   ```
   http://<servername>:< port>/axis/services
   ```

   Note: The exact URL depends upon your installation settings.

SOAP Error Handling

If an error occurs with a Web Services method, a SOAP Fault is returned. The SOAP Fault is the standard means of returning exception information for Web Services.

The Fault message contains standardized <Message> and <Code> elements, but the most informative is the <Detail> element. The <Detail> element contains <ErrorCode> and <ErrorMessage> elements. The <ErrorCode> element returns an enumerated error code specific to either the CA SDM or Knowledge Management product. The <ErrorMessage> element contains an English string describing the errors. The <ErrorMessage> elements are more suitable for aiding the developer and more appropriate messages should display to users.

For example, the following illustrates a SOAP Fault when a bad parameter is supplied to the CA SDM getObjectValues() method:

```
<soap:Fault>
   <faultcode>soap:Client</faultcode>
   <faultstring>Error on fetch with attribute list:persistent_id,first_name,
last_nameParamErrorHere<faultstring>
   <detail>
<ErrorCode>1001</ErrorCode>
<ErrorMessage>Error on fetch with attribute list: persistent_id,first_name,
last_nameParamErrorHere </ErrorMessage>
   </detail>
   </soap:Fault>
```

If you are using a client built with Microsoft .NET managed code, a failed Web Services method call raises a "SOAPException" exception. All errors cancel the operation invoked.

In some cases, the servlet container may write errors and therefore, display in the servlet container logs. In other cases, error information may be written to CA SDM logs. These logs are located in the following subdirectories:

- In the /bopcfg/www/CATALINA_BASE/logs subdirectory of CA SDM installation
- In the /log subdirectory of the CA SDM installation and to all logs that have the prefix “stdlog”.

Note: We recommend that you constantly monitor these logs, as the server may log its own errors without reporting them to the CA SDM Web Services.

Lock Errors

CA SDM objects are locked during updates. Methods that update objects (such as, updateObject() or transfer()) may return the following lock error code:

```
UDS_LOCK_ERR
```

This code indicates that another user is updating the record. Often the locking user’s handle is returned in the ErrorMessage element.

Time Outs

If the CA SDM server is heavily loaded, a method may take a long time to process. In rare cases, a method may never return because a separate process failed to reply or some other error occurred. To guard against excessive blocking, every Web Services method times out after a number of seconds. Web Services method time-out is a CA SDM server time-out, *not* a Web server time-out, network time-out, and so on.

Note: The Web Services delay a few seconds the first time accessed after the J2EE application server is recycled. This happens because the application is initializing, loading DLLs, libraries, and so on, and occurs only with the first Web Services method call. All subsequent calls return much faster.

If a method times out, it returns the following error code:

```
UDS_TIMEOUT_ERR
```

The operation is not aborted! The server may have received the request and processes it successfully, although slowly. This type of problem may occur when using the *doSelect( )* method to retrieve several 1000 records.

Note: For information about the *doSelect* method, see the CA Service Desk Manager Reference Commands (see page 3496) section.

Error Codes

The following table lists the possible values for the <ErrorCode> value in a SOAP Fault returned from a Web Services call:

Error Name	Value	Description
UDS_OK	0	Successful.
UDS_FAILURE	1	General failure, check system logs.
UDS_BAD_PARAM	1000	A bad parameter was passed to a method. This error occurs if a required parameter is missing, the wrong type was passed, or an invalid value was used.
UDS_INTERNAL_ERR	1001	Signals that an internal error occurred. A description is found in the return array and the system logs.
UDS_LOCK_ERR	1002	An attempt was made to update an object locked by another user or process. Usually the ID of the contact responsible for locking the object is returned in the return data.
UDS_UPDATE_ERR	1003	An error occurred updating an object. Make sure all required attributes were set and check the system log.
UDS_CREATION_ERR	1004	An error occurred creating an object. Make sure all required attributes were set and check the system logs.
UDS_NOT_FOUND	1005	A search method failed to find any matches or failed to find an object specified. This can happen if a bad or invalid handle is passed to any method.
UDS_SESSION_TIMEOUT	1006	The current method timed out, the CA SDM server may be heavily loaded or the method itself was bad.
UDS_SERVER_GONE	1007	The CA SDM server connection is lost, UDS methods will no longer function and all list references are lost.
UDS_FETCH_ERR	1008	An error occurred while retrieving list data.
UDS_BAD_SESSION	1010	An invalid SID was used.
UDS_CNTXT_TIMEOUT	1011	The SID timed out.
UDS_SECURE_CHANNEL_REQUIRED	1012	The Web Services (or a web service method) requires a secure channel (for example: SSL) for access, but an unsecured channel is being used.
UDS_SECURITY_VIOLATION	1013	The attempted operation violates CA SDM security and was aborted.
UDS_OVER_POLICY_LIMIT	3002	The attempted request is refused because it exceeds the limit defined in the policy.

User Authentication and Authorization

CA SDM lets you specify user access authentication and the features available by access control and management.

User Access Authentication

CA SDM Web Services provides two access authentication schemes. They are associated with the new access control and management feature, which uses an access policy.

- **User Name/Password**
  Verifies the User Name/Password, as described in previous releases of the product.

- **Public Key Infrastructure (PKI) Technology**
  Verifies that the person requesting the access has ownership of a certain private key.

Important! If you plan to use an application that accesses this version of CA SDM Web Services, we recommend strongly that you first define a Web Service Access Policy, complete with its code value, in CA SDM. A default access policy with a policy code of DEFAULT is available when CA SDM is installed and configured.

Credential Authentication

This article contains the following topics:

If you plan to use the User Name/Password type of access authentication, the user application needs to invoke one of following two web services methods to gain access to CA SDM Web Services.

Note: The login user that you specify in the username parameter (not the proxy contact specified in the policy) is responsible for activities initiated in a session. All function group security and data partition is enforced for this login user.

login (Username, Password)

This method is provided for backward compatibility, where access authentication is performed on the username and password supplied. A SID (session ID) is returned only if the access is authenticated. All subsequent web services calls need to include this SID. Default access policy is then applied to all subsequent web services accesses labeled with the SID.

Username and password are required fields that require plain text when you define them.

loginService (Username, Password, Policy)

This method is similar to the previous login function in that access authentication is performed on the username and password supplied. A SID is returned only if the access is authenticated. However, a specific access policy, as identified in the third parameter, is applied to control and manage all subsequent Web Services accesses. Empty content in the policy parameter automatically applies the default policy.

Username and password are required fields that require plain text when you define them. Policy is required, but can be empty, and you must use plain text. Use the policy code defined in a policy.

How a login is validated depends on the contact's assigned *access type*. The access type object is hosted by CA SDM and sets the validation type. You can use the product to view the access type record, and you can also use the getAccessTypeForContact() web method to retrieve any access type object information.

Note: For more information about access types, see the Security and Role Management (see page 1986) section.

CA SDM REST API

This article contains the following topics:

Representational State Transfer (REST) is a style of software architecture for distributed hypermedia systems such as the World Wide Web. The CA SDM REST API lets application, integration, and web developers build UIs and applications for devices such as tablet computers and smartphones. Users such as analysts, employees, and customers can then use the UI or application on these devices. For example, application developers can develop a CA SDM UI that lets analysts use devices to update tickets.

The REST API accesses resources by using a Uniform Resource Identifier (URI) -- a character string that identifies a name or resource on the Internet. In CA SDM, resources can be objects such as tickets, assets, contacts, and so on. An application using the REST API makes an HTTP request to a URI and parses the response. Such identification enables interaction with representations of the resource over a network. Each client to server request contains all the information necessary to understand the request, and does not use any stored context on the server.

Developers use the REST API directly to send HTTP requests to the server for the resource they want to manipulate. Developers only need an HTTP client library, which is available with most programming languages. Because the REST API is based on open standards, you can use any Java programming language to access it.

Note: For information about REST HTTP methods, see the REST HTTP Methods (see page 3981).

REST and SOAP

CA SDM provides REST and SOAP web services APIs. The audience for the REST API is a UI client whereas the audience for the SOAP API is a program. REST services are about resources (manipulating objects, changing object states, exchanging representations, and using nouns rather than verbs). SOAP services are about services (calling methods, using verbs, and doing actions).

REST provides the following advantages over SOAP:

- REST is lightweight, HTTP-based, and stateless (for scalability).
- REST supports client bookmarking and caching.
- REST maintains data contract loosely.
- REST is easily consumed by front-end technologies such as WEB 2.0 and AJAX.
- REST supports XML and JSON data formats.
- REST improves performance.

REST Security

Security uses multiple authentication mechanisms including a custom approach that uses shared secret keys.

The product supports the following security authentication schemes:

- REST web services secret key authentication (uses SSL and HMAC for login)
- REST basic authentication (clear text encoded username/password)
- REST BOPSID authentication (validates CA SDM BOPSIDs)
- External (CA EEM) artifact authentication (CA EEM artifact token)

How Secret Key Authentication Works

The CA SDM Secret Key authentication is a process that verifies the following:

- The identity of the request sender.
- That the sender is a registered user.

Secret Key authentication requires that each request includes information about the identity of the request sender. The request must also include additional information that CA SDM can use to verify the authenticity of the user. When the request passes this verification test, the request is determined to be authentic. During authentication for an Access Key request, CA SDM secret authentication does the following:

1. Assigns an access key to a client. The access key identifies the client responsible for a request and uses the CA SDM session ID as the key value. Because an access key is sent as a request parameter, it is not secret. Anyone sending a request to CA SDM can use the request parameter, therefore, a secret key is needed.

2. Assigns a secret key. A secret key is a 40-character alphanumeric sequence dynamically generated by CA SDM during login. The product encrypts this secret key before storing it in the database.

3. Uses client-provided information (a request signature using the secret key) to identify the client and verify that the request is legitimate. This additional information protects users from impersonation and demonstrates possession of a shared secret known only to CA SDM and the sender of the request.

How to Version System Customizations Across CA SDM Servers

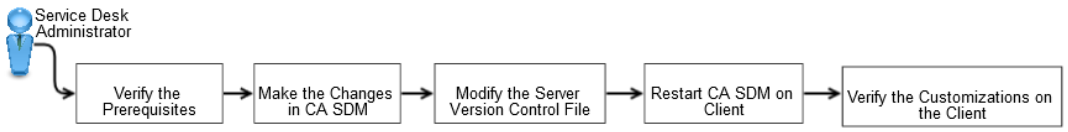
CA SDM version control helps you to manage the system customizations across all CA SDM servers (client and servers). Depending upon the CA SDM configuration, the following client and servers are used:

- Conventional configuration,
  - Client: Secondary server
  - Server: Primary server
- Advanced availability configuration,
  - Client: Application and Standby servers
  - Server: Background server

Example: As a system administrator, you added a field in the detail_usp_server.htmpl page of CA SDM. Now, you want to synchronize this change across the client and the servers. This example is used throughout the scenario to explain how the customization is synchronized.

The following diagram shows how to version the system customizations across the CA SDM servers:

How to Version System Customizations Across CA SDM Servers



Follow these steps:

1. Verify the Prerequisites (see page 1891).

2. Make changes in CA SDM. In this example, add the new field in the CA SDM HTMPL page.
3. Modify the Server Version Control File (see page 1891).
4. Restart CA SDM on Client (see page 1896).
5. Verify the Customizations on the Client (see page 1897).

Verify the Prerequisites

Verify the following prerequisites:

- Ensure that the ver_ctl option set to the **upgrade** value. When a version discrepancy is detected, an upgrade of the affected components is attempted on the client. If the upgrade is successful, the client connection with the server continues; otherwise, the connection terminates. For more information about the ver_ctl option, see the *Online Help*.
- Ensure that the server_secondary_custom.ver file is created at $NX_ROOT\site\mods directory of the primary server or background server (depending upon the CA SDM configuration). All customizations to a version control component must be done in this file. If the file does not exist, ensure that you create it at the same location.

Modify the Server Version Control File

After you complete the customization, (for example, added a field in the HTMPL page) add or update the version control components on the server version control file. A version control component can represent a file, directory, or the client_nx.env environment variable file.

Follow these steps:

1. Log in to the following server depending on your CA SDM configuration:
   - Conventional: Primary server
   - Advanced availability: Background server
2. Go to the following directory:

   ```
   $NX_ROOT\site\mods
   ```

3. Open the server_secondary_custom.ver file.
4. Add the following components:

   ```
   [ MY_USP_SERVERS_HTMPL ]
   directory="$NX_ROOT/site/mods/www/htmpl/web/analyst/Analyst"
   filename="detail_usp_servers.htmpl"
   version="2.0 , 20121119"
   o_mode="RW"
   g_mode="RW"
   w_mode="RW"
   file_ctl
   ```

Note: For more information about adding or updating version control components, see the Version Control Component (see page 1892) topic.

5. Save the server_secondary_custom.ver file.
   The version control component is added in the version control file.

Version Control Components

To define a new component,

- Use the following syntax. Items in *italics* represent data that you supply. The *component-name* and version parameters are always required. Other parameters are required, depending on the value of *control-type*. All other items represent keywords that you must enter exactly as shown in the following example:

```
[ component-name ]

version = "x.x, yyyymmdd"

control-type

filename = "filename"

directory = "directory"

link = "link-directory"

source = "source-directory"

effectivity = "effect-spec"

checksum

min_release = "release"

max_release = "release"

component_type = "file-type"

o_mode = "owner-mode"

g_mode = "group-mode"

w_mode = "world-mode"
```

Note: For more information about the parameters, see Version Control Parameters (see page 1893). For more information about the structure and syntax of version control files, see the .ver files that are installed in the $NX_ROOT\site directory. These files have useful comments and example settings that can help you.

To update an existing component entry,

- Change the parameter. For example, you change the version number.

To remove control from a component,

- Edit the component as follows:

```
! uncontrol component-name
```

Version Control Parameters

The following parameters apply to version control:

- **[component-name]**
  Specifies the name of an item under version control. The name must be unique and enclosed in square brackets. *component-name* is not case-sensitive. This parameter is required to begin a component definition.

- **version="x.x. yyymmd"**
  Specifies a version number (*x.x*) and a date (*yyyymmdd*) that define the version of the component. This parameter is required, and must be enclosed in double quotes. Version control verifies the version of a component by comparing the version number and date on the server with the version number and date on the client. Both version number and date must match for the component to be considered in sync between the client and server. Optionally, if the checksum property is enabled, the file is verified by checksum verification before being updated.

- **control-type**
  Specifies the type of version control for this component. The following settings are valid for control-type:

Setting	Description
dir_ctl	Specifies that the component represents a directory. You must provide the directory parameter to specify the path to the directory. You can also provide the filename parameter to specify the filename parameter to filter a set of files in the directory. Subdirectories are not upgraded on either UNIX or Windows.
file_ctl	Specifies that the component represents a file. You must provide the directory and filename parameters to specify the path to the file.
Nxenv _ctl	Specifies that this component represents the client_nx.env file, which is used to store internal CA SDM environment variables. CA SDM version control and the Options Manager automatically maintain this file. There is one nxenv_ctl component, and its component name must be CLIENT_NXENV.
ver_ctl	This is the default control type. It specifies that the component is generic; that is, not associated with any specific external object. You can use a generic component to provide version control for the client as a whole, or for a file or directory too large for an automatic upgrade. Components with a control type of ver_ctl cannot be upgraded; a version mismatch on a ver_ctl component when the server is in UPGRADE mode causes the client connection to fail.

- **filename="filename"**
  Specifies the name of a file under version control. It does not contain directory specifications. This parameter is required for file_ctl components, but is optional for directory (dir_ctl) control components. When used with directory components, the filename parameter acts as a file mask to restrict the files associated with the dir_ctl component. For example, if the filename for a dir_ctl component is *.README, then an upgrade from that directory includes only files ending with ".README.".

- **directory="directory"**
  Specifies the path to the directory for dir_ctl components, or to the directory containing the file for file_ctl components. This parameter is ignored for ver_ctl and nxenv_ctl components. The directory path must be enclosed in quotes, and can contain references to environment variables preceded with a $.

  Note: Always use forward slashes (not backslashes) to separate subdirectories in the path name, even on a Windows server.

- **link="link-directory"**
  Specifies a link directory on the client in the same format described previously for directory parameter. This parameter is optional for file_ctl and dir_ctl components, and ignored for ver_ctl and nxenv_ctl components. If it is specified, an upgrade to a Linux client causes a symbolic link to be placed in the link directory, pointing to the actual file copied to the location specified by the directory parameter. An upgrade to a Windows client causes the actual file to be copied to both the link and directory locations.

- **source="source-directory"**
  (Optional) Specifies a different directory on the server where the server can retrieve files for delivery. This parameter has the same format described previously for the directory parameter. It is useful if the files that are to be delivered to the client are different from the same files in the directory location on the server. This parameter is used to tell the server to retrieve the file from *source-directory* and deliver it to the location on the client specified by the directory parameter. The directory parameter is required if you specify the source parameter.

- **effectivity="effect-spec"**
  (Optional) Specifies whether the client should get this component. It lets you exclude download to some clients. If a client is not included in the effectivity specification, it does not get the component. If this parameter is omitted, all clients receive the component. The effectivity specification uses the following symbols:

  - **+ (plus sign)**
    Indicates to add a client group.

  - **- (minus sign)**
    Indicates to exclude a client group.

The following client groups are valid:

- SUN4SOL
- AIX
- LINUX
- LINUX390
- HP
- WINDOWS_CLIENTS

- UNIX_CLIENTS

For example, the following specification indicates that only UNIX clients get the files:

```
effectivity = "+ UNIX_CLIENTS"
```

- **checksum**
  Directs the component to upgrade if the checksum of the component on the client does not match the corresponding checksum on the server. If it is applied to a directory, then checksum is applied to each file.

- **min_release="release" and max_release="release"**
  Specifies the oldest and latest client to which this component should be distributed. Statements in the server_default.ver file define releases. These parameters are in the following form, where G*axx* indicates the release, and the values following are genlevels associated with the release.

  ```
  ! Release GA50 50MVV000900 50W7T000900

  ! Release GA45 45MW000900 50WTT000900
  ```

  The order indicates that GA50 is newer than GA45.

- **component_type**
  Specifies the type of component used. Following types of components are used:

Setting	Description
file	This is the default component type. It specifies that files copied to the client be obtained directly from the location on the server indicated by the directory parameter.
exe_file	Specifies that files copied to the client be obtained from a location on the server that is dependent on the client's operating system, as shown by the following: windows (Windows) sun4Sol (Solaris) hp (HP-UX) aix -- AIX) linux (Linux) linux390 (Linux390) Locations for these subdirectories are dependent on the directory parameter setting. If this parameter is set, then subdirectories are located under the indicated *directory*. Otherwise, they are located under the bin directory of the main CA SDM installation directory.

- **o_mode="owner-mode"**
  Specifies file access permissions for the owner of the file.

- **g_mode="group-mode"**
  Specifies file access permissions for users in the file owner group (used for UNIX clients only).

- **w_mode="world-mode"**
  Specifies file access permissions for users not in the file owner group (used for UNIX clients only).
  The three mode parameters allow different versions of the same executable to be maintained on the server. They specify access controls on the file when copied to the client. These parameters are used only during an upgrade operation. They consist of one to three characters, with the following significance:

Setting	Description
R	Read
W	Write
X	Execute

PC clients ignore Write and Execute permissions.

You can specify any combination of one or more file access modes. On UNIX clients, the file is given the access mode of specified. On PC clients, the file is made writable or read-only, depending on whether w_mode has been specified.

Restart CA SDM on Client

You restart CA SDM on the client servers to update the client version control files with the customizations.

Note: Select **Start**, **Settings**, **Control Panel**, **Administrative Tools**, **Services**. Right-click the **CA SDM Server** and choose **Start** to restart or start a server.

Follow these steps:

1. For the conventional configuration, restart the secondary server.
2. For the advanced availability configuration, complete the following steps:
    a. Restart all standby servers.
    b. Choose the less active application server (see page 1896).
    c. Restart the less active application server.
    d. Stop the other application server (see page 1897).
    e. Start the application server.
    f. Performs steps d and e for more application servers.

    The client connects to the server to send a list of its controlled components. The server compares the list to its own master list. The affected components on the client are upgraded.

Choose the Less Active Application Server

You choose an application server with the least user activity. Run the following command on each application server to choose the one with no or minimal active sessions.

```
pdm_webstat
```

Note: This command does not capture the SOAP or REST Web Service sessions.

Stop the Other Application Server

You inform all the active users on an application server to move to the less active application server before you stop it. Ensure that you have restarted the less active application server before moving all the users to it.

Follow these steps:

1. (Recommended) Inform all active Support Automation analysts on the application server which you want to stop, to create a ticket in CA SDM with their session information. This process ensures that the session information is not lost. For example, the Support Automation analyst is in a session with a customer to resolve a hardware issue. In such a case, the Support Automation analyst can create an issue in CA SDM with the session information before the application server shuts down.

2. Send a notification (for example, an email notification) to all the active users on the application server to move to the less active application server that you just restarted. This notification can include the details of the updated application server.

3. Execute the following command on the application server:

   ```
   pdm_server_control [-h] -q interval -s server_name
   ```

   - **-h**
     Displays the help page.

   - **-q interval -s server_name**
     Notifies a local or remote application server to quiesce in a specified time interval. This interval is the number of seconds before the server goes offline. When using this option without a server_name, the local server is notified to quiesce. This option cannot be used for a background or a standby server.

   A pop-up message is displayed to all the active users on the application server to notify them about the server shutdown and the time left for the shutdown. The users must save their work and logout within that time. The application server stops after the specified time. The users log on to the other application server to resume their work. The Support Automation analyst can refer to the ticket and resume their work.
   The application server is stopped successfully.

Verify the Customizations on the Client

You verify the version control file on the client to check if all customizations have been synchronized.

Follow these steps:

1. Log in to the following client depending on your CA SDM configuration:

   - Conventional: Secondary server

- Advanced availability: Standby server and Application server

2. Open the stdlog file from the following location:

   ```
   $NX_ROOT\log
   ```

3. Find out if all the customizations made on the server are applied on the client.

Using the Web Screen Painter (WSP)

Web Screen Painter (WSP) is a component of the CA SDM that provides tools for designing and customizing CA SDM forms. You can modify the existing forms to suit your needs, and you can create forms from scratch. WSP helps you reduce the time and effort it takes to modify and test HTMPL forms. With customized forms, your service desk analysts and customers can quickly find and enter the information that is important to your organization.

With WSP, it is also very easy to modify the database schema, such as adding new tables or columns to the database. It provides a user-friendly interface and automates the complex process of updating a schema. Using WSP, you can build and test forms using custom schema before making any changes to the database.

Readonly Preview Session

In order to allow you to preview how an updated form looks with real data, Web Screen Painter (WSP) previews forms with data from your CA SDM database. Forms you preview in WSP appear in this browser window. Since this is a readonly session, all update operations are ignored. As a reminder of this, the caption of all "Save" buttons is changed to "noSave". Please use WSP itself to logout from this session.

For detail forms, WSP shows the edit version of a form (you can display the readonly version by pressing the noSave button). When you preview a tab, WSP shows the entire detail form containing the tab, with the notebook opened to the previewed tab.

To prevent inadvertent damage to production data from a previewed form in edit mode, WSP normally suppresses updates from a preview session, so that you cannot modify the database from a preview session. To indicate this, WSP automatically changes the text on a "Save" button to "noSave", and displays a small red WSP palette in the upper left corner of the form. You can still press the noSave button (or take other actions that would normally modify the database), but CA SDM will discard your changes.

Optionally, your CA SDM system administrator may choose to enable updates from preview. When this is done, "Save" buttons are displayed normally, and the WSP palette is yellow. You should be cautious when updating the database from a preview session, as WSP preview sometimes bypasses the normal procedure for reaching a form, and the form's environment may not be completely set up. To ensure updates work correctly, return to the CA SDM main form and navigate to your form as you normally would in a standard (non-preview) CA SDM session. For more information about enabling updates from the preview session, see Assign Web Screen Painter Permissions to an Access Type (see page 1986).

Open the CA Standard Version of a Form

The CA standard version of a form is the same form with no site modifications (although it may contain CA-supplied patches). The edit window for the CA standard version of a form includes the words CA STANDARD VERSION in its title.

Follow these steps:

1. Open the form in Web Screen Painter.
2. Click File, Open CA Standard Version.

Insert Controls to a Form

The Insert menu on WSP inserts a field on the form. The insert menus follow:

- **Insert Row**
  Inserts a new row in the form on which you can place controls. If a control is selected, it causes the selected control to be the last in its row, and moves following controls to the new row.
- **Delete Row**
  Deletes a complete row. If there are controls on the row, WSP prompts you before deleting the row along with the controls.
- **Insert Textbox**
  Inserts a simple text field on the form. A text field is displayed as a box where the user can enter unedited text.
- **Insert Dropdown**
  Inserts a dropdown (select) field on the form. A dropdown box is displayed as a list of selections for a field. The user can click the dropdown arrow to choose a response from the list.
- **Insert Lookup**
  Inserts a lookup field on the form. A lookup field is displayed as a text box with a header consisting of a small magnifying glass icon followed by a link that the user can click to display a selection list.
  Lookup fields have an autofill feature. If a user clicks the hyperlink and the text specified is sufficient to identify a value in the underlying table, the pop-up search form is suppressed and CA SDM fills in the value. In addition, if the Autofill configuration property is set and the user presses the Tab key to leave a field after supplying a value, the effect is the same as clicking the hyperlink; either the value is filled in or a pop-up search form appears.
- **Insert Hierarchical Lookup**
  Inserts a hierarchical lookup field on the form. A hierarchical lookup field is displayed as a text box with a header consisting of a small plus sign icon followed by a link that the user can click to pop-up a hierarchical selection list.
  Hierarchical search fields have an autofill feature. If a user clicks the hyperlink and the text specified is sufficient to identify a value in the underlying table, the pop-up list form is suppressed and CA SDM fills in the value. In addition, if the Autofill configuration property is set and the user presses the Tab key to leave a field after supplying a value, the effect is the same as clicking the hyperlink; either the value is filled in, or a pop-up search appears.

- **Insert Date**
  Inserts a date field on the form. A date field is displayed as a text box with a header consisting of a small calendar icon followed by a link that the user could click to pop-up a date helper to allow specification of the date.

- **Insert HTML Editor**
  Inserts an HTML editor on the form for a text field that contains HTML. An HTML editor field is displayed as a multi-line text box with a header containing icons that a user can click to insert HTML tags into the text.

- **Insert Checkbox**
  Inserts a checkbox field on the form. Use checkboxes when an option may be toggled on and off.

- **Insert Read Only Textbox**
  Inserts a read-only version of the textbox field. A read-only textbox field is displayed as simple text.

- **Insert Read Only Lookup**
  Inserts a read-only version of the of the lookup field. A read-only lookup field is displayed as a hyperlink that the user can click to display the detail form for the field's value.

- **Insert Read Only Date**
  Inserts a read-only version of the date field. A read-only date is displayed as simple text, formatted as a date.

- **Insert Button**
  Inserts a rectangular button on the form. The button invokes the JavaScript string associated with it.

- **Insert Notebook**
  Inserts a Notebook with three tabs. You can use the Notebook Designer to delete tabs or insert additional tabs. A notebook allows several sets of fields to be displayed in the same physical area of the screen, with only one set visible at a time. The user can select the set of fields that is visible by clicking a named tab at the top of the notebook.

- **Insert If/Else If/Else/End If**
  Inserts conditional logic that allows a form's layout and contents to be controlled at the time the form is displayed.

- **Insert Object**
  Inserts an Object tool to place an object control on the form. Place an object control on the form when you want to introduce specific code. You can place the object control on the form in Design mode and edit the code in the Object Designer.
  If WSP cannot recognize something on a page, it converts it into an Object control. For example, an Object tag could represent straight JavaScript or Java between PDM_MACRO tags.

Add Controls to Detail Forms

This article contains the following topics:

- Add a Hierarchical Lookup Box (see page 1903)
- Add a HTML Editor (see page 1904)
- Add a Notebook (see page 1904)
- Add a Lookup Box (see page 1906)
- Add a Read Only Date (see page 1907)
- Add a Read Only Lookup Box (see page 1907)
- Add a Read Only Text Box (see page 1907)
- Add a Text Box (see page 1908)
- Add Conditional If (see page 1908)
- Add Conditional Else If (see page 1909)
- Add Conditional Else (see page 1909)
- Add Conditional End If (see page 1909)
- Add Object Button (see page 1909)
- Add a Row (see page 1910)

The Controls available in the ToolBox vary depending on the type of form that is open currently. When a Detail type form is open, the following controls are available in the ToolBox.

- Checkbox
- Command Button
- Date
- Dropdown Box
- Hierarchical Lookup Box
- Tab
- Lookup Box
- Read Only Date
- Read Only Lookup Box
- Read Only Text Box
- Text Box
- Conditional If
- Conditional Else If
- Conditional Else
- Conditional End If
- Object Button

- Row

Add a Checkbox

You can add a Checkbox control to a form.

Follow these steps:

1. Click the CheckBox button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Checkbox control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.

   The Properties dialog lists the following properties for a checkbox control:

- Attribute (see page 1915)
- Caption (see page 1915)
- Column Span (see page 1915)
- Event (see page 1915)
- On (see page 1915)
- Off (see page 1915)

Add a Date

You can add a Date control to a form.

Follow these steps:

1. Click the Date button  on the Control Palette and then, click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Date control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog lists the following properties for a date control:

- Attribute (see page 1915)
- Caption (see page 1915)
- Column Span (see page 1915)
- Size (see page 1915)
- Time (see page 1915)

Add a Dropdown Box

You can add a Dropdown box control to a form.

Follow these steps:

1. Click the Dropdown button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Dropdown Box control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog lists the following properties for a dropdown control:

- Attribute (see page 1915)
- Autofill (see page 1915)
- Caption (see page 1915)
- Column Span (see page 1915)
- Default (see page 1915)
- Event (see page 1915)
- Factory (see page 1915)
- Initial (see page 1915)
- Link (see page 1915)
- Lookup (see page 1915)
- Size (see page 1915)
- Where Clause (see page 1915)

Add a Hierarchical Lookup Box

You can add a Hierarchical Lookup Box control to a form.

Follow these steps:

1. Click the Hierarchical Lookup button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Hierarchical Lookup control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog lists the following properties for a hierarchical lookup control:

- Attribute (see page 1915)

- Autofill (see page 1915)
- Caption (see page 1915)
- Column Span (see page 1915)
- Event (see page 1915)
- Factory (see page 1915)
- Size (see page 1915)

Add a HTML Editor

You can add a HTML Editor to a form.

Follow these steps:

1. Click the HTML Editor button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The HTML Editor is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog lists the following properties for a HTML editor control:

- Attribute (see page 1915)
- Caption (see page 1915)
- Column Span (see page 1915)
- Event (see page 1915)
- Max Length (see page 1915)
- Option ID (see page 1915)
- Preview (see page 1915)
- Read Only (see page 1915)
- Rows (see page 1915)
- Size (see page 1915)
- Spell Check (see page 1915)
- Toolbar

Add a Notebook

Add a notebook to modify how HTMPL forms appear.

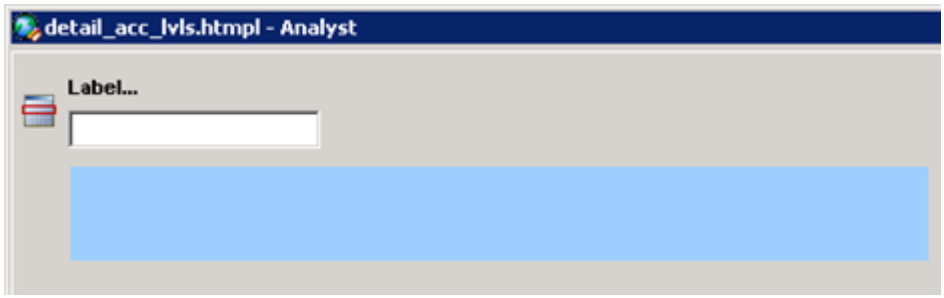
Follow these steps:

1. Create a form in WSP, such as a form based on detail.template.
   The HTMPL file opens.

2. Click the Source view and add the following lines of code:

   ```
   <PDM_MACRO name=startNotebook hdr=cng_nb>
   <PDM_MACRO name=endNotebook>
   ```

3. Click the Design view.
   The notebook area appears after the text box, such as shown in the following example:

   BSVC--WSP Notebook Design--SCR

4. Click the Source view and add the following example code after the <PDM_MACRO name=startNotebook hdr=cng_nb> line:

   ```
   <PDM_MACRO name=startTabGroup title="Additional Information">
   ```

   The following example shows the updated notebook area in Design view:

   BSVC--Additional Information Label--SCR

5. Click the Source view and add the following example code after the previous addition:

   ```
   <PDM_IF "$args.id" == "0">
   <PDM_MACRO name=tab title="Attachments" height=300 id=attmnt src="
   OP=SHOW_DETAIL+HTMPL=xx_attmnt_tab.htmpl+FACTORY=cr+PERSID=$args.
   persistent_id+NO_DP=yes">
   <PDM_ELSE
   ```

   The following example shows the updated notebook area in Design view:

   BSVC--Attachments Tab--SCR

6. Continue adding tab groups and end the notebook with the following code:

```
<PDM_MACRO name=endNotebook>
```

Note: Open default forms in WSP to view how notebooks and nested tab groups appear. For example, open the detail_in.htmpl form. You can also move tabs and tab groups within a notebook using drag-and-drop in Design view. Moving a tab group moves all the tabs within the group with it.

7. To insert a tab or tab group, right-click a control or within the notebook background and select Insert Tab, Insert Tab Group, or Insert Control (see page 1899).
   If you select Insert Tab or Insert Tab Group, WSP inserts a new tab or tab group to the left of the currently selected control. If you select Insert Control, WSP displays the Insert Control dialog that lets you add the desired control to the form.

8. Click Preview.
   Your unpublished changes appear in the web browser.

9. Save the form.
   The notebook is added.

Add a Lookup Box

You can add a Lookup Box control to a form.

Follow these steps:

1. Click the Lookup button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Lookup Box control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog lists the following properties for a lookup control:

- Attribute (see page 1915)
- Autofill (see page 1915)
- Caption (see page 1915)
- Column Span (see page 1915)
- Event (see page 1915)
- Factory (see page 1915)
- Link (see page 1915)
- Size (see page 1915)

Add a Read Only Date

You can add a Read Only Date control to a form.

Follow these steps:

1. Click the Read Only Date button  on the Control Palette and then, click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Read Only Date control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog lists the following properties for a read-only date control:

- Attribute (see page 1915)
- Caption (see page 1915)
- Column Span (see page 1915)
- Time (see page 1915)

Add a Read Only Lookup Box

You can add a Read Only lookup box control to a form.

Follow these steps:

1. Click the Read Only Lookup button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Read Only Lookup control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog lists the following properties for a read-only lookup control:

- Attribute (see page 1915)
- Caption (see page 1915)
- Column Span (see page 1915)
- Link (see page 1915)

Add a Read Only Text Box

You can add a Read Only text box control to a form.

Follow these steps:

1. Click the Read Only Text Box button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Read Only Text Box control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog lists the following properties for a read-only text box control:

- Attribute (see page 1915)
- Caption (see page 1915)
- Column Span (see page 1915)
- ID (see page 1915)

Add a Text Box

You can add a text box control to a form.

Follow these steps:

1. Click the Text Box button  on the toolbar, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Text Box control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog lists the following properties for a text box control:

- Attribute (see page 1915)
- Caption (see page 1915)
- Column Span (see page 1915)
- Event (see page 1915)
- Keep Links (see page 1915)
- Keep Tags (see page 1915)
- Max Length (see page 1915)
- Rows (see page 1915)
- Size (see page 1915)
- Spell Check (see page 1915)

Add Conditional If

You can add a conditional if control to a form.

Follow these steps:

1. Click the If button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Conditional If control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog lists the following properties for an if condition:
   Condition (see page 1915)

Add Conditional Else If

You can add a conditional else if control to a form.

Follow these steps:

1. Click the Elif button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Conditional Else If control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog lists the following properties for an else if condition:
   Condition (see page 1915)

Add Conditional Else

To add a conditional else control to a form:

1. Click the Else button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Conditional Else control is placed on the form.

Add Conditional End If

To add a conditional end if control to a form:

1. Click the Endif button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Conditional End If control is placed on the form.

Add Object Button

You can add an Object Button control to a form.

Follow these steps:

1. Click the Object button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   The Object Button control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Object Code dialog appears so you can define the source associated with the Object control.

Add a Row

To add a Row control to a form:

1. Click the ROW button  on the Control Palette and then, click the left mouse button and hold it down as you drag-and-drop it on the desired location.
   A blank Row is placed on the form. You can place the controls on the row.

Add Controls to List Forms

This article contains the following topics:

The controls available for a List form are different from the controls available for a Detail form. Some of the controls in the List form have a different set of properties compared to the controls in the Detail forms. When a List form is open, the following controls are available in the ToolBox in addition to the conditional logic controls like IF, Else, and so on, which are exactly the same the controls in the Detail form.

- Date
- Drop down Box
- Hierarchical Lookup Box
- Lookup Box
- Results List
- Text Box

Add a Command Button

To add a Command Button control to a form

1. Click the Command Button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and- drop it on the desired location.
   The Command Button control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the drop down list.
   The Properties dialog lists the following properties for a command button control:
   Caption (see page 1915)
   Disabled (see page 1915)
   Function (see page 1915)
   ID (see page 1915)
   Tooltip (see page 1915)
   Width (see page 1915)

Add a Date

To add a Date control to a form

1. Click the Date button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location of the form.
   The Date control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the drop down list.
   The Properties dialog lists the following properties for a date control:
   Attribute (see page 1915)
   Caption (see page 1915)
   Column Span (see page 1915)
   QBE Condition (see page 1915)

Add a Dropdown Box

To add a Dropdown Box control to a form

1. Click the Drop down button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location of the form.
   The Drop down Box control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the drop down list.
   The Properties dialog lists the following properties for a drop down box control:
   Attribute (see page 1915)
   Caption (see page 1915)
   Column Span (see page 1915)
   Default (see page 1915)
   OP Code (see page 1915)

Add a Hierarchical Lookup Box

To add a Hierarchical Lookup Box control to a form

1. Click the Hierarchical Lookup button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location of the form.
   The Hierarchical Lookup Box control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the drop down list.
   The Properties dialog lists the following properties for a hierarchical lookup control:
   Attribute (see page 1915)
   Caption (see page 1915)
   Column Span (see page 1915)
   Factory (see page 1915)

Add a Lookup Box

To add a Lookup Box control to a form

1. Click the Lookup button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location of the form.
   The Lookup control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog appears so you can define properties for the control. The Properties dialog lists the following properties for a lookup control:
   Attribute (see page 1915)
   Caption (see page 1915)
   Column Span (see page 1915)
   Factory (see page 1915)

Add Results List

To add a Results List control to a form

1. Click the List button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location of the form.
   The Results List control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog lists the following properties for a lookup control:
   Custom

Add Text Box

To add a Text Box control to a form

1. Click the Text Box button  on the Control Palette, and then click the left mouse button and hold it down as you drag-and-drop it on the desired location of the form.
   The Text Box control is placed on the form.

2. Click the control, click the right mouse button, and select Properties from the dropdown list.
   The Properties dialog lists the following properties for a text box control:
   Attribute (see page 1915)
   Caption (see page 1915)
   Column Span (see page 1915)
   Disabled (see page 1915)
   QBE Condition (see page 1915)
   QBE Display (see page 1915)
   QBE Value (see page 1915)
   Size (see page 1915)
   Spell Check (see page 1915)

Customize a Form

This article contains the following topics:

After you open the form you want to edit in WSP, you can use the toolbar, menu commands, and shortcuts to customize it. You can perform the following customization:

- Insert a Control
- Edit Control Properties
- Modify Menu Bars
- Modify Stylesheets
- Modify Mouse-Over Preview Form
- Modify Data Grid List on List Form
- Modify Notebooks on Detail Form
- Modify HTML and JavaScript Files

Add Controls

There are four ways to add a new control to the screen. To add any type of control to a form, follow one of these examples:

Example 1: Drag-and-Drop

1. Click on the button in the Control Palette for the control that you want to add by holding down the left mouse button as you drag the control to the desired location on the form. Release the mouse button to place the control.
   The control is placed on the form.

2. Save the form when you finish adding controls.

Example 2: Double-Click and Reposition

1. Double-click the control you want to add in the Control Palette.
   The control appears on the form.

2. Place the mouse pointer over the control, then click the left mouse button and hold it down as you reposition the control on the form.
   The control is placed in the desired location on the form.

3. Save the form when you finish adding controls.

Example 3: Right-Click and Select

1. Right-click the form at the location where you wish to add the control.
   A dropdown list appears.

2. Select the control that you want to add from the dropdown menu.
   The control is placed on the form.

3. Save the form when you finish adding controls.

Example 4: Controls Menu

1. Click the Controls menu.
   Select the control you want to add from the dropdown menu..
   The control appears on the form.

2. Place the mouse pointer over the control, then click the left mouse button and hold it down as you reposition the control on the form.
   The control is placed on the form.

3. Save the form when you finish adding controls.

Arrange Controls on a Form

You can reposition a control on a form by selecting and dragging it. This changes the control's positioning properties, which set the relative placement of a control on a form.

To move controls:

1. On the form, select the control you want to move by left-clicking on it and holding down the mouse button.
   Handles appear around the selection as the following example shows:

BSVC_r12.1--Handle Bar

2. Drag the selected control to a new position on the form and release the mouse button.

Note: If necessary, choose Undo once from the Edit menu to reverse the most recent editing action, or choose Undo repeatedly to undo a series of actions.

Move a Control

To move a control by dragging, place the mouse pointer over the control, then click the left mouse button and hold it down as you reposition the control on the form.

To resize a control by dragging it:

1. Click to select the control.
2. Place the mouse pointer over a resizing handle so that the pointer changes to ↘, ⤢, ↕, or ↔ .
3. Click the left mouse button and hold it down as you drag the control to the appropriate size.

Note: Some controls, for example, conditionals, have a white border instead of black and cannot be resized. Also, you can change the height of only certain controls, for example, text boxes.

Control Properties

This article contains the following topics:

Attribute

The Attribute property specifies the field in a CA SDM table that is associated with the control. To set this value in the Properties dialog, click the Browse button that displayed at the right side of the selection box when you click on the cell to the right of the Attribute property. Then select the attribute you want from the Select Attribute tree, and click Select.

Autofill

The Autofill feature verifies and completes a lookup field before the form is submitted. If a user clicks the hyperlink and the text specified is sufficient to identify a value in the underlying table, the pop-up search form is suppressed and CA SDM fills in the value. Autofill is also activated when a user types a new value into a lookup field and presses Tab. This causes CA SDM to query the server for a list of all records eligible for the lookup field whose first few characters match the value specified. If it finds a match, it copies the full value into the field. If it finds more than one match, it pops-up a selection form.

The Autofill property is provided for dropdown fields because CA SDM can automatically convert a dropdown field to a lookup when the number of items exceeds a configurable threshold (see the Lookup property).

You can set the Autofill property for a dropdown box, hierarchical lookup box, or a lookup box control in the Properties dialog. To specify this property, select Yes or No from the dropdown displayed when you click in the cell to the right of the Autofill property in the Properties dialog. No means that the control will not be filled in automatically when you tab out of it. True is the default Autofill value.

Caption

The Caption property specifies the header label that is displayed above a control. To specify this property, enter the desired value in the cell to the right of the Caption property in the Properties dialog.

Notebook tabs and list columns also have captions. Specify them on the Notebook (see page 1745) or List Designer (see page 1926) that replaces the Properties dialog for these controls.

You can set the caption for a menu item from the Menu Designer (see page 1745) dialog. To do so, select the appropriate item from the list and enter text in the Caption text box.

Column Span

CA SDM lays out controls on a detail form or a search filter in a HTML table, with controls in rows and columns of the table. The Column Span property specifies the number of columns occupied within the table by a control. To specify this property, enter the desired numeric value in the cell to the right of the Column Span property in the Properties dialog.

You can set the column span for a control from the Properties dialog. To do so, enter an integer in the cell to the right of the Column Span property.

Condition

The Condition property sets the conditional logic for the Conditional If and Conditional Else If controls. To specify this property, enter the desired logical condition in the cell to the right of the Condition property in the Properties dialog.

The syntax of the Condition property is as follows:

- 0 is false; any other number is true
- "" is false; “any-string” is true
- “value op value” evaluates the left and right values against each other according to op. If both values consist of digits (optionally preceded by - or +), the comparisons are done numerically. Otherwise, they are done lexically (ASCII collation). Valid op values include:

op values	What it means
==	Equal to
!=	Not equal to
>=	Equal to or greater than (must be written as \>= or >=)
<	Less than (must be written as \< or <)
>	Greater than (must be written as \> or >)
<=	Equal to or less than (must be written as \<= or <=)
&	Performs a bit-and of the left and right values. True if any bits are set; false if none are set
%	Returns true if the left value is an even multiple of the right value, and false otherwise (useful for building two-dimensional tables).

:	Performs a byte-oriented pattern match like the UNIX grep command. It returns true if the left value contains the regular expression defined by the right value

For example:

```
<PDM_IF $count \>= 10> . . .
<PDM_ELIF $count &lt; 5>  . . .
<PDM_ELSE> . . .
</PDM_IF>
```

A condition can include connectors, either && (and) or || (or). There is no precedence for either connector. The web engine examines a conditional from left to right until it reaches a connector. If the initial condition is true and the connector is ||, it considers the entire condition to be true without further evaluation. If the initial condition is false and the connector is &&, it considers the entire condition to be false without further evaluation. Otherwise, it considers the condition undermined, and evaluates the conditional from after the connector.

Default

The Default property specifies a default value for a dropdown field when the associated attribute is empty. To specify this property, enter the desired value in the cell to the right of the Default property in the Properties dialog.

When this property is specified and the underlying attribute has an empty value (normally only when a new record is created), the select box has the specified value automatically selected. This property has no effect if the specified value does not correspond to one of the selections in the dropdown, or if the field is displayed as a lookup. This property is optional; if omitted, the default for an empty attribute is to leave it empty.

Disabled

The Disabled property specifies whether the control is disabled on initial display. A disabled control is displayed in gray text, and the user can neither select it nor enter text into it.

To specify this property, select Yes or No from the dropdown displayed when you click in the cell to the right of the Disabled property in the Properties dialog. To specify that a control should be disabled by default, select Yes for this property. A disabled control can be enabled only by JavaScript executed after the form is displayed.

If you specify Yes for the Disabled property in a textbox in the search filter part of a list form, you must also specify values for the QBE Condition, QBE Display, and QBE Value properties.

Event

The Event property specifies one or more event handlers to be associated with the attribute.

To specify this property, enter the desired value in the cell to the right of the Event property in the Properties dialog. Specify the value in the same format, as it would appear on an HTML statement, except that any double quotes in the handler string must be prefixed by three backslashes. For example, the Event property for the Request Area control on form detail_cr.htmpl is:

```
onChange=\\\"change_category_func('cr')\\\"
```

This specifies that the JavaScript function change_category_func('cr') should be invoked whenever the value of the field changes.

You can specify multiple event handlers in the same Event property by separating them with spaces. Consult HTML or JavaScript documentation for a list of available event handlers and their usage.

Factory

The Factory property specifies the CA SDM table referenced by a field in a lookup or dropdown control. This property is normally left blank, meaning that the factory defaults to the one associated with the attribute in the CA SDM object definition. It is seldom necessary or useful to override this value.

To specify this property, select the desired value from the dropdown displayed when you click in the cell to the right of the Factory property in the Properties dialog.

Function

The Function property of a menu item specifies the JavaScript invoked when the user selects the item. To specify this property, enter the desired value in the cell to the right of the Function property in the Menu Designer dialog. Any valid JavaScript can be specified for Function, except that double quotes must be preceded by a backslash.

The following predefined JavaScript functions may be useful:

- **upd_frame(form)**
  Loads a new form into the main window content frame.
- **create_new(factory, use_template, width, height [,args])**
  Pops-up a form to define a new record.
- **popup_window(name, form[, width, height [,features [,args]]])**
  Pops-up a new window.
- **showDetailWithPersid(persid)**
  Pops-up a detail record.

In the above functions:

- **form**
  Is either an HTMPL file name of the form xxx.htmpl or an operation code (example: CREATE_NEW).
- **factory**
  Is the name of a database object.
- **use_template**
  Specifies whether or not the new object should be created with a template that the user must select from a list. It can either be true or false.

- **width**
  Is the desired form width in pixels or zero for default.

- **height**
  Is the desired form height in pixels or zero for default.

- **features**
  Is a list of window features, in the same format as used with the JavaScript window.open() function.

- **args**
  Is one or more arguments of the form "keyword=value" for the operation specified for form.

- **persid**
  Is a persistent ID in the form factory:id.

ID

The ID property sets the HTML or JavaScript id of the command button, tab, or read-only text box controls for use in JavaScript that references the control. To specify this property, enter the desired value in the cell to the right of the ID property in the Properties dialog.

Initial

The Initial property specifies the initial value of a dropdown field. When this property is specified, the database value of the attribute associated with the control is ignored and the select box has the specified initial value selected.

To specify this property, enter the desired value in the cell to the right of the Initial property in the Properties dialog. The specified value should correspond to one of the selections in the dropdown; if it does not, the initial value for the dropdown is empty. This argument is optional; if not specified, the dropdown displays the database value of its associated attribute.

Keep Links

The Keep Links property specifies whether or not HTML Action: tags within a text box on the read-only view of a detail form are displayed as hyperlinks or as simple (non-clickable) text.

To specify this property, select Yes or No from the dropdown displayed when you click in the cell to the right of the Keep Links property in the Properties dialog. Specify Yes for this property to specify that Action: tags should be displayed as hyperlinks. Specify the default value of No to specify that Action: tags should be displayed as literal text. HTML tags other than Action: tags are always displayed as literal text (unless the Keep Tags property is specified).

The Keep Links property is ignored if the Keep Tags property is specified as Yes. Note that this property affects only the read-only view of a detail form. HTML is always displayed as literal text in Edit view.

Keep Tags

The Keep Tags property specifies whether or not HTML tags within a text box on the read-only view of a detail form are formatted as HTML or as simple (non-clickable) text.

To specify this property, select Yes or No from the dropdown displayed when you click in the cell to the right of the Keep Tags property in the Properties dialog. Specify Yes for this property to specify that HTML tags should have their normal effect. Specify the default value of No to specify that HTML tags should be displayed as literal text.

A value of Yes for Keep Tags overrides the Keep Links property. Note that this property affects only the read-only view of a detail form. HTML is always displayed as literal text in Edit view.

Link

The Link property specifies whether or not a Dropdown, Lookup, or Read Only Lookup field should be displayed as a clickable hyperlink in the read-only view of a detail form. A user can click on a field displayed as a hyperlink to show the detail of the record referenced by the field.

To specify this property, select Yes or No from the dropdown displayed when you click in the cell to the right of the Autofill property in the Properties dialog. Select the default value of Yes to specify that the field should be displayed as a link on the read-only view; specify No to specify that the field should be displayed as simple non-clickable text on the read-only view.

Lookup

The Lookup property specifies whether or not a Dropdown control is converted into a Lookup control if the number of entries for the Dropdown control is exceeds an installation-specified threshold (normally ten).

To specify this property, select Yes or No from the dropdown displayed when you click in the cell to the right of the Lookup property in the Properties dialog. Select the default value of Yes to specify that the Dropdown control should become a lookup control if the number of entries in the dropdown exceeds the threshold. Select No to specify that the control should always remain a dropdown, regardless of how many entries it contains.

Max Length

The Max Length property specifies the maximum number of characters that can be typed in the Textbox control. This property is normally left blank, meaning that the maximum defaults to the actual length of the database column associated with the textbox.

To specify this property, enter the desired numeric value in the cell to the right of the Max Length property in the Properties dialog.

Off

The Off property sets the value that is displayed on read-only screens when a checkbox value is false. To set this value, enter text in the cell to the right of the Off property.

On

The On property sets the value that is displayed on read-only screens when a checkbox value is true. To set this value, enter text in the cell to the right of the On property.

OP Code

The Op Code property specifies the SQL select operator used with the value of a dropdown on a search filter. The value must be a character string beginning with “QBE.” followed by an operator chosen from:

Operator	Description
EQ	equals
NE	not equals
LT	less than
GT	greater than
LE	less than or equals
GE	greater than or equals
IN	LIKE

The default value of QBE.EQ specifies that the search filter should select rows where the attribute associated with the control exactly matches the value selected from the dropdown.

To specify this property, enter the desired value in the cell to the right of the OP Code property in the Properties dialog.

Option ID

The Options ID sets the HTML or JavaScript id of the option buttons for use in JavaScript that references the control. To specify this property, enter the desired value in the cell to the right of the Options ID property in the Properties dialog.

Preview

The Preview property specifies whether or not to show the Quick View mode in the dtlHTMLEditBox. To specify this property, select Yes or No from the dropdown displayed when you click in the cell to the right of the Preview property in the Properties dialog. Select the default value of Yes to specify that the dtlHTMLEditBox control will have the quick view mode. Select No to specify that the control will have only the HTML source mode.

Preview Clause

The Preview Clause property specifies a where clause to retrieve data for the form. WSP uses this where clause to retrieve data to be displayed on the form when it is previewed. If no preview clause is specified, WSP finds the most recently added row in the table associated with the form, and displays that data on the previewed form.

Preview Mode

The Preview Mode property specifies how the form will be previewed during preview mode. To set the Preview Mode of the form, select edit or read-only from the dropdown list to the right of the Preview Mode property. Edit is the default Preview Mode value. If you are previewing the form, in read-only mode, you will not be able to edit any of the control boxes on the form. If the Preview Mode is set to edit, you can edit the control boxes.

Preview URL

The Preview URL property specifies the preview URL. This can be an HTMPL file name, in the form xxxx.htmpl; a CA SDM URL (used unaltered if it begins with “OP=”); or the keyword “no”, indicating the form cannot be previewed. A value not beginning OP= is modified by replacing a reference of the form {factory} or {factory:} with an id or persistent id (respectively) of the most-recently created row from the referenced factory that you are authorized to see.

QBE Condition

The QBE Condition property specifies the SQL select operator used with the QBE Value property of a disabled textbox field on a search filter. The value must be a character string chosen from:

Operator	Description
EQ	equals
NE	not equals
LT	less than
GT	greater than
LE	less than or equals
GE	greater than or equals
IN	LIKE

For example, a value of IN specifies that the search filter should select rows where the attribute associated with the disabled textbox control matches the QBE Value property according to the rules of an SQL LIKE comparison.

To specify this property, enter the desired value in the cell to the right of the QBE Condition property in the Properties dialog.

QBE Display

The QBE Display property specifies the value displayed to the user for a disabled textbox field on a search filter. To specify this property, enter the desired value in the cell to the right of the QBE Display property in the Properties dialog.

QBE Value

The QBE Value specifies the value used for comparison in the portion of an SQL select where clause generated from a disabled textbox field on a search filter. The generated where clause includes a portion selecting rows where the attribute associated with the control compares with the value specified for QBE Value using the operator specified for QBE Condition.

To specify this property, enter the desired value in the cell to the right of the QBE Value property in the Properties dialog.

Read Only

Like all other detail controls in detail form, when you are in read only mode you are not able to edit the control.

Note: This parameter is ignored when Bound is set to Yes.

Rows

The Rows property specifies the number of rows that a text box control or a HTML editor will occupy on a form. To specify this property, enter the desired numeric value in the cell to the right of the Rows property in the Properties dialog.

Note: This property is available only for text boxes on the detail form and not for text boxes in the list forms.

Size

The Size property specifies the width of the control in pixels. If this property is left blank, the control is displayed at whatever width is required to hold its data.

To specify this property, enter the desired numeric value in the cell to the right of the Size property in the Properties dialog.

Spell Check

The Spell Check property specifies whether or not a Textbox control should have Spelling button to the right of its caption to allow the user to spellcheck the contents of the text box. To specify this property, select Yes or No from the dropdown displayed when you click in the cell to the right of the Spell Check property in the Properties dialog. Select Yes to specify that a Spelling button should be displayed; select the default value of No to specify no button.

Time

The Time property specifies whether or not the time will be displayed along with the date for the Date and Read Only Date controls. To specify this property, select Yes or No from the dropdown displayed when you click in the cell to the right of the Time property in the Properties dialog. Select the default value of Yes to specify that the time should be displayed; select No to specify that only the date should be displayed.

Title

The Title property specifies the title of the element.

To specify this property, enter the desired value in the cell to the right of the Title property in the Properties dialog.

Toolbar

The Toolbar property specifies which toolbar set will be shown in the HTML Editor associated to the dtlHTMLEditBox control.

- **tmpl**
  Displays the toolbar set for document template editor.

- **reportcard**
  Displays the toolbar set for report cards editor.

- **default**
  Displays the default toolbar set.

Tooltip

The Tooltip property specifies the text displayed when the user places the mouse pointer over a control item.

To specify this property, enter the desired value in the cell to the right of the Tooltip property in the Properties dialog.

Where Clause

The Where Clause property specifies a where clause to select the values included in a Dropdown control on a detail form. This property is optional; if left empty, a dropdown on a detail form includes all rows from the table referenced by the attribute associated with the control.

To specify this property, enter the desired value in the cell to the right of the Where Clause property in the Properties dialog.

Wildcard

The Wildcard feature enables a wildcard search for Lookup and Hierarchical Lookup boxes on a List form. A wildcard search is equivalent to adding the "%" symbol around a text string when performing a search. For example, using the string %option% when performing a search on a text field, would retrieve all of the records that contain the word "option" in that text field. To specify this property, select Yes or No from the dropdown displayed when you click in the cell to the right of the Wildcard property in the Properties dialog. Yes means that the control will automatically have the wildcard property enabled. No is the default Wildcard value. If this option is true, the % symbols are no longer required on searches.

Width

The Width property specifies the width of a button control in pixels. If this property is left blank, the control is displayed at whatever width is required to hold its data.

To specify this property, enter the desired numeric value in the cell to the right of the Size property in the Properties dialog.

Menu Designer

Use the Menu Designer dialog in WSP to add a menu bar, menus, submenus, and menu commands to the open form.

Add a Menu Bar

You can add a menu bar to a form.

Follow these steps:

1. Select File, New.
2. On the New Form window, select menubar.template as the File Name.
3. On the menubar.htmpl window, double click to open the Menu Editor dialog. The list box at the top left area of the dialog shows the structure of the menu as you define it.
4. To add the first item, enter its name in the Caption field. To add subsequent items, click Add before entering the caption.

List Designer

This article contains the following topics:

List forms (HTML templates with names of the form list_xxx.htmpl) are used to search the database and display search results. They consist of a search filter at the top of the form, where the user specifies search criteria, and a results list at the bottom of the form, listing records retrieved by the search. Use the drag-and-drop method to design the results list.

Add a Results List

BSVC_r12.1--List

To add the results list control to the List form, use drag-and-drop on the List button to place it on the desired area. This action places a blank frame on the form. Double-click the frame to define the columns and headers.

Modify Results List

To modify the Results List, double-click it and modify the properties. Click OK after making the required changes.

How to Disable Tenant Column Sorting

By default, you can sort the Tenant column on a list form. To disable Tenant column sorting, add the following value to the appropriate list form:

```
tenantSort=no
```

Note: If a form includes a Tenant column, and you do not want it sorted, you can add the following line to the list form:

```
var tenantSort = "no"
```

The Tenant column is disabled on the list form.

Disable the Export Button on a List Form

You can disable the Export button that appears on the list form pages in CA SDM.

Follow these steps:

1. Open a list form, such as list_cr.htmpl (Request List).
2. Double-click the results list.
   The properties dialog appears, showing the existing list definition.
3. On the Source tab, locate the sfStart macro.
4. Change the value to export=no as follows:

   ```
   <pdm_macro name=sfStart factory=nr export=no>
   ```

   The Export button is disabled on the list form.

How to Export Fields Not Included on List Forms

You can include a new field to export but not list.

Follow these steps:

1. Open the Properties dialog and click Add.
2. Select an attribute from the Attribute list, for example, Urgency.
3. Select the Export option.
4. On the Source tab, replace NAME=lsCol with NAME=lsExport as follows:

   ```
   <PDM_MACRO NAME=lsExport hdr="Urgency" attr=urgency justify=left>:
   ```

5. Click OK.
   When a user clicks the Export button on a list form, the Urgency field is exported.

Export the Relative Attribute Value

By default, the common name value of an SREL column is exported. You can export the Relative Attribute value by modifying the lsCol macro.

Follow these steps:

1. Open a list form for editing, for example, list_cr.htmpl.
   The list form opens.

2. Click the Source tab and locate the lsCol macro as follows:

   ```
   <PDM_MACRO NAME=lsCol hdr="Priority/Parent" attr=priority sort="DESC">
   ```

3. Copy the code string to the next line, and do the following:

   - Change the lsCol value to lsExport.
   - Add the common_name= no option.

4. Click OK.
   When a user clicks the Export button on the list form, the Relative Attribute value exports.

PDM Macro Definitions

This article contains the following topics:

- tabBanner (see page 1985)
- tabList (see page 1986)

PDM_Macro

CA SDM builds web forms in a language named HTMPL. HTMPL extends standard HTML with references to server variables and a number of proprietary tags of the form PDM_xxx. One of these tags, PDM_MACRO, copies a named JavaScript code segment from the database into the form. Most PDM_MACRO tags invoke client-side JavaScript that builds the web forms just in time, immediately before they are presented to the user. Most web form controls are built with the PDM_MACRO tag. For example, the PDM_MACRO tag that builds the site field on the Location Detail form is coded as follows:

```
<PDM_MACRO NAME=dtlLookup hdr="Site" attr="site">
```

A PDM_MACRO tag contains one or more keyword parameters (properties). The NAME parameter is required on every PDM_MACRO to specify the name of the macro. Other parameters are required or optional depending on the macro.

Note: Site customization of PDM_MACRO definitions stored in the database is not supported and should not be attempted.

btnEndRow

The btnEndRow macro marks the end of a group of one or more buttons displayed in a horizontal row on a form. The button row starts with either a btnStartRow macro or with a button macro with the NewRow=yes argument. The button row ends with either a btnEndRow macro or with a button macro with the EndRow=yes property. For example:

```
<PDM_MACRO name=btnStartRow . . .>
<PDM_MACRO name=button . . .>
<PDM_MACRO name=button . . .>
. . .
<PDM_MACRO name=btnEndRow>
```

This macro has no properties.

btnStartRow

The btnStartRow macro marks the start of a group of one or more buttons displayed in a horizontal row on a form. The button row starts with either a btnStartRow macro or with a button macro with the NewRow=yes argument. The button row ends with either a btnEndRow macro or with a button macro with the EndRow=yes property. For example:

```
<PDM_MACRO name=btnStartRow . . .>
<PDM_MACRO name=button . . .>
<PDM_MACRO name=button . . .>
. . .
<PDM_MACRO name=btnEndRow>
:
```

This macro has the following properties:

- **centered=true|*false***
  Specifies whether the row of buttons is centered on the form. When you do not specify this property, the row of buttons is left-justified.

- **padding=*0*|*number***
  Specifies the number of hard (nonbreaking) spaces between buttons in the row. When you do not specify this property, buttons are placed as close together as possible.

button

The button macro defines a button that a user of a form can click to invoke an action.

This macro has the following properties:

- **btnType=negative|*positive***
  Specifies whether a button performs a positive action (such as Save) or a negative action (such as Cancel). This specification is for documentation only; specifying a button as positive or negative has no effect on the appearance or use of the button.

- **Caption=*text***
  (Required) Specifies the text for the label of the button. You can optionally end the caption with a hotkey hint enclosed in square brackets, for example, Caption="Save[Sv]". When you provide a hotkey hint, CA SDM selects the hotkey for the button from the characters in the hint. When you do not provide a hotkey hint, CA SDM selects the hotkey from the characters of the entire caption.

- **Disabled=true|*false***
  Specifies whether the button is disabled on the initial display. When you do not specify this property, the button is enabled.

- **EndRow=yes|*no***
  Specifies whether this button is the last of a horizontal row of buttons. If specified as EndRow=yes, CA SDM automatically inserts a btnEndRow macro after this button. When you do not specify this property, CA SDM does not configure the button as the last one in a row.

- **Func=*string***
  (Required) Specifies the JavaScript that is invoked when the user of the form clicks the button.

- **hotkey_name=*string***
  (Required) Specifies the caption for selecting a hotkey. You must specify this property and an ASCII string. CA SDM selects the hotkey for the button from the characters in the hotkey_name string. The hotkey_name macro is ignored in locales using the Latin alphabet; these locales always use the Caption to determine a hotkey.

- **ID=*string***
  (Required) Specifies a JavaScript identifier for the button.

- **NewRow=yes|*no***
  Specifies whether this button is the first of a horizontal row of buttons. When you specify NewRow=yes, the product automatically inserts a btnStartRow macro before this button. When you do not specify this property, the product does not configure the button as the first one in a row.

- **tabIndex=n|*-1***
  Specifies the HTML tabIndex for the button. TabIndex is meaningful only in relation to other HTML elements on the form with a tabIndex. A user of the form tabs from element to element in sequence by the tabIndex values of the element. When you do not specify this property, the button receives a default tabIndex.

- **Tooltip=*string***
  Specifies the tooltip text for the button. When you do not specify this property, the property defaults to the button caption.

- **Width=*0*|*number***
  Specifies the width of the button in pixels. If you omit this property or specify it as 0, the product creates the button exactly wide enough for its caption.

cmdbMetadata

The cmdbMetadata macro provides attribute-level metadata for the versioning, TWA viewer, and CMDBf viewers for use when displaying CI and transaction information. This metadata is used for the following purposes:

- To categorize and provide help information about each attribute.

- To map each MDR provider attribute name with its corresponding CA CMDB attribute name so they are displayed together. This macro does not create a UI control and typically, use it in an HTMPL file. The HTMPL file is then included in a display form, which the versioning, TWA viewer, and CMDBf viewers use.

This macro has the following properties:

- **attr=*attributeName***
  Specifies a CA CMDB attribute name. This property is required in all cases except hiding a provider attribute from the CI displays. All subsequent properties refer to the handling of this attribute. The attribute name specified must be a valid, case sensitive, CI attribute name.

- **category=*attributeCategoryName***
  Specifies the category of this attribute to group-related attributes on the versioning and CMDBf viewer attribute displays. The category is typically the tab that contains the attribute on the CI detail display. Attributes are sorted by category on those forms.

- **common=yes|*no***
  (Deprecated) Specifies whether this attribute is a common attribute (in the nr object). Do not use this property. Do not specify an extension for the metadata for common attributes.

- **currentcivalue=*dottedNotation***
  Explicitly specifies special dotted notation for the current value of the attribute. This property is required when the default dotted notation to access the current CI value is incorrect. For example, this property is required when defining common attributes, and those attributes are not in the extension table.

  
  Note: For dotted notation examples, see the cmdb_metadata_common.htmpl form.

- **dbcolumn=*UAPMcolumnName***
  Specifies a UAPM database column name so that it can be associated with the specified CA CMDB attribute name.

- **extension=*objectName***
  Specifies the extension object name that contains the attribute name. This property is required when defining attributes that are in an extension table.

- **heading=*string***
  Specifies a short label that describes this attribute. Typically, you set this property the default label that the CI detail form displays.

- **help=*string***
  Specifies a brief description of the attribute.

- **hide_provider_attr=yes|*no***
  (For use with the CMDBf viewer only) Hides the provider attribute from the CMDBf viewer display when you specify YES. Requires the specification of provider_attr and either provider_name or provider_name_regexp.

- **provider_attr=*MDRattributeName***
  (For use with the CMDBf viewer only) Specifies the MDR provider attribute name that maps to the current attribute (attr). Requires the specification of attr, and either provider_name or provider_name_regexp.

- **provider_name=*MDRname***
  (For use with the CMDBf viewer only.) Specifies the MDR provider name that is associated with the MDR attribute name (provider_attr). This property specifies an exact match with a particular MDR provider name. Requires the specification of provider_attr. This property is mutually exclusive with provider_name_regexp.

- **provider_name_regexp=*regularExpression***
  (For use with the CMDBf viewer only.) Specifies the MDR provider name regular expression that is associated with the MDR attribute name (provider_attr). This property specifies a regular expression pattern to match with the MDR provider names. Regular expressions use a valid JavaScript RegExp() pattern. Requires the specification of provider_attr. For example, \"MyMdr.*\" matches all provider names starting with \"MyMdr\" such as \"MyMdr1\", \"MyMdrAbcd\", and so on. The characters \".*\" indicate to match all provider names. This property is mutually exclusive with provider_name.

- **standardcivalue=*dottedNotation***
  Explicitly specifies special dotted notation for the corresponding value of the attribute for the standard CI. This property is required when the default dotted notation to access the standard CI value is incorrect. For example, this property is required when defining common attributes, and those attributes are not in the extension table.

dtlCheckbox

The dtlCheckbox macro specifies a check box control on an HTMPL detail form. The control appears as follows:

- A check box on the edit view of the form.
- The text specified by the on or off properties on the read-only view.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1|number***

  Specifies the number of columns on the form.

- **evt=*"eventName='script'"***

  Specifies one or more HTML event handlers in the same way you specify them in an HTML statement, with quotes escaped as required. For example:

```
evt="onclick='myfunc()' onchange=\\\"myfunc2()\\\""
```

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **off=*0|text***
  Specifies the text displayed on a read-only form when the check box is not selected.

- **on=*1|text***
  Specifies the text displayed on a read-only form when the check box is selected.

- **title=*text***

  Specifies the title for screen reader users.

dtlCheckboxReadonly

The dtlCheckboxReadonly macro specifies a read-only check box control on an HTMPL detail form. The control appears as the text specified by the on or off properties on both the edit and read-only views of the form.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1|number***

  Specifies the number of columns on the form.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **off=*0|text***
  Specifies the text displayed on a read-only form when the check box is not selected.

- **on=*1|text***
  Specifies the text displayed on a read-only form when the check box is selected.

dtlCheckboxWithDesc

The dtlCheckboxWithDesc macro defines a check box control with a description.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **code=*string***
  Specifies the internal value of the check box. This property is not intended for customer use.

- **desc=*text***
  Specifies the text of the description appearing after the check box.

- **evt=*"eventName='script'"***

  Specifies one or more HTML event handlers in the same way you specify them in an HTML statement, with quotes escaped as required. For example:

```
evt="onclick='myfunc()' onchange=\\\"myfunc2()\\\""
```

- **func=*script***
  Provides the function to select or clear the check box. This property is not intended for customer use.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **title=*text***

  Specifies the title for screen reader users.

- **padding=*0*|*number***
  Specifies the number of spaces before the check box.

- **sameCol=true|*false***
  Specifies that the check box and description are in one column. By default, the check box and description are in two columns.

- **title=*text***

  Specifies the title for screen reader users.

- **value**
  Specifies the value of the attribute in the read-only view.

dtlDate

The dtlDate macro specifies a date control on an HTMPL detail form. A date control contains a date and time that can be edited with a date picker pop-up in the edit view of a detail form.

This macro has the following properties:

- **attr**
  Specifies the name of the attribute.

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **make_required=YES|*NO***
  Makes a field required when you specify YES regardless of whether the associated attribute is required at the object level. A required field forces the user to specify a nonblank value.

- **size=*20*|*number***

  Specifies the width of the input field.

- **time=*yes*|no**
  Specifies whether the field contains both a date and time, or only a date.

dtlDateDropdown

The dtlDateDropdown macro specifies a date control on an HTMPL detail form. When empty, this field displays as a drop-down control on the edit view of the form. The drop-down control includes date selections such as "In One Day" or "In One Week". This control displays date fields with a nonempty value in the same way as the dtlDate control.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **codename=*string***

  Specifies the name of a set of values from the ui_selection object that are displayed in the date drop-down control. The values are those values with code attributes that match the value specified for codename.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **evt=*"eventName='script'"***

  Specifies one or more HTML event handlers in the same way you specify them in an HTML statement, with quotes escaped as required. For example:

```
evt="onclick='myfunc()' onchange=\\\"myfunc2()\\\""
```

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **make_required=YES|*NO***

Makes a field required when you specify YES regardless of whether the associated attribute is required at the object level. A required field forces the user to specify a nonblank value.

- **size=*20*|*number***

  Specifies the width of the input field.

dtlDateReadonly

The dtlDateReadonly macro specifies a noneditable date control on an HTMPL detail form.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **time=*YES*|NO**
  Specifies whether the field contains both a date and time, or only a date.

dtlDropdown

The dtlDropdown macro specifies a drop-down selection control on an HTMPL detail form. The control appears as a drop-down or lookup on the edit view of the form, and as the text in the read-only view.

Note: The CA SDM administrator can specify the maximum number of entries a drop-down list should contain (default 10); when the size of a drop-down list exceeds this number, CA SDM automatically converts the list to a lookup. You can override this behavior with the lookup property of this macro.

This macro has the following properties:

- **attr*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **autofill=*yes*|no**

  Specifies whether the field allows autofill when it is displayed as a lookup. Autofill lets a user enter a value in the field by typing the first few characters of a value and pressing Tab. These actions cause the product to perform one of the following actions:

  - Request the full value for the field from the server.
  - Pop up a selection form when the specified value is missing or ambiguous.

- **cbwidth=*0*|*number***
  Specifies the width of the drop-down list in pixels. If omitted or specified as zero, the list automatically sizes to the width of its widest entry.

- **codename=*string***

  Specifies the name of a set of values from the ui_selection object that are displayed in the date drop-down control. The values are those values with code attributes that match the value specified for codename.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **default=*text***

  Specifies the default value when the attribute is null.

- **evt=*"eventName='script'"***

  Specifies one or more HTML event handlers in the same way you specify them in an HTML statement, with quotes escaped as required. For example:

```
evt="onclick='myfunc()' onchange=\\\"myfunc2()\\\""
```

- **extraURL=*string***

  Specifies a where clause predicate in URL format to restrict the contents of the control.

- **factory=*name***

  Specifies the name of a Majic factory for the selection list. Defaults to the factory referenced by the associated attributes, and so is not typically required.

- **hdr=*text***

Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **title=*text***

  Specifies the title for screen reader users.

- **initial=*value***
  Specifies the initial selection in the drop-down list, overriding the value of the attribute in the database.

- **link=*yes*|no**

  Specifies whether the control on the read-only view is a link to detail for the value of the attribute.

- **list_display=*attributeName***
  Specifies the common attribute name of the table. Effective only if use_list_display=1, codename is blank, and the factory, rel_attr_name, and whereclause properties are supplied.

- **list_orderby=*attributeName***
  Specifies the order of the drop-down list. Effective only if use_list_display=1, codename is blank, and the factory, rel_attr_name, and whereclause properties are supplied.

- **lookup=*yes*|no**
  Specifies whether the field should automatically convert to a lookup if the number of entries in the drop-down list exceeds a configured value (typically 10).

- **make_required=YES|*NO***

  Makes a field required when you specify YES regardless of whether the associated attribute is required at the object level. A required field forces the user to specify a nonblank value.

- **rel_attr_name=*attributeName***
  Specifies the attribute from the referenced table that is stored. This property is required when use_list_display=1 is specified, codename is blank, and the factory, list_display, and whereclause properties are supplied.

- **size=*20*|*number***

  Specifies the width of the input field.

- **title=*text***

  Specifies the title for screen reader users.

- **use_list_display=*0*|1**
  Specifies whether the drop-down control should be built from an explicit query instead of from the referenced attribute. When use_list_display=1, the factory, list_display, rel_attr_name, and whereclause properties must also be supplied.

- **whereclause=*string***
  Specifies a where clause.

dtlDropdownWithDesc

The dtlDropdownWithDesc macro specifies a drop-down list on an HTMPL detail form. A caption (header) precedes the drop-down list with a text description following it.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **desc=*text***
  Specifies the description that appears after the drop-down list.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **sel_fac=*factoryName***
  Specifies a factory whose entire contents will display in the drop-down list. This property is effective only if sel_list is empty.

- **sel_list="text@,@value@,…,@text@,@value"**
  Specifies a comma-separated list of values for the drop-down. Values are specified in pairs, with the displayed value followed by the corresponding internal value. At symbols (@) delimit the individual values, except for the first and last value in the list.

- **title=*text***

  Specifies the title for screen reader users.

- **value=*string***
  Specifies the value of the attribute in the read-only view.

dtlEnd

The dtlEnd macro marks the end of the macros that define the contents of a detail form. This macro must be the last macro on the form. You structure all detail forms with the following code:

```
<PDM_MACRO name=dtlForm . . .>
<PDM_MACRO name=dtlStart . . .>
```

```
<PDM_MACRO name=dtlStartRow . . .>
. . .
<PDM_MACRO name=dtlEnd>
```

This macro has no properties.

dtlEndDiv

The dtlEndDiv macro marks the end of a group of detail form macros that JavaScript can show or hide. Pair this macro with a dtlStartDiv macro and use a dtlEndTable macro. For example:

```
<PDM_MACRO name=dtlStartDiv divid="my_div" . . .>
. . .
<PDM_MACRO name=dtlEndTable>
<PDM_MACRO name=dtlEndDiv>
```

This macro has no properties.

dtlEndTable

The dtlEndTable macro marks the end of an HTML table, and is not intended for customer use. No dtlStartTable macro exists; the detail form table automatically starts and ends HTML tables as required for the layout. A dtlEndTable macro is required only when a macro group must be separated into HTML blocks, such as when dtlStartDiv and dtlEndDiv create a division.

dtlEndTable has no properties.

dtlForm

The dtlForm macro marks the beginning of the macros that define the contents of a detail form. This macro must be the first macro on the form. All detail forms must be structured with the following code:

```
<PDM_MACRO name=dtlForm . . .>
<PDM_MACRO name=dtlStart . . .>
<PDM_MACRO name=dtlStartRow . . .>
. . .
<PDM_MACRO name=dtlEnd>
```

This macro has the following properties:

- **button=*true*|false**
  Specifies whether to show the default buttons on the edit view and the Edit button on the read-only view. The default buttons are Save, Cancel, and Reset.

- **factory=*name***

  Specifies the name of a Majic factory for the selection list. Defaults to the factory referenced by the associated attributes, and so is not typically required.

- **hideeditbtn=true|*false***
  Specifies whether to hide the Edit button in the read-only view.

- **onsubmit=*script***
  Overrides the default form submit handler. The default handler is sufficient for most cases.

- **saveclose=true|*false***
  Specifies whether to show a "Save and Close" button in the edit view.

- **skip_tenant_hdr=yes|*no***
  Specifies whether to suppress the tenant field at the header of the form.

- **skiphdr=yes|*no***
  Specifies whether to skip standard form headers, such as default buttons.

dtlHier

The dtlHier macro specifies a hierarchical lookup control on a detail form. In the edit view, a user can click the caption (header) of the control to pop up a hierarchical selection form.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **autofill=*yes*|no**

  Specifies whether the field allows autofill when it is displayed as a lookup. Autofill lets a user enter a value in the field by typing the first few characters of a value and pressing Tab. These actions cause the product to perform one of the following actions:

  - Request the full value for the field from the server.
  - Pop up a selection form when the specified value is missing or ambiguous.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **common_name=*attributeName***
  Specifies the name of the attribute from the referenced table that should be displayed on the detail form. This macro is not intended for customer use.

- **evt=*"eventName='script'"***

  Specifies one or more HTML event handlers in the same way you specify them in an HTML statement, with quotes escaped as required. For example:

```
evt="onclick='myfunc()' onchange=\\\"myfunc2()\\\""
```

- **factory=*name***

Specifies the name of a Majic factory for the selection list. Defaults to the factory referenced by the associated attributes, and so is not typically required.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **make_required=YES|*NO***

  Makes a field required when you specify YES regardless of whether the associated attribute is required at the object level. A required field forces the user to specify a nonblank value.

- **size=*20*|*number***

  Specifies the width of the input field.

dtlHTMLEditbox

The dtlHTMLEditbox macro defines an HTML edit field in a detail form.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **bound=*yes*|no**
  Specifies whether the control is bound to an attribute.

- **className=*value***
  Specifies a style sheet class.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **escape=*JS2*|C|JS|HTML**
  Specifies how data is escaped in the read-only view. This property is not intended for customer use.

- **evt=*"eventName='script'"***

  Specifies one or more HTML event handlers in the same way you specify them in an HTML statement, with quotes escaped as required. For example:

```
evt="onclick='myfunc()' onchange=\\\"myfunc2()\\\""
```

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **make_required=YES|*NO***

  Makes a field required when you specify YES regardless of whether the associated attribute is required at the object level. A required field forces the user to specify a nonblank value.

- **maxlength=*number***

  Specifies the maximum length of the edit field.

- **optionid=*string***
  Specifies the JavaScript identification of the HTML edit field control. This property is not intended for customer use.

- **persid=*value***
  Specifies the persistent identifier of the object displayed in the edit field. This property is not intended for customer use.

- **preview=*yes*|no**
  Specifies whether the edit field supports Quick View mode.

- **readonly=yes|*no***
  Specifies whether the HTML editor is read-only. This property is ignored unless bound=no.

- **rows=1|number**

  Specifies the number of rows on the form occupied by the textbox.

- **size=*20*|*number***

  Specifies the width of the input field.

- **spellchk=yes|*no***

  Specifies whether to display a Spell button next to the field label in the edit view.

- **tenant=*value***
  Specifies the internal identification (UUID) of the tenant. This property is not intended for customer use.

- **tenantName=*value***
  Specifies the name of the tenant. This property is not intended for customer use.

- **toolbar=*default*|reportcard|tmpl**
  Specifies the set of HTML editing tools displayed in the edit field. This property has the following possible values:

  - default -- the default toolbar set
  - reportcard -- a toolbar set appropriate for the knowledge report card
  - tmpl -- a toolbar set appropriate for the document template editor

dtlLookup

The dtlLookup macro specifies a lookup control on a detail form. In the edit view, a user can click the caption (header) of the control to pop up a selection form.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **autofill=*yes*|no**

  Specifies whether the field allows autofill when it is displayed as a lookup. Autofill lets a user enter a value in the field by typing the first few characters of a value and pressing Tab. These actions cause the product to perform one of the following actions:

  - Request the full value for the field from the server.
  - Pop up a selection form when the specified value is missing or ambiguous.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **common_name_attr=*attributeName***
  Specifies the name of the attribute from the referenced table to display on the detail form. This property is not intended for customer use.

- **evt=*"eventName='script'"***

  Specifies one or more HTML event handlers in the same way you specify them in an HTML statement, with quotes escaped as required. For example:

  ```
  evt="onclick='myfunc()' onchange=\\\"myfunc2()\\\""
  ```

- **extraURL=*string***

  Specifies a where clause predicate in URL format to restrict the contents of the control.

- **factory=*name***

  Specifies the name of a Majic factory for the selection list. Defaults to the factory referenced by the associated attributes, and so is not typically required.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **link=*yes*|no**

  Specifies whether the control on the read-only view is a link to detail for the value of the attribute.

- **make_required=YES|*NO***

  Makes a field required when you specify YES regardless of whether the associated attribute is required at the object level. A required field forces the user to specify a nonblank value.

- **size=*20*|*number***

  Specifies the width of the input field.

dtlLookupReadonly

The dtlLookupReadonly macro specifies a read-only lookup control on an HTMPL detail form.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **link=*yes*|no**

Specifies whether the control on the read-only view is a link to detail for the value of the attribute.

dtlLrelMultiselbox

The dtlLrelMultiselbox macro displays a multiselect field (side-by-side selection) control for a many-to-many selection form. This macro displays a set of input controls, including the following:

- A left-side multiselect field and its header
- A right-side multiselect field and its header
- Two select buttons between the multiselect fields
- Pagination text below the multiselect fields if any
- Two Clear Selection buttons at the bottom of the multiselect fields

This macro has the following properties:

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

dtlRadio

The dtlRadio macro displays a group of option button controls with optional text following the control.

This macro has the following properties:

- **actcode=*string***
  Specifies the action code.
- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.
- **codename=*string***
  (Required) Specifies the name of a set of values from the ui_selection object that are displayed in the date drop-down list control. These values have code attributes that match the value specified for codename.
- **dataclass=*string***
  Specifies the CSS class name used for the text of the option button.
- **evt=*"eventName='script'"***

  Specifies one or more HTML event handlers in the same way you specify them in an HTML statement, with quotes escaped as required. For example:

```
evt="onclick='myfunc()' onchange=\\\"myfunc2()\\\""
```

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **title=*text***

  Specifies the title for screen reader users.

- **sameRow=true|*false***
  Specifies whether to display the option buttons on the same row.

- **title=*text***

  Specifies the title for screen reader users.

Example: dtlRadio

NX_ROOT\bopcfg\www\htmpl\web\analyst\detaikl_pri_cal.htmpl file has the following use of the macro:

<PDM_MACRO name=dtlRadio hdr="Duplicate Ticket Action" attr="action" actcode="$args.action" codename="dupActions">

dtlReadonly

The dtlReadonly macro specifies a read-only textbox on an HTMPL detail form.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **fmtfunc=*name***
  Specifies the name of a JavaScript function that formats the field for display. The function is passed a single argument containing the value of the attribute, and must return a string that is displayed on the form.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **hdrclass=*text***
  Specifies the CSS class used to format the caption. This property is not intended for customer use.

- **title=*text***

  Specifies the title for screen reader users.

- **inline=yes|*no***
  Specifies whether the header text and the data are on the same line, separated by a colon (:). Use this property only when attr="n/a".

- **value=*value***
  Specifies the value displayed on the form when attr="n/a".

dtlShowtext

The dtlShowtext macro displays plain text on the form without any label or header that is associated with the text. This macro lets you do the following activities:

- Associate the text to display with an attribute.
- Format and display the text when needed.
- Show a bar image below the text.

This macro has the following properties:

- **argumts=*string***
  Specifies the arguments that are passed to the fmtmsg format function.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **dataclass=pageHeader|hdr|required|alertmsg|className**
  Specifies the CSS class that is applied to displayed text.

- **fmtmsg=*string***
  Specifies the name of the function to format the text for display. The arguments for this function are specified in the argumts parameter. The function must return a text string that is the value displayed.

- **keeplinks=yes|*no***

  Specifies whether HTML links (Action: tags) are displayed as links or formatted as raw text. Preserves HTML links when the text to display contains HTML links. The default value is no.

- **keeptags=yes|*no***

Specifies whether HTML tags are interpreted as HTML links or formatted as raw text. keeptags=yes overrides the keeplinks property.

- **showbarimg=yes|*no***
  Specifies whether to display a bar image below the text.

- **value=*text***
  (Required) Specifies the value to display. The value can be associated to an attribute.

Example: dtlShowtext

NX_ROOT\bopcfg\www\htmpl\web\analyst\detaikl_pri_cal.htmpl file uses the following macro:

<PDM_MACRO name=dtlShowtext colspan=6 dataclass=hdr value="Priority Calculation Options">

- **Colspan**
  Specifies the number of field columns we want to span.

- **Dataclass**
  Specifies the css we want to apply for the text.

- **Value**
  Specifies the displayed text value.

dtlStart

The dtlStart macro begins a detail form, and must be the second macro on the form. Structure all detail forms with the following code:

```
<PDM_MACRO name=dtlForm . . .>
<PDM_MACRO name=dtlStart . . .>
<PDM_MACRO name=dtlStartRow . . .>
. . .
<PDM_MACRO name=dtlEnd>
```

This macro has the following properties:

- **center=true|*false***
  Specifies whether the form is centered.

- **scroll=true|*false***
  Specifies whether the form always has a scroll bar.

dtlStartDiv

The dtlStartDiv macro marks the beginning of a group of detail form macros that JavaScript can show or hide. Pair this macro with a dtlEndDiv macro. For example:

```
<PDM_MACRO name=dtlStartDiv divid="my_div". . .>
. . .
<PDM_MACRO name=dtlEndTable>
<PDM_MACRO name=dtlEndDiv>
```

This macro has the following properties:

- **align=*left*|center|right**
  Specifies the alignment of the DIV.
- **class=*className***
  Specifies the CSS class of the DIV.
- **divid=*string***
  (Required) Specifies the JavaScript identification of the DIV.
- **style=*string***
  Specifies the style of the DIV.

dtlStartExpRow

The dtlStartExpRow macro specifies the start of an expandable row on a detail form. An expandable row lets the user hide the row controls by clicking the title bar of the row.

This macro has the following properties:

- **class=*className***
  Specifies the CSS class of the HTML table containing the controls in the new row.
- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **exp_rows="1,2,..."**
  Specifies the row numbers in the expandable section as a quoted string containing a sequence of numbers from 1 to *N*. *N* represents the number of rows desired in the expandable section. The section includes the controls following dtlStartExpRow, and the next n-1 dtlStartRow macros.
- **form_name=*name***
  Specifies the name of the containing HTMPL file name without the htmpl extension. The name value is the name of the file. When the expandable section is in a tab, this argument specifies the name of the file containing the tab.
- **label=*string***
  Specifies the label shown on the expandable section bar.

dtlStartRow

The dtlStartRow macro marks the start of a row on a detail form.

This macro has the following properties:

- **class=*className***
  Specifies the CSS class of the HTML table containing the controls in the new row.

- **hrClass=*className***
  Specifies the CSS class of an optional dividing line. This property is effective only when hrSpan specifies a nonzero value.

- **hrSpan=*0*|*number***
  Specifies the number of columns spanned by an optional dividing line above the new row. The default value of zero specifies no dividing line.

dtlSurvey

The dtlSurvey macro displays multiple choice answers for each survey question. Survey questions can accept single answers for which option buttons are displayed or can accept multiple answers for which check boxes are displayed. You can use this macro in survey forms like preview risk survey, submit risk survey, and view submitted survey.

This macro has the following properties:

- **answerselected=*number***
  Specifies the index of the selected answer.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **factory=*name***
  Specifies the factory containing the survey, usually risk_svy_atpl.

- **parentid=*number***
  Specifies the database id of the question, usually $question.id.

- **parentmultiflag=*number***
  Specifies whether to display a check box or a option button. This value is usually $question. mult_resp_flag.

- **parentsequence=*number***
  Specifies the question sequence. This value is usually $question.sequence.

- **view=*preview*|doview|viewsubmitted**
  Specifies the survey view to display. You can specify any of the following views:

  - preview -- specifies to display preview survey page

  - doview -- specifies to display survey page which is ready to be submitted

  - viewsubmitted -- specifies to display the previously submitted survey page

dtlTextbox

The dtlTextbox macro specifies a text field on a detail form. In the edit view, the field allows entry of free-form text.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **disp_entities=yes|*no***
  Specifies whether to display HTML entities (for example, & or &#26237) in read-only view. If disp_entities=no, HTML entities are displayed exactly as entered; if disp_entities=yes, HTML entities are converted to their external value.

- **evt=*"eventName='script'"***

  Specifies one or more HTML event handlers in the same way you specify them in an HTML statement, with quotes escaped as required. For example:

  ```
  evt="onclick='myfunc()' onchange=\\\"myfunc2()\\\""
  ```

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **title=*text***

  Specifies the title for screen reader users.

- **JSButton=function()**
  Specifies a JavaScript function that creates a button next to the header of the control.

- **keeplinks=yes|*no***

  Specifies whether HTML links (Action: tags) are displayed as links or formatted as raw text. Preserves HTML links when the text to display contains HTML links. The default value is no.

- **keeptags=yes|*no***

  Specifies whether HTML tags are interpreted as HTML links or formatted as raw text. keeptags=yes overrides the keeplinks property.

- **make_required=YES|*NO***

Makes a field required when you specify YES regardless of whether the associated attribute is required at the object level. A required field forces the user to specify a nonblank value.

- **maxlength=*number***

  Specifies the maximum length of the edit field.

- **password=yes|*no***
  Specifies whether the text field contains a password field. CA SDM replaces passwords with a string of asterisks in both the edit and read-only views.

- **rows=1|number**

  Specifies the number of rows on the form occupied by the textbox.

- **size=*20*|*number***

  Specifies the width of the input field.

- **spellchk=yes|*no***

  Specifies whether to display a Spell button next to the field label in the edit view.

- **srchknow=yes|*no***
  Specifies whether to display a search knowledge button next to the field label.

- **title=*text***

  Specifies the title for screen reader users.

- **value=*text***
  Specifies the value to display when the value cannot be retrieved from the attribute.

dtlWriteproperty

The dtlWriteproperty macro specifies a custom property for a change or issue category, or a request, incident, or problem area. Properties appear on the properties tab of the respective tickets. This macro formats a single property with the label on the left, input field value in the middle, and a sample value on the right. The Input field can be a textbox, drop-down list, or a check box.

This macro has the following properties:

- **label=prop*n*.label**
  Specifies a label for the property, in the form propn.label. n is the property number specified in the propNum argument.

- **make_required=YES|*NO***

  Makes a field required when you specify YES regardless of whether the associated attribute is required at the object level. A required field forces the user to specify a nonblank value.

- **propNum**
  (Required) Specifies a number for the property. Properties are displayed in sequence by property number.

- **sample=prop*n*.sample**
  Specifies an example of a value for the property, in the form propn.sample. n is the property number specified in the propNum argument.

- **validation_rule=prop*n*.validation_rule.id**
  Specifies the validation rule for the property, in the form propn.validation_rule.id. n is the property number specified in the propNum argument.

- **validation_type=prop*n*.validation_type**
  Specifies the validation type for the property, in the form propn.validation_type. n is the property number specified in the propNum argument.

- **value=prop*n*.sample**
  Specifies the value of the property. n is the property number specified in the propNum argument.

ebr_search_filter

The ebr_search_filter macro specifies an Advanced filter for a related knowledge search. This macro is not intended for customer use.

This macro has the following properties:

- **factory=*name***

  Specifies the name of a Majic factory for the selection list. Defaults to the factory referenced by the associated attributes, and so is not typically required.

- **order_by=*true*|false**
  Specifies whether the filter should include an Order by combo box.

- **view=Architect|*Generic*|Knowledge**
  Specifies whether the filter should be displayed in a Knowledge tab, an Architect tab, or generically (any tab except Knowledge or Architect).

elsEditField

The elsEditField macro specifies an editable field for the Edit in List feature of a list form. You specify that a list form has the Edit in List feature by including the elsStartEdit and elsEndEdit macros. You define the fields on the Edit in List form with one or more elsEditField and elsEditReadOnly macros. For example:

```
<PDM_MACRO name=elsStartEdit search_filter="__search_filter">
```

```
<PDM_MACRO name=elsEditField . . .>
<PDM_MACRO name=elsEditField . . .>
<PDM_MACRO name=elsEditReadonly . . .>
. . .
<PDM_MACRO name=elseEndEdit>
```

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **datatype=0**
  Specifies the data type for input validation. The only datatype supported is 0, which causes the field to be validated as an integer.

- **EndRow=yes|*no***

  Specifies whether the field is the last one in a row on the Edit in List form. Specifying EndRow=yes causes CA SDM to display the next field on a new line of the form.

- **extraEvt=function()**
  Specifies a JavaScript function that is called as an onchange event handler when a user modifies the field.

- **extraURL=*string***

  Specifies a where clause predicate in URL format to restrict the contents of the control.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **size=*20*|*number***

  Specifies the width of the input field.

- **StartRow=yes|*no***

  Specifies whether the field starts a new row on the Edit in List form.

elsEditReadonly

The elsEditReadonly macro specifies a read-only field for the Edit in List feature of a list form. You specify that a list form has the Edit in List feature by including the elsStartEdit and elsEndEdit macros. You define the fields on the Edit in List form with one or more elsEditField and elsEditReadOnly macros. For example:

```
<PDM_MACRO name=elsStartEdit search_filter="__search_filter">
<PDM_MACRO name=elsEditField . . .>
<PDM_MACRO name=elsEditField . . .>
<PDM_MACRO name=elsEditReadonly . . .>
. . .
<PDM_MACRO name=elseEndEdit>
```

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **EndRow=yes|*no***

  Specifies whether the field is the last one in a row on the Edit in List form. Specifying EndRow=yes causes CA SDM to display the next field on a new line of the form.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **size=*20*|*number***

  Specifies the width of the input field.

- **StartRow=yes|*no***

  Specifies whether the field starts a new row on the Edit in List form.

elsEndEdit

The elsEndEdit macro marks the end of the fields specified for the Edit in List feature of a list form. You specify that a list form has the Edit in List feature by including the elsStartEdit and elsEndEdit macros. You define the fields on the Edit in List form with one or more elsEditField and elsEditReadOnly macros. For example:

```
<PDM_MACRO name=elsStartEdit search_filter="__search_filter">
<PDM_MACRO name=elsEditField . . .>
<PDM_MACRO name=elsEditField . . .>
<PDM_MACRO name=elsEditReadonly . . .>
. . .
<PDM_MACRO name=elseEndEdit>
```

This macro has no properties.

elsStartEdit

The elsStartEdit macro activates the Edit in List feature of a list form, and marks the start of the list of fields. You specify that a list form has the Edit in List feature by including the elsStartEdit and elsEndEdit macros. You define the fields on the Edit in List form with one or more elsEditField and elsEditReadOnly macros. For example:

```
<PDM_MACRO name=elsStartEdit search_filter="__search_filter">
<PDM_MACRO name=elsEditField . . .>
<PDM_MACRO name=elsEditField . . .>
<PDM_MACRO name=elsEditReadonly . . .>
. . .
<PDM_MACRO name=elseEndEdit>
```

This macro has the following properties:

- **search_filter="__search_filter"**
  (Required) Specifies the JavaScript object name of the search filter. Specify this property exactly as shown.

endFrameset

The endFrameset macro marks the end of a frameset definition. You define a page of the frame with the startFrameset, endFrameset, and frame macros. For example:

```
<PDM_MACRO name=startFrameset. . .>
<PDM_MACRO name=frame. . .>
<PDM_MACRO name=frame. . .>
. . .
<PDM_MACRO name=endFrameset>
```

This macro has no properties.

endMenu

The endMenu macro marks the end of a menu within a menubar definition. You define a menubar page with the startMenubar, menubarItem, endMenubar, startMenu, menuItem, menuItemLocal, and endMenu macros. For example:

```
<PDM_MACRO name=startMenubar. . .>
<PDM_MACRO name=menubarItem. . .>
<PDM_MACRO name=menubarItem. . .>
. . .
<PDM_MACRO name=endMenubar>
<PDM_MACRO name=startMenu. . .>
<PDM_MACRO name=menuItem. . .>
<PDM_MACRO name=menuItemLocal. . .>
. . .
<PDM_MACRO name=endMenu>
<PDM_MACRO name=startMenu. . .>
. . .
<PDM_MACRO name=endMenu>
. . .
```

This macro has no properties.

endMenubar

The endMenubar macro marks the end of definition of a menubar, and is followed by the definitions of the menus on the menubar. You define a menubar page with the startMenubar, menubarItem, endMenubar, startMenu, menuItem, menuItemLocal, and endMenu macros. For example:

```
<PDM_MACRO name=startMenubar. . .>
<PDM_MACRO name=menubarItem. . .>
<PDM_MACRO name=menubarItem. . .>
. . .
<PDM_MACRO name=endMenubar>
<PDM_MACRO name=startMenu. . .>
<PDM_MACRO name=menuItem. . .>
<PDM_MACRO name=menuItemLocal. . .>
. . .
<PDM_MACRO name=endMenu>
<PDM_MACRO name=startMenu. . .>
. . .
<PDM_MACRO name=endMenu>
. . .
```

This macro has no properties.

endNotebook

The endNotebook macro marks the end of the definition of a notebook on a detail page. Only one notebook can exist on a page and it must be the last item on the page. You define a notebook with the startNotebook, startTabGroup, tab, and endNotebook macros. For example:

```
<PDM_MACRO name=startNotebook. . .>
<PDM_MACRO name=startTabGroup. . .>
<PDM_MACRO name=tab . .>
<PDM_MACRO name=tab . .>
. . .
<PDM_MACRO name=startTabGroup. . .>
<PDM_MACRO name=tab . .>
. . .
<PDM_MACRO name=endNotebook>
```

This macro has no properties.

frame

The frame macro specifies a frame on a frameset page. You define a frameset page with the startFrameset, frameab, and endFrameset macros. For example:

```
<PDM_MACRO name=startFrameset. . .>
<PDM_MACRO name=frame . .>
<PDM_MACRO name=frame . .>
. . .
<PDM_MACRO name=endFrameset >
```

This macro has the following properties:

- **extra=*string***
  Specifies a string of keywords in the same way as in an HTML <frame> statement, with quotes escaped as required.

- **frame_name=*name***
  (Required) Specifies a name for the frame (the "name" argument on an HTML <frame> statement).

- **frameborder=*yes*|no**
  Specifies whether the frame has a border (the "frameborder" argument on an HTML <frame> statement).

- **id=*name***
  (Required) Specifies the JavaScript ID of the frame (the "id" argument on an HTML <frame> statement).

- **marginheight=*number***
  Specifies the size of the top and bottom margins (the "marginheight" argument on an HTML <frame> statement).

- **marginwidth=*number***
  Specifies the size of the top and bottom margins (the "marginwidth" argument on an HTML <frame> statement).

- **noresize=true|*false***
  Specifies whether the frame is resizable (the "noresize" keyword on an HTML <frame> statement).

- **scrolling=*auto*|yes|no**
  Specifies whether the frame has a scroll bar (the "scrolling" argument on an HTML <frame> statement).

- **style=*string***
  Specifies CSS style information for the frame (the "style" argument on an HTML <frame> statement).

- **tabindex=*number***
  Specifies the tab index of the frame (the "tabindex" argument on an HTML <frame> statement).

- **title=*text***

  Specifies the title for screen reader users.

- **web_form_name=*string***
  Specifies the code name of an object in the web_form factory where CA SDM can obtain the URL for the form displayed in the frame. This property is effective only when web_form_url is not specified.

- **web_form_url=*string***
  Specifies the URL of the form that displays in the frame.

kt_Categories_Tree

The kt_Categories_Tree macro creates a knowledge category frame.

This macro has the following properties:

- **frameborder=*0*|*number***
  Specifies the size of the border.

- **height=*100px*|*value***
  Specifies the frame height.

- **iframe=*yes*|no**
  Specifies whether to generate an iframe for the tree. Specify iframe=no when you are using a predefined frame.

- **menu=*name***
  Specifies the tree menu type. Specify adm_tree, DOCUMENT_EDITOR, HTML_EDITOR, ATTACHMENTS_IMAGES, ATTACHMENTS_TAB, ATTACHMENTS_ADMIN, ARCHITECT, or FAQ.

- **ParentTenant=*value***
  Specifies the parent tenant. Typically, you code this property as ParentTenant="$args. ParentTenant"

- **tabindex=*number***
  Specifies the tab index of the frame.

- **UseTenant=*0*|1**
  Specifies whether to use a tenant.

- **view=*ArchitectTree*|FAQ**
  Specifies the view: ArchitectTree or FAQ.

- **width=*100px*|*value***
  Specifies the frame width.

lsCol

The lsCol macro specifies a column on a list form. You define the contents of a list form with the lsStart, lsCol, and lsEnd macros. You can optionally include lsWrite and lsExport macros. For example:

```
<PDM_MACRO name=lsStart. . .>
<PDM_MACRO name=lsCol . .>
<PDM_MACRO name=lsCol . .>
<PDM_MACRO name=lsWrite . .>
<PDM_MACRO name=lsCol . .>
. . .
<PDM_MACRO name=lsEnd>
```

HTML for the entire list is output by the lsEnd macro. The other list macros save information used by lsEnd to generate the list.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

  Note: This property is not used and is ignored. This property is retained for compatibility with previous releases.

- **common_name_option=*yes*|no**
  Specifies whether the column contains an SREL attribute. The common name of the referenced table when the list is exported replaces the attribute value.

- **disp_entities=yes|*no***
  Specifies whether to display HTML entities (for example, & or &#26237 in read-only view. This property has the following values:

  - **YES** -- HTML entities are converted to their external value.

  - **NO** -- HTML entities are displayed exactly as entered.

- **display_attr=*COMMON_NAME*|attrName**
  Specifies the column from the referenced table that is displayed on the list for columns containing an SREL attribute. This property is ignored for columns that are not SRELs.

- **escape=*C*|HTML|JS|JS2**
  Specifies how the value of the column is escaped. This property has the following values:
  - **C** -- Prefix quotes, backslashes, and newlines with a backslash
  - **HTML** -- Convert quote, backslash, '<', and '>' to HTML entities
  - **JS** -- Convert quote, backslash, and newline to JavaScript hex (%nn)
  - **JS2** -- Same as JS, but also convert '%' to '%25'
- **export=*yes*|no**
  Specifies whether this column is exported when the user clicks the Export button.
- **export_hdr_default**
  Specifies the default header text. The list result export uses this property.
- **exportFmt=*function***
  Specifies the name of a JavaScript function (without parentheses) that returns a string format code which controls formatting the column when it is exported. This property has the following function values:
  - **"YES_NO"** -- Return either "yes" or "no"
  - **"FACTORY_LINK"** -- No formatting (reserved for future use)
  - **"LIST_LOOKUP:v1,v1a,v2,v2a,.."** -- Convert from a list. A value matching the first element in a pair is converted to the second element in the pair.
- **exportHdr=*text*|DISPLAY_NAME**
  Specifies the header for the column when it is exported. You can specify the value as explicit text, or as the keyword value DISPLAY_NAME, which sets the header to the value of export_hdr_default.
- **export_hdr_default=*text***
  Specifies the text of the export column header when exportHdr has the keyword value DISPLAY_NAME. You rarely must specify this property, which defaults to the display name of the attribute for the column.
- **fmtfunc=*function***
  Specifies the name of a JavaScript function that formats the field for display. The function is passed as a single argument containing the value of the attribute, and must return a string that is displayed on the form.
- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **hidden=yes|*no***
  Specifies whether the column is invisible. A hidden column can be useful for Edit in List or export.

- **img=*name***
  Specifies a JavaScript variable containing the URL of an image to display in the column. Set the JavaScript variable with a preceding lsWrite macro.

- **justify=*left*|center|right**
  Specifies the position of content within the columns.

- **keeplinks=yes|*no***

  Specifies whether HTML links (Action: tags) are displayed as links or formatted as raw text. Preserves HTML links when the text to display contains HTML links. The default value is no.

- **keeptags=yes|*no***

  Specifies whether HTML tags are interpreted as HTML links or formatted as raw text. keeptags=yes overrides the keeplinks property.

- **label=*string***

  Specifies text for a label positioned to the left of data.

- **link=*yes*|no**

  Specifies whether the control on the read-only view is a link to detail for the value of the attribute.

- **max_char=*0*|*number***
  Specifies the maximum number of characters to display in column.

- **nowrap=yes|*no***
  Specifies whether to suppress wrapping of text in a call. When you specify nowrap=yes, text for the column is not permitted to wrap to multiple lines.

- **required=yes|*no***
  Specifies whether text must appear in the column. When you specify required=yes and the attribute has no value, its value is replaced with "Not Available."

- **sort=*ASC*|DESC|no**
  Specifies the sort sequence of the list when a user clicks the column as follows:

  - ASC (ascending)
  - DESC (descending)
  - no (column is not a sort column)

- **startrow=yes|*no***
  Specifies whether the column is the first one in the expansion section. This property works as follows:

- Columns defined by lsCol macros prior to one specifying startrow=yes are displayed on the main portion of the list.
- Columns defined by the lsCol macro specifying startrow=yes are included in the expansion section that is hidden from view unless the user clicks the plus sign at the beginning of the list row.
- The startrow property is effective only for the first lsCol macro specifying startcol=yes; it is ignored on subsequent lsCol macros.

- **style=*string***
  Specifies CSS formatting for the column.
- **uid=*string***
  Specifies an additional identifier to distinguish between columns with the same attribute. This property is not intended for customer use.
- **width=*0*|*number***
  Specifies the maximum width of a column.

lsEnd

The lsEnd macro marks the end of a list form specification. You define the contents of a list form with the lsStart, lsCol, and lsEnd macros. You can optionally include lsWrite and lsExport macros. For example:

```
<PDM_MACRO name=lsStart. . .>
<PDM_MACRO name=lsCol . .>
<PDM_MACRO name=lsCol . .>
<PDM_MACRO name=lsWrite . .>
<PDM_MACRO name=lsCol . .>
. . .
<PDM_MACRO name=lsEnd>
```

HTML for the entire list is output by the lsEnd macro. The other list macros save information used by lsEnd to generate the list.

This macro has the following properties:

- **alt_data_src=*name***
  Specifies the name of a JavaScript variable containing the contents of the list. This property is used to display data from a source other than the database. For example:

```
var alternative_source = new Array();

var row1 = new Object();

row1. column0 = "column0";

row1. column1 = 4;

alternative_source[0] = row1;

......

<PDM_MACRO name=lsEnd alt_data_src=alternative_source>
```

- **factory=*name***

  Specifies the name of a Majic factory for the selection list. Defaults to the factory referenced by the associated attributes, and so is not typically required.

- **isTicketFactory=*0*|1**
  Specifies a list of tickets (requests, incidents, problems, changes, or issues).

- **list=*name***
  Specifies the source variable of a database list. This property is not intended for customer use.

- **sort=*attributeName***
  Specifies the initial sort sequence of the list.

- **start=*number***
  Specifies the ordinal number of the first row of the list to display. This property is not intended for customer use.

lsExport

Use the lsExport macro in place of lsCol to specify a column for a list form that is not included in the web UI list. However, this column is included in the spreadsheet generated by exporting the list. You define the contents of a list form with the lsStart, lsCol, and lsEnd macros. You can optionally include lsWrite and lsExport macros. For example:

```
<PDM_MACRO name=lsStart. . .>
<PDM_MACRO name=lsCol . .>
<PDM_MACRO name=lsCol . .>
<PDM_MACRO name=lsWrite . .>
<PDM_MACRO name=lsCol . .>
. . .
<PDM_MACRO name=lsEnd>
```

HTML for the entire list is output by the lsEnd macro. The other list macros save information used by lsEnd to generate the list.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **common_name_option=*yes*|no**
  Specifies whether the column contains an SREL attribute. The common name of the referenced table replaces this attribute value when the list is exported.

- **export=*yes*|no**
  Specifies whether this column is exported when the user clicks the Export button.

- **export_hdr_default**
  Specifies the text of the header.

- **exportFmt=*function***
  Specifies the name of a JavaScript function (without parentheses) that returns a string format code used to control formatting the column when it is exported. The function can return the following values:

  - "YES_NO" -- Return either "yes" or "no"
  - "FACTORY_LINK" -- No formatting (reserved for future use)
  - "LIST_LOOKUP:v1,v1a,v2,v2a,.." -- Convert from a list. A value matching the first element in a pair is converted to the second element in the pair.

- **exportHdr=*text*|DISPLAY_NAME**
  Specifies the header for the column when it is exported. You can specify the value as explicit text, or as the keyword value DISPLAY_NAME, which sets the header to the value of export_hdr_default.

- **export_hdr_default=*text***
  Specifies the text of the export column header when exportHdr has the keyword value DISPLAY_NAME. You rarely must specify this property, which defaults to the display name of the attribute of the column.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **label=*string***

  Specifies text for a label positioned to the left of data.

lsStart

The lsStart macro marks the beginning of a list form specification. You define the contents of a list form with the lsStart, lsCol, and lsEnd macros, and can optionally include lsWrite and lsExport macros. For example:

```
<PDM_MACRO name=lsStart. . .>
<PDM_MACRO name=lsCol . .>
<PDM_MACRO name=lsCol . .>
<PDM_MACRO name=lsWrite . .>
<PDM_MACRO name=lsCol . .>
. . .
<PDM_MACRO name=lsEnd>
```

HTML for the entire list is output by the lsEnd macro. The other list macros save information used by lsEnd to generate the list.

This macro has the following properties:

- **search_type=*DISPLAY*|GET_DOB**
  Specifies how data for the list is retrieved. The default of DISPLAY causes all data to be retrieved directly from the database. The alternate value of GET_DOB causes data to be formatted by the object engine (domsrvr), and may be required if the list includes local attributes not stored in the database. A specification of search_type=GET_DOB reduces the performance of the list form, and only use it when necessary.

lsWrite

The lsWrite macro specifies JavaScript code executed for every row of a list. The text specified by lsWrite is inserted into the HTML form multiple times, once for each row of the list. You define the contents of a list form with the lsStart, lsCol, and lsEnd macros. You can optionally include lsWrite and lsExport macros. For example:

```
<PDM_MACRO name=lsStart. . .>
<PDM_MACRO name=lsCol . .>
<PDM_MACRO name=lsCol . .>
<PDM_MACRO name=lsWrite . .>
<PDM_MACRO name=lsCol . .>
. . .
<PDM_MACRO name=lsEnd>
```

HTML for the entire list is output by the lsEnd macro. The other list macros save information used by lsEnd to generate the list.

This macro has the following properties:

- **both=yes|*no***
  Specifies whether the JavaScript text defined by the macro is inserted before the list and for every row on the list.

- **text=*script***
  Specifies the text to insert.

menubarItem

The menubarItem macro defines an item on a menubar. You define a menubar page with the startMenubar, menubarItem, endMenubar, startMenu, menuItem, menuItemLocal, and endMenu macros. For example:

```
<PDM_MACRO name=startMenubar. . .>
<PDM_MACRO name=menubarItem. . .>
<PDM_MACRO name=menubarItem. . .>
. . .
<PDM_MACRO name=endMenubar>
<PDM_MACRO name=startMenu. . .>
<PDM_MACRO name=menuItem. . .>
<PDM_MACRO name=menuItemLocal. . .>
. . .
<PDM_MACRO name=endMenu>
<PDM_MACRO name=startMenu. . .>
. . .
```

```
<PDM_MACRO name=endMenu>
. . .
```

This macro has the following properties:

- **hotkey=*string***

  Provides a hotkey suggestion for this menubar item. CA SDM selects the hotkey for the menubar item from the characters in the string; otherwise, it selects the hotkey from the characters in the label.

- **id=*name***
  (Required) Specifies a JavaScript identifier for the menubar item.

  Note: The startMenu macro references this identifier. The startMenu macro defines the contents of the menu dropped down from the menubar for this item.

- **img=*url***
  Specifies the URL of an image to display on the toolbar section of the menubar.

- **label=*text***
  (Required) Specifies the text of the menu bar item.

- **variable=*name***
  Specifies a JavaScript variable that can be used to reference the menubar item. This property is not intended for customer use.

menuItem

The menubarItem macro defines an item on a menu. The item invokes a JavaScript function in the main CA SDM form, even if the menu is in a pop-up form. Use the menuitemLocal macro to invoke a local function. You define a menubar page with the startMenubar, menubarItem, endMenubar, startMenu, menuItem, menuItemLocal, and endMenu macros. For example:

```
<PDM_MACRO name=startMenubar. . .>
<PDM_MACRO name=menubarItem. . .>
<PDM_MACRO name=menubarItem. . .>
. . .
<PDM_MACRO name=endMenubar>
<PDM_MACRO name=startMenu. . .>
<PDM_MACRO name=menuItem. . .>
<PDM_MACRO name=menuItemLocal. . .>
. . .
<PDM_MACRO name=endMenu>
<PDM_MACRO name=startMenu. . .>
. . .
<PDM_MACRO name=endMenu>
. . .
```

This macro has the following properties:

- **extended=*0*|1**
  Specifies whether this item is an extended menu item supporting disabling, hiding, and changing an image.

- **function=*script***
  (Required) Specifies the JavaScript function invoked when the menu item is selected. This function must be available in the main CA SDM form, and not in the pop-up form containing the menu. Menu items invoking functions in the pop-up form should be defined with the menuitemLocal macro.

- **hotkey=*string***

  Provides a hotkey suggestion for this menubar item. CA SDM selects the hotkey for the menubar item from the characters in the string; otherwise, it selects the hotkey from the characters in the label.

- **icon_name=*string***
  Specifies the name of an image file displayed as an icon on the menu next to the menu item.

- **id=*name***
  Specifies a JavaScript ID for the menu item.

- **label=*text***
  (Required) Specifies the text of the menu item.

- **local=*0*|1**
  Specifies whether extended menus use the function in the local frame. This property is not intended for customer use.

- **tooltip=*string***
  Specifies a tooltip for the icon.

menuItemLocal

The menuItemLocal macro defines an item on a menu that invokes a JavaScript function in the form containing the menu. You define a menubar page with the startMenubar, menubarItem, endMenubar, startMenu, menuItem, menuItemLocal, and endMenu macros. For example:

```
<PDM_MACRO name=startMenubar. . .>
<PDM_MACRO name=menubarItem. . .>
<PDM_MACRO name=menubarItem. . .>
. . .
<PDM_MACRO name=endMenubar>
<PDM_MACRO name=startMenu. . .>
<PDM_MACRO name=menuItem. . .>
<PDM_MACRO name=menuItemLocal. . .>
. . .
<PDM_MACRO name=endMenu>
<PDM_MACRO name=startMenu. . .>
. . .
<PDM_MACRO name=endMenu>
. . .
```

This macro has the following properties:

- **function=*script***
  (Required) Specifies the JavaScript function invoked when the menu item is selected. This function must be available in the form containing the menu.

- **hotkey=*string***

  Provides a hotkey suggestion for this menubar item. CA SDM selects the hotkey for the menubar item from the characters in the string; otherwise, it selects the hotkey from the characters in the label.

- **icon_name=*string***
  Specifies the name of an image file displayed as an icon on the menu next to the menu item.

- **id=*name***
  Specifies a JavaScript ID for the menu item.

- **label=*text***
  (Required) Specifies the text of the menu item.

- **tooltip=*string***
  Specifies a tooltip for the icon.

priMatrix

The priMatrix macro specifies a priority calculation matrix.

This macro has the following properties:

- **impact_label=*name***
  Specifies an impact label.

- **matrix_name=*name***
  (Required) Specifies the name of this matrix.

- **reset_btn_name=*name***
  Specifies a reset button name.

- **urgency_label=*name***
  Specifies an urgency label.

schedAttr

The schedAttr macro specifies an attribute included on a schedule form, either the change schedule (list_chgsched_config.htmpl) or the knowledge schedule (list_kdsched_config.htmpl). You define a schedule form with the schedConfig, schedAttr, and schedGroup macros. For example:

```
<PDM_MACRO name=schedConfig. . .>
<PDM_MACRO name=schedAttr . .>
<PDM_MACRO name=schedAttr . .>
. . .
```

```
<PDM_MACRO name=schedGroup . .>
<PDM_MACRO name=schedGroup . .>
. . .
```

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **attrRef=*.COMMON_NAME*|attributeName**
  Specifies the attribute in the table referenced by an SREL attribute that should be shown on the schedule.

- **detail=0|*1***
  Specifies whether to include the attribute in the detailed n-day view.

- **fmtfunc=*none*|function**
  Specifies the name of a JavaScript function that formats the field for display. The function is passed a single argument containing the value of the attribute, and must return a string that is displayed on the form.

- **hoverInfo=*0*|1**
  Specifies whether to include the attribute in the monthly view info pop-up.

- **ident=*0*|1**
  Specifies whether to include the group name on the n-day view.

- **label=0|string|*$args.&{attr].DISPLAY_NAME***
  Specifies a label for the attribute. A value of zero signifies no label; the default is the display name of the attribute.

- **summary=*0*|1**
  Specifies whether to include the attribute in the summary n-day view.

schedConfig

The schedConfig macro controls the appearance and contents of a schedule form, either the change schedule (list_chgsched_config.htmpl) or the knowledge schedule (list_kdsched_config.htmpl). You define a schedule form with the schedConfig, schedAttr, and schedGroup macrosle. For example:

```
<PDM_MACRO name=schedConfig. . .>
<PDM_MACRO name=schedAttr . .>
<PDM_MACRO name=schedAttr . .>
. . .
<PDM_MACRO name=schedGroup . .>
<PDM_MACRO name=schedGroup . .>
. . .
```

This macro has the following properties:

- **autoSearch=0|1**
  Specifies whether to reissue a search automatically if necessary.

- **defaultView=0|1|7|*30*|99**
  Specifies the initial view as 1 (day), 7 (week), 30 (month), 99 (*n*day), or 0 (list).

- **export=0|*codename***
  Specifies the iCalendar export template code (0=no export).

- **firstday=*0*|1|2|3|4|5|6**
  Specifies the first weekday from 0 (Sunday) to 6 (Saturday).

- **hoverMax=*35*|number**
  Specifies the maximum number of rows in a hover information pop-up.

- **legend=0|*1*|2**
  Specifies the position of a legend (1=top, 2=bottom, 0=none).

- **maxgroups=*4*|*number***
  Specifies the maximum number of groups per cell in month view.

- **ndays=0|(*3,7,14,28*)|(*n1,n2,..*)**
  Specifies the contents the n-days drop-down list as a comma-separated list of numbers. A value of 0 signifies no n-days drop-down list.

- **round=0|(*0,15*)|(*hh,mm*)**
  Specifies event times in hours and minutes enclosed in parentheses. The default of (0,15) specifies rounding to the nearest 15 minutes. A value of 0 signifies no rounding.

- **timefmt=*24hr*|(*am,pm*)**
  Specifies time format as either 12 or 24 hour. You specify the 12-hour value as two comma-separated strings, the first for am and the second for pm.

- **tzSelect=*string***
  Specifies where clause restrictions on the time zone drop-down list.

schedGroup

The schedGroup macro controls the name and styling of groups of items on a schedule form, either the change schedule (list_chgsched_config.htmpl), or the knowledge schedule (list_kdsched_config.htmpl). You define a schedule form with the schedConfig, schedAttr, and schedGroup macrosle. For example:

```
<PDM_MACRO name=schedConfig. . .>
<PDM_MACRO name=schedAttr . .>
<PDM_MACRO name=schedAttr . .>
. . .
<PDM_MACRO name=schedGroup . .>
<PDM_MACRO name=schedGroup . .>
. . .
```

This macro has the following properties:

- **bgcolor=*white*|color**
  Specifies the background color for the group as any valid web color.

- **color=*black*|color**
  Specifies the foreground (text) color for the group as any valid web color.

- **grpname=*name***
  (Required) Specifies the name of the group.

- **icon=*filename***
  Specifies an icon for the group as the name of a file in $NX_ROOT/bopcfg/www/wwwroot/img.

- **label=*string***
  Specifies a label for the group.

- **legend=0|*string***
  Specifies description of the group for the legend. A value of 0 signifies that group is not in the legend.

- **style=*normal*|bold|italic**
  Specifies the text style for the group.

sfDate

The sfDate macro specifies a date control in the search filter of a list form.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

  colspan=*1*|*number*

  Specifies the number of columns on the form.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **qbe_condition=*condition***

  Specifies one of the following conditions for comparing the value in this field to the database value:

  - EQ is equal to the value.
  - NE is not equal to the value.
  - GT is greater than the value.
  - LT is less than the value.
  - GE is greater than or equal to the value.

- LE is less than or equal to the value.
- NU is null
- NN is not null.
- IN matches the SQL LIKE expression.
- KY contains the text entered.

sfDropdown

The sfDropdown macro specifies a drop-down selection control in the search filter of a list form.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **codename=*string***

  Specifies the name of a set of values from the ui_selection object that are displayed in the date drop-down control. The values are those values with code attributes that match the value specified for codename.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **default=*text***

  Specifies the default value when the attribute is null.

- **factory=*name***

  Specifies the name of a Majic factory for the selection list. Defaults to the factory referenced by the associated attributes, and so is not typically required.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **lookup=*yes*|no**
  Specifies whether the field should automatically convert to a lookup when the number of entries in the drop-down list exceeds a configured value (typically 10).

- **Noempty=yes|*no***
  Specifies whether the empty value is included in the drop-down list. Specify Noempty=yes to suppress the empty value.

- **op=QBE.op**
  Specifies one of the following conditions for comparing the value in this field to the database value:

  - EQ is equal to the value.
  - NE is not equal to the value.
  - GT is greater than the value.
  - LT is less than the value.
  - GE is greater than or equal to the value.
  - LE is less than or equal to the value.
  - NU is null
  - NN is not null.
  - IN matches the SQL LIKE expression.
  - KY contains the text entered.

- **win=*windowName***
  Specifies the target window. This property is not intended for customer use.

sfEnd

The sfEnd macro marks the end of the definition of a search filter on a list page. You define a search filter with the sfStart, sfEnd, and other sfxxx macros. For example:

```
<PDM_MACRO name=ssfStart. . .>
<PDM_MACRO name=sfxxx. . .>
<PDM_MACRO name=sfxxx. . .>
. . .
<PDM_MACRO name=sfEnd>
```

The macro has no properties.

sfHier

The sfHier macro specifies a hierarchical lookup control in the search filter of a list form. A hierarchical lookup control allows a user to click the caption (header) of the control to pop up a hierarchical selection form.

This macro has the following properties:

- **addPercent=yes|no**

Specifies whether to allow wildcard character searches. This property defaults to the value of the web_wildcard_search option.

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **factory=*name***

  Specifies the name of a Majic factory for the selection list. Defaults to the factory referenced by the associated attributes, and so is not typically required.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

sfLookup

The sfLookup macro specifies a lookup control in the search filter of a list form. A lookup control allows a user to click the caption (header) of the control to pop up a selection form.

This macro has the following properties:

- **addPercent=yes|no**

  Specifies whether to allow wildcard character searches. This property defaults to the value of the web_wildcard_search option.

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **extraURL=*string***

  Specifies a where clause predicate in URL format to restrict the contents of the control.

- **factory=*name***

Specifies the name of a Majic factory for the selection list. Defaults to the factory referenced by the associated attributes, and so is not typically required.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

sfMultiLookup

The sfMultiLookup macro specifies a multi-value lookup control in the search filter of a list form. A multi-value lookup control allows a user to selection one or more values for the attribute associated with the control.

This macro has the following properties:

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **factory=*name***

  Specifies the name of a Majic factory for the selection list. Defaults to the factory referenced by the associated attributes, and so is not typically required.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **size=*20*|*number***

  Specifies the width of the input field.

sfStart

The sfStart macro marks the beginning of the definition of a search filter on a list page. You define a search filter with the sfStart, sfEnd, and other sfxxx macros. For example:

```
<PDM_MACRO name=ssfStart. . .>
<PDM_MACRO name=sfxxx. . .>
<PDM_MACRO name=sfxxx. . .>
. . .
```

```
<PDM_MACRO name=sfEnd>
```

This macro has the following properties:

- **button=*true*|false**
  Specifies whether to show the default search filter buttons: Search, Show Filter, Clear Filter, and Create New.

- **color=*string***
  This property is not used in this release (reserved for future use).

- **create=*true*|false**
  Specifies whether to show the Create New button.

- **export=*yes*|no**
  Specifies whether to show the Export button.

- **extraCreateURL=*string***
  Specifies additional arguments for the URL used to create an object.

- **factory=*name***

  Specifies the name of a Majic factory for the selection list. Defaults to the factory referenced by the associated attributes, and so is not typically required.

- **ForceSearchWithKeywords=true|*false***
  Specifies whether to request a nonempty search text. This property is effective only when KnowledgeSearchText is true.

- **KnowledgeSearchText=true|*false***
  Specifies whether to show the knowledge search text at the top of the filter.

sfStartRow

The sfStartRow macro marks the start of a row on a search filter.

This macro has the following properties:

- **type=Set**
  Specifies that the new row begins a row set that is hidden from view until the user clicks the green filter icon at the end of the previous row.

sfTextbox

The sfTextbox macro specifies a textbox in a search filter.

This macro has the following properties:

- **addPercent=yes|no**

  Specifies whether to allow wildcard character searches. This property defaults to the value of the web_wildcard_search option.

- **attr=*attributeName***

  (Required) Specifies the name of the attribute associated with the control.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **disabled=yes|*no***
  Specifies whether the textbox is disabled for input. If you disable the textbox, you must also specify the value, display_value, and qbe_condition properties.

- **display_value=*text***
  Specifies the human-readable value of a disabled textbox. This property is effective only when disabled=yes.

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **qbe_condition=*condition***

  Specifies one of the following conditions for comparing the value in this field to the database value:

  - EQ is equal to the value.
  - NE is not equal to the value.
  - GT is greater than the value.
  - LT is less than the value.
  - GE is greater than or equal to the value.
  - LE is less than or equal to the value.
  - NU is null
  - NN is not null.
  - IN matches the SQL LIKE expression.
  - KY contains the text entered.

- **size=*20*|*number***

  Specifies the width of the input field.

- **value=*string***
  Specifies the value of a disabled textbox used in the search. This property is effective only when disabled=yes.

startFrameset

The startFrameset macro marks the beginning of a frameset definition. You define a frame page with the startFrameset, endFrameset, and frame macros. For example:

```
<PDM_MACRO name=startFrameset. . .>
<PDM_MACRO name=frame. . .>
<PDM_MACRO name=frame. . .>
. . .
<PDM_MACRO name=endFrameset
```

This macro has the following properties:

- **border**
  Specifies the space between the frames.
- **cols**
  Specifies the quantity and sizes of the columns in the frame set.
- **frameborder=*yes*|no**
  Specifies whether the frame has a border (the "frameborder" argument on an HTML <frame> statement).
- **id=*name***
  (Required) Specifies the JavaScript ID of the frame (the "id" argument on an HTML <frame> statement).
- **onload**
  Specifies the onLoad handler of the frame set.
- **onunload**
  Specifies the onUnload handler of the frame set.
- **rows**
  Specifies the quantity and sizes of the rows in the frame set.

startMenu

The startMenu macro marks the beginning of a menu within a menubar definition. You define a menubar page with the startMenubar, menubarItem, endMenubar, startMenu, menuItem, menuItemLocal, and endMenu macros. For example:

```
<PDM_MACRO name=startMenubar. . .>
<PDM_MACRO name=menubarItem. . .>
<PDM_MACRO name=menubarItem. . .>
. . .
<PDM_MACRO name=endMenubar>
<PDM_MACRO name=startMenu. . .>
```

```
<PDM_MACRO name=menuItem. . .>
<PDM_MACRO name=menuItemLocal. . .>
. . .
<PDM_MACRO name=endMenu>
<PDM_MACRO name=startMenu. . .>
. . .
<PDM_MACRO name=endMenu>
. . .
```

This macro has the following properties:

- **parentid=*name***
  (Required) Specifies the ID of the menubarItem macro specifying this menu.

startMenubar

The startMenubar macro marks the beginning of a menubar definition. You define a menubar page with the startMenubar, menubarItem, endMenubar, startMenu, menuItem, menuItemLocal, and endMenu macros. For example:

```
<PDM_MACRO name=startMenubar. . .>
<PDM_MACRO name=menubarItem. . .>
<PDM_MACRO name=menubarItem. . .>
. . .
<PDM_MACRO name=endMenubar>
<PDM_MACRO name=startMenu. . .>
<PDM_MACRO name=menuItem. . .>
<PDM_MACRO name=menuItemLocal. . .>
. . .
<PDM_MACRO name=endMenu>
<PDM_MACRO name=startMenu. . .>
. . .
<PDM_MACRO name=endMenu>
. . .
```

This macro has no properties.

startNotebook

The startNotebook macro marks the beginning of the definition of a notebook on a detail page. A page can only have one notebook and it must be the last item on the page. You define a notebook with the startNotebook, startTabGroup, tab, and endNotebook macros. For example:

```
<PDM_MACRO name=startNotebook. . .>
<PDM_MACRO name=startTabGroup. . .>
<PDM_MACRO name=tab . .>
<PDM_MACRO name=tab . .>
. . .
<PDM_MACRO name=startTabGroup. . .>
<PDM_MACRO name=tab . .>
. . .
<PDM_MACRO name=endNotebook>
```

This macro has the following properties:

- **hdr=*text***

  Specifies the text of the caption on the control; defaults to the DISPLAY_NAME of the attribute associated with the control.

- **ilayer_height=*number***
  This property is deprecated; not used in this release.

- **nb_height=*number***
  Specifies the height of the notebook in pixels.

startTabGroup

The startTabGroup macro specifies the beginning of a group of tabs in a notebook on a detail page. This macro indicates that the notebook is organized in tab groups. A notebook with tab groups shows the groups as the highest level of tab. Tabs following the group are visible only when the group is selected.

You define a notebook with the startNotebook, startTabGroup, tab, and endNotebook macros. For example:

```
<PDM_MACRO name=startNotebook. . .>
<PDM_MACRO name=startTabGroup. . .>
<PDM_MACRO name=tab . .>
<PDM_MACRO name=tab . .>
. . .
<PDM_MACRO name=startTabGroup. . .>
<PDM_MACRO name=tab . .>
. . .
<PDM_MACRO name=endNotebook>.
```

This macro has the following properties:

- **title=*string***
  Specifies the name of the tab group that is shown at the top of the notebook. If you omit this property, CA SDM creates the name of the tab group by concatenating the names of all the tabs within the group.

tab

The tab macro specifies a tab in a notebook on a detail page. You define a notebook with the startNotebook, startTabGroup, tab, and endNotebook macros. For example:

```
<PDM_MACRO name=startNotebook. . .>
<PDM_MACRO name=startTabGroup. . .>
<PDM_MACRO name=tab . .>
<PDM_MACRO name=tab . .>
. . .
<PDM_MACRO name=startTabGroup. . .>
<PDM_MACRO name=tab . .>
```

```
. . .
<PDM_MACRO name=endNotebook>
```

This macro has the following properties:

- **accordion_specific_tab=true**
  Specifies that this macro defines an CA SDM Release 12.9 notebook. If present, you must specify this property exactly as shown.

- **file=*filename*.htmpl**
  Specifies an immediate tab. The contents of an immediate tab are part of the form containing it, and are formatted at the same time the containing form is formatted. This property specifies the HTMPL file containing its contents. CA SDM looks for a <PDM_FORM> tag in the referenced file, and includes the contents of this form as the contents of the tab. This property is mutually exclusive with the src property.

- **filename=*string***
  Specifies the value of the $prop.filename server variable that is passed to the tab contents. This property has no relationship to the similarly named file property.

- **height=*number***
  Specifies the height of this tab.

- **id=*string***
  Specifies the JavaScript identification of this tab.

- **new_row=yes|*no***
  (Deprecated) Indicates that the tab starts a new row of tabs. This property is informational only and CA SDM ignores it. The startTabGroup macro handles the grouping of tabs into rows.

- **src=*url***
  Specifies that this tab is a deferred tab. The contents of a deferred tab are independent of the main form and are loaded only when the user selects the tab. This property specifies the URL invoked to load the content of the tab. This property is mutually exclusive with the file property.

- **title=*string***
  Names the tab on the notebook.

- **tooltip=*string***
  Specifies a tooltip for a tab on the notebook.

tabBanner

The tabBanner macro specifies a banner (header) within a tab. You can only use this macro within an immediate tab loaded by the file property of the tab macro. The banner can contain text and one or more buttons.

This macro has the following properties:

- **add_btns=true|*false***
  Specifies whether the tab banner contains buttons. When this property is true, the containing form must include a JavaScript that defines the buttons. The btnfunc property specifies the name of the function and defaults to add_button_to_tab_banner().

- **btnfunc=*add_button_to_tab_banner*|*functionName***
  Specifies the name of the function that creates the buttons in the banner when add_btns=true.

- **btns_in_two_rows=*true*|false**
  Specifies whether to include an additional line in the banner for scrolling in the Internet Explorer browser.

- **show_bar=*true*|false**
  Specifies whether to display a horizontal bar below the tab banner.

- **title=*string***
  The text displayed in the tab banner. The string can be an empty string.

tabList

The tabList macro specifies a list included within an immediate tab loaded by the file property of the tab macro.

This macro has the following properties:

- **brBefore=yes|*no***
  Specifies whether to insert a line break before the list for spacing.

- **btnTitle=*string***
  Specifies a title for the Load button displayed when the Screen Reader preference is active.

- **colspan=*1*|*number***

  Specifies the number of columns on the form.

- **frmName=*string***
  Specifies a JavaScript identification of the HTML iframe that contains the list.

- **height=*number***
  Specifies the height of the generated list.

- **src=*url***
  (Required) Specifies the URL to invoke to generate the list.

Security and Role Management

This article contains the following topics:

Set up security and role management for user authentication, user access level, and the mode of authentication while logging in.

Access Types

Access types define contact roles, contacts authentication, and whether the contacts can modify web forms or the database schema.

Modify the predefined access types and create new ones.

Assign Access Type Using LDAP Groups

Assign AccessTypesvaluestocontactsautomatically with a Lightweight Directory Access Protocol (LDAP) server.

Note: To enable this feature, install the ldap_enable_group and ldap_group_object_class options.

Follow these steps:

1. Select Security and Role Management, Access Types on the Administrator tab.
2. Select the Access Type you want to associate with an LDAP Group. For example, select Administration.
   If the ldap_enable_group option is installed, the LDAP Access Group field appears on the Web Authentication tab.

   Note: If an LDAP Group is already associated with the selected Access Type, a link to the LDAP Group Detail appears. Click the link for a read-only description of the LDAP Group and a listing of its members.

3. Click Edit on the Access Type Detail page to associate an Access Type with an LDAP Group.
4. Click the LDAP Access Group link.
5. (Optional) Enter filter criteria to limit the search to the LDAP groups of interest.
6. Select the LDAP Group that you want to associate with this Access Type.
7. Click Save.
   Association of the selected LDAP Group with the Access Type is complete.

Create an Access Type

Access types define how contacts are authenticated when they log in to the web interface, whether the contacts can modify web forms or the database schema using Web Screen Painter, and which roles are available for the contacts.

You can modify the predefined access types and create new ones.

The access types define all aspects of security. Several predefined access types are included, and you can modify them or can define new ones. Each access type for a user controls the following aspects of system behavior:

- How CA SDM performs the web authentication when the user logs in.
- The access level for the user.
- Whether the user can modify web forms or the database schema using Web Screen Painter.
- What are the roles available to the user.

Follow these steps:

1. Select Security and Role Management, Access Types on the Administration tab.
   The Access Type List page opens.
   Default: 15
2. Click Create New and complete the access type fields (https://wiki.ca.com/display/CASM1401/Data+Partition+Associations#DataPartitionAssociations-AccessTypeFields), as appropriate, on the Create New Access Type page.
3. Use the tabs to complete the following tasks:
   - Configure Web Authentication for an Access Type (https://wiki.ca.com/display/CASM1401/Data+Partition+Associations#DataPartitionAssociations-ConfigureWebAuthenticationforanAccessType)
   - Assign Web Screen Painter Permissions to an Access Type (https://wiki.ca.com/display/CASM1401/Data+Partition+Associations#DataPartitionAssociations-AssignWebScreenPainterPermissionstoanAccessType)
   - Assign Roles to an Access Type (https://wiki.ca.com/display/CASM1401/Data+Partition+Associations#DataPartitionAssociations-AssignRolestoanAccessType)
4. Click Save.
   The access type is created.

Access Type Fields

The following fields appear on the Create Access Type, Access Type Detail, and Update Access Type pages.

- **Symbol**
  Specifies a unique identifier for the access type.

- **Default?**
  Indicates whether this access type is the default that is associated with contacts.

- **Record Status**
  Specifies whether this access type is Active or Inactive.

- **Description**
  Describes the access type. Use this field to help identify the characteristics of the access type.

- **Receive Internal Notification**
  Determines whether the contacts associated with the access type receive internal notification of activities that are related to tickets.

- **Access Level**
  Determines which access types a user can grant to another user. A user can assign an access typeto the contact record of another user only if the access level of the access type they are attempting to assign is ranked the same as or lower than thegrant level for their own access type. The levels are ranked as follows:

  - Admin (highest)
  - Analyst
  - Cust/Emp
  - None (lowest)

  Licensed?
  Determines whether thiscontact is a licensed access type. Contacts assigned to unlicensed access types can only view or update their own personal data.

Configure Web Authentication for an Access Type

You can configure the web authentication and validation type to specify how roles assigned to this access type are authenticated when users attempt to access the CA products. Complete the following fields in the **Web Authentication** tab.

- **Allow External Authentication**
  Select this check box if you want to allow contacts to be authenticated externally, for example by the HTTPD server or the operating system. If you select this option, users with this access type are validated by the appropriate external method as configured during installation.Checks ensure that no external validation has taken place (for example, that the user has not attempted access through a non-secure server) and that the user is defined as a valid contact in the system using the login ID. Then, it uses the access type to determine the correct interface to use.

- **Validation Type**
  Defines how users are authenticated when an external authorization is either not permitted or fails (for example, if the user is attempting access through a non-secure server). The available options are:

  - **No Access**
    Denies access to CA products unless external authentication is allowed and is valid.

  - **Open**
    Access to the CA products are always allowed, with no additional authentication required.

  - **OS**
    Access to the CA products are allowed through operating system user name and password.

  - **PIN / PIN Number**
    Users of this type can access only if they enter the correct value for the PIN field in their contact record. If you select the PIN option, you can choose which field in the contact record stores the PIN by entering the field attribute name in the PIN Field edit box.

  - **CA EEM**
    Access to the CA products are allowed through CA EEM. This option is available only if CA SDM is integrated with CA EEM.

  - **OS-Use Operating System**
    When the Administration Access Type Validation Type drop-down is set to **OS-Use Operating System Authentication** and if you want to login using the CASMAdmin user, you must first create the CASMAdmin user in the Operating System for the login to be successful.

Assign Web Screen Painter Permissions to an Access Type

The Web Screen Painter (WSP) utility allows CA SDM users to build and publish web forms and schemas. The Web Screen Painter tab also controls the database access for Web Screen Painter preview sessions. For the details about WSP, see Using the Web Screen Painter (WSP) (https://wiki.ca.com/pages/viewpage.action?pageId=103915346).

Select the permissions that you want to allow for an access type in the Web Screen Painter tab.

- **Modify Forms**
  Allows the users todo the changes to existing forms withoutdoing the changes available to all users.

- **Modify Schema**
  Allows the users todo the changes to an existing schema withoutdoing the changes available to all users.

- **Publish Forms**
  Allows the users to make their modified forms available to all users.

- **Publish Schema**
  Allows the users to make their modified schema available to all users.

- **Preview Session Can Update Database**
  Allows the users to do the changes to the database during a preview session. By default, database changes are not allowed during a preview session.

Assign Roles to an Access Type

Assign the roles to an access type to limit contacts access to functional areas for assigned roles.

Follow these steps:

1. Select the following roles for this access type:
   - **Reporting Role**
     Defines the reporting access for this type.
   - **REST Web Service API Role**
     Defines the access to the REST web services for this type.
   - **SOAP Web Service API Role**
     Defines the access to the SOAP web services for this type.
   - **Command Line Utility Role**
     Defines the access to the command-line utilities for this type.
2. Click Update Roles.
   The Role Search page opens.
3. Enter any search criteria that you want to limit the list tothe roles of interest, and then click Search.
   The Roles Assigned - Update page opens, listing the roles that matched the search criteria.
4. Select the roles that you want to assign. To select multiple items, hold down the CTRL key while clicking the left mouse button.
5. Click the double right-directional arrows, after you have selected all the roles that you want.
   The selected roles move to the Roles Assigned list on the right.
6. Click OK.
   The Access Type Detail page opens, with the assigned roles listed on the Roles tab.
7. Click Save.
   The Access Type Detail page opens, with a confirmation message that your changes have been saved.
8. Select the role that you want to be the default for this access type upon login. Click Set Default Role.
   Your selection for the default role is saved.

Create Contacts Manually

If you do not want to use an active directory such as LDAP for your contacts information, you can create the contacts manually in CA SDM.

Note: If multi-tenancy is enabled, select the appropriate tenant from the drop-down list.

Follow these steps:

1. Select File, New Contact from the menu bar on the Scoreboard.
   The Create New Contact window opens.

2. Complete the following fields as appropriate for the contact:

Tenant

Specifies the tenant that is associated with the contact (for multi-tenancy installations).

Contact ID

Specifies a unique identifier for the contact. If the default user authentication is being used, the value in this field is used as the password when the user logs in.

User ID

Specifies the user name of the contact. The contact uses this value to log in to the system.

Service Type

Specifies the level of support that is received by the contact.

Data Partition

Specifies the data partition for this contact. This value determines the records that this contact can access.

Access Type

Specifies the access type. The access type determines the system functions the contact can access.

Available

Indicates whether the contact is available for ticket assignments.

Confirm Self-Service Save

Indicates whether the contact receives a confirmation when saving a record from the self-service interface.

Analyst's Tenant Group

(Analyst Contact Type Only) Specifies the tenant group that the analyst is responsible for.
To configure the contact, use the following controls available on the tabs.

Notification

Defines the contact information and method for notifying the contact.

- Select the notification method from the drop-down list (Email, Notification, Pager_Email, xMatters/Email, xMatters/Notification, and xMatters/Pager_Email) that you want to use for each message urgency level for this contact.

  Note: CA SDM supports only one notification method at a time. If you are using Email, then you cannot use Notification at the same time. This applies to all out of the box notification methods like Email, Notification, Pager_Email, xMatters/Email, xMatters /Notification, and xMatters/Pager_Email.

  Note: CA SDM Administrators must update the notification method manually in the contact details page if the xMatters and CA SDM integration is disabled. For more information, see Create a Notification Method (see page 834) and Options Manager xMatters (see page 1303).

- Select the workshift that is valid for each notification urgency level.

For example, you may assign a Regular workshift (five-day week, eight-hours a day) to the normal level notification, but a 24 hour workshift to the emergency level notification.

Address

Specifies the location of the contact.

Organizational Info

Specifies the functional or administrative organization, department, cost center, or vendor information of the contact.

Environment

Specifies the environment of the contact, such as equipment, software, and services.

Groups

Assigns a contact to a group (a collection of contacts with a common area of responsibility).

Roles

Assigns the contact to one or more roles.

Service Contracts

Displays any service contracts that have been associated with the contact.

Special Handling

Lists the special handing contacts and lets you search for and associate a contact to a special handling type, such as a visitor or security risk type.

Event Log

Lists events that are associated with the contact, such as self service and knowledge activities.

Activities

Lists the activity log for the contact.

Click Save.
The contact information is saved.

Building CA Service Catalog

This section contains the following articles:

Guidelines for Modifying Catalog Content

When you modify the catalog content, follow these guidelines, mostly in sequential order, but with iteration as needed:

- Install all content onto a test system, and then browse and understand the default catalog content.
- Review the frequently asked questions. (see page 1995)
- Understand the basic structure of catalog entries. (see page 1996)
- Understand the main parts of a service specification (see page 1999). View the sample service specification (see page 2000) for further details.

- Illustrate the fulfillment of the service as steps in a business process that you can follow logically.
- Create a detailed logical design to help you design the service in the CA Service Catalog.
- Determine what parts of the default catalog you want to modify in your production catalog.
- On subsequent installations, load only those sections of the content that fit into your test catalog.
- Configure all customizations in a test catalog. Test and refine them until you approve them.
- Copy only the approved modifications into your production catalog.
- Consider maintaining a separate development catalog in addition to a test catalog. Keeping the two separate ensures that testing and development can occur in parallel.

Frequently Asked Questions

The following information provides answers to frequently asked questions and includes instructions for managing your catalog content.

- **How do I modify the catalog content?**
  Modify the catalog content by using the standard CA Service Catalog component of the web browser user interface.
- **How do I back up, import, and export catalog content?**
  Use the IXUtil utility to back up the content. You can then export this content from one system, and to import it into another system.
- **How do I make bulk changes to the catalog content?**
  Make bulk changes to the catalog, as follows:

  1. Export the catalog folder or service to be changed, using the IXUTIL utility.
  2. Edit the exported XML file using a text editor.
  3. Delete and reimport the folder into the catalog.

  This process works well for simple changes in descriptions and naming conventions. For example, suppose that your IT organization is named General Information Services (GIS). In that case, consider a bulk change to replace the word "IT" with "GIS" within the catalog.
  You must be familiar with using a text editor for editing the XML files. Be especially careful to use a text editor like Notepad, not a word processor like Microsoft Word.
  Also follow these guidelines:

  - Back up frequently. If referential integrity issues occur, the import process does not always import all content.
  - Review the ixutil.log in the USM_HOME\logs\install folder after each import. Review it for duplicate name errors and other errors that incorrect syntax in the imported data can cause.
- **How do I copy catalog entries from test catalogs to production catalogs?**
  Copy catalog entries from test catalogs to production catalogs, as follows:

1. Use a test catalog to modify the default catalog content.
2. Back up the test catalog.
3. Export the updated catalog content from the test catalog.
4. Import the updated catalog content into your production catalog.

The two entities included in your catalog are the catalog entries and the associated images and URL links.
Use the IXUtil utility to export the catalog entries from the test catalog. Use the same utility to import the exported content into the production catalog.
The catalog entries include folders, services, service option groups, and service option elements. Copy the following entities to the production environment separately: category, class, and subclass definitions (category.xml), images, and status definitions.

Catalog Entries

As an administrator, you use the CA Service Catalog to create and maintain catalog entries. The following types of catalog entries exist:

- Folders (see page 1996)
- Services (see page 1997)
- Service Option Groups (see page 1997)
- Service Options and Service Option Elements (see page 1998)
- Images (see page 1999)
- Category, Class, and Subclass (see page 1999)

Understand these types before you create or modify catalog entries.

Many entries in a single container can be difficult for catalog users to navigate. Therefore, as a general guideline, we recommend that you limit the number of entries in a container to ten. For example, verify that no folder contains more than ten sub-folders or services. Similarly, verify that no service contains more than ten service options.

Note: The out of the box content does *not* add new statuses to the predefined statuses in CA Service Catalog.

Folders

The installation process creates the folders that you select. If you select all folders, then the installation process creates the following top-level folders:

- IT Services
- Telecom Services
- Network Services

- Application Services
- Project Services
- Corporate Services
- Personnel Services
- Facilities Services
- Reservation Services

The names of the folders and services in your catalog must be unique.

If you create your own folders, you can name them any unique name. You can modify the content from the predefined folders. We recommend short descriptive names for folders.

Services

The catalog supports services that contain multiple service option groups. In this starter implementation, however, most services contain one associated service option group. As the catalog designer, you decide to use either one or multiple service option groups per service. In both cases, we recommend that you organize related service option groups in services logically and intuitively.

Focus on the user when designing services and service option groups. A common flaw in catalog design is placing service option groups in a non-intuitive service or folder. When service option groups in a service or folder are unrelated, users have difficulty finding the services that they want. For example, consider a service option group for a network design program. You could place it in a service or folder named Development Tools. However, such a service option group fits better in a service or folder named Miscellaneous Software. A network administrator is more likely to view the latter folder first for this program.

The catalog provides a search tool that can be helpful. This tool supplements thoughtful design, but does not replace it.

Service Option Groups

Most service option groups in the predefined catalog are named the same as the corresponding service, for simplicity. They have multiple service options that are contained within them.

As your catalog becomes more mature, this one-to-one relationship between services and service option groups is likely to decrease. Some examples of having multiple service option groups in a service exist in the "Procure Laptop" and "Procure Desktop" services. The hardware configuration of laptops and desktops have differences. However, the standard and optional software that is bundled with them is typically identical. Therefore, the catalog does not duplicate the service options that are related to software choices in the two services. Instead, both services include service option groups for standard and optional software bundles.

The naming conventions become more important as the number of services and service option groups increases. The naming standards are as follows:

- All folders and services have unique names.

- If a service contains only one service option group, their names are the same.
- If a service contains multiple service option groups, one service option group has the same name as the service, and the others have unique names.

Service Options and Service Option Elements

A service option is the most basic element that users can request or subscribe to in the catalog. A service option consists of one or more service option elements. The service options in the Best Practice content have the following service option elements. Your modified catalog can have more or fewer service option elements, depending on its design.

- **Short Description**
  Specifies a plain text field (not rich text) that describes the service being requested or subscribed to.
  Use this option to describe the service in cases where rich text or HTML is not processed properly. For example, the workflows use this column to title the email.

- **Long Description**
  Specifies a rich text field.
  This text describes the service in detail. This text can also include a hyperlink to an internal web page containing more information about the service.

- **Rate**
  Specifies the cost of the service option.
  Consumers must understand the cost of the service to the corporation, regardless of whether the request is charged back.
  Because the cost structure at your location is unique, all service option elements have been set to a one-time charge. Determining cost and rate structures depends on a number of factors. In some cases, the rate posted in the catalog is only advisory: The rate reminds users that although they are not charged, the service is not free. In other cases, however, the posted rate is linked to a chargeback policy. In these cases, it is designed to recover the cost of the service. Accounting Component is designed for automating the process of tracking service costs.

- **Service Level**
  Describes the level of service the user can expect. The user can click the "More Information" link to get a description of the basic levels of service that they can subscribe to. The sample information that is displayed when you click the "More Info" hyperlink is contained in "sladescription.html" located in the USM_HOME\filestore\images\offerings directory.
  You can change this location, as follows: Use the CA Service Catalog, Service Offerings, Options Group to modify each service option element in your catalog to reference a file in another location.

- **Special Instructions**
  Specifies more instructions for the user. Many services require users to specify more detail information. An example is a "backup production server" service on which you must back up files and must specify the backup interval. The instructions tell users to place this information in the notes that are associated with a request.
  You can use the Form service option element type to present custom forms to gather more information from the requester.

Images

You can optionally associate images with every folder, service, and service option. All images reside in USM_HOME\filestore\images\offerings.

Images whose size is 32x32 pixels fit best in the catalog.

Images can be in any format suitable for a web browser (For example, .jpg, .bmp).

Many predefined images exist in this directory. The Best Practice content does not use all of them. You can optionally use these predefined images and add others to meet the needs of your organization. Use images that help users searching for a service to find the service they need.

Category, Class, and Subclass

The first service option element in a service option determines the Category, Class, and Subclass for the other items in that row. The Best Practice: Foundation catalog uses several Category/Class /Subclasses which are defined in category.xml. If you are building your catalog "from scratch," you can use any Class/Subclass structure. The Category drives associated Workflow processing and other downstream activities. So, do not change the predefined Category corresponding numeric values.

The predefined service option elements reference the predefined category, class, and subclass values in the category.xml file. If you build your catalog on top of the best practices content, do not *change* the predefined settings in the file. Instead, *add* new categories, classes, or subclasses in the file, if necessary.

Service Specification

When you design your catalog, consider the following service specification factors. These attributes help your customers understand the service.

Attribute Name	Definition
Service Description	Brief description of the service which explains what the service includes.
Service Exclusions	Brief description regarding what is not included in the service.
Service Core Dependencies	Listing of the underlying services and processes that are necessary for this service.
Service Options	The various components and options available to users when ordering the service from the catalog.
Service Hours	The time period during which the service is typically available.
Service Maintenance and Planned Down Time	The time period during which the service is typically not available due to scheduled maintenance.
Service Availability	The targeted percentage (of the defined Service Hours) during which service is available for requests.
	The person responsible for the service.

Attribute Name	Definition
Service Owner (Performance Measure Owner)	
Service Users	The intended group of requesters for this service.
Performance Measures /Descriptions	One or more defined performance measurements for the service fulfillment with a base line target.
Key Performance Indicators	The performance measurement which is the primary indicator of the performance of the fulfillment of this service.
Key Goal Indicators	The overall company benefit from this service.
Data Collection Method /Frequency	An overview of the intended data collection method and frequency. If tools and methods are known, specify them in this attribute.
Cost Categorization (to Business Unit)	Definition of the cost categorization of the service regarding the following aspects of costs: direct and indirect, capital and operational, fixed and variable, cost type, cost elements, cost units.
Charging Policies	The charging policy for this service. The template gives examples both for internal and external providers.

Sample Service Specification

This sample server specification illustrates the following costs that are associated with the "Personal Computer (PC)" service:

- Direct (associated costs that are allocated directly to the IT organization) for the request of the other vendor software.
- Capital for the acquisition of the new PC.
- Variable depending on the number of new PC requests.

Charges are based on the following elements:

- Internal Service Provider
- Initial setup of the service at the time of SLA signature plus Hardware
- Fixed subscription per year
- Cost of usage per request
- External Service Provider
- Market Standard

Element	Description
Service Name	Personal Computer

Element	Description
Service Description	New Desktop or Laptop
Service Exclusions	No support, No Equipment Returns
Service Core Dependencies	Architectural standards, including approved server hardware lists Procurement process for IT infrastructure equipment, including appropriate vendor agreements
Service Options	Options, such as Standard Laptop, Deluxe Laptop, Standard Desktop, Deluxe Laptop
Service Hours	24 hours per day, 7 days per week, 365 days per year This value can vary, depending on Service Level that the customer selects.
Service Maintenance and Planned Down Time	Last Sunday of every month from 2AM - 3AM EST This value can vary, depending on Service Level that the customer selects.
Service Availability	Availability Target: 99% of Service Hours This value can vary, depending on Service Level that the customer selects.
Service Owner (Performance Measure Owner)	John Doe - Director, IT Organization
Service Users	Finance, Marketing, Operations, and Customer Service Organizations
Performance Measures and Descriptions	Acknowledgment of order Number of hours that have elapsed between user submitting the request and user receiving acknowledgment of the order. Target: Average less than eight hours Order Fulfillment: Normal Number of days that have elapsed between user submitting the request and user receiving acknowledgment that the requested items are available. Target: Average less than seven days
Key Performance Indicators	Number of days that have elapsed between the time the user submitted the request and the time the vendor notified the user that order was shipped
Key Goal Indicators	Better capacity planning and inventory management through standardized procurement processes Compliance to SLAs by third-party vendors and providers Standardization of computers throughout the organization
Data Collection Method /Frequency	Data is collected for “time of request”, “time of acknowledgment” and “PC available” by feeds. The feeds are available from tools that are used at each event. If the feeds are not available, collect the data daily.
Cost Categorization	Direct and Indirect - Direct cost of service Capital and Operational Capital Fixed and Variable - Fixed based for subscription - variable per request Cost Type - Service + Hardware Cost Elements - Hardware + Services Defined in Service Dependencies Cost Units - Per Request + Hardware
Charging Policies	Internal Service Provider - Fixed Setup Price + Hardware External Service Provider - Market Price

Add Custom Fields to the User Interface

On the CA Service Catalog user interface, you can optionally add custom field that is related to business units, accounts, or users. You can add a new field to meet a custom requirement for your organization or one of your customers. To do so, follow this process:

- Step 1 - Review the Additional Data Fields (see page 2002)
- Step 2 - Review the Sample custom.xml File (see page 2002)
- Step 3 - Expose Additional Data Fields (see page 2002)

Step 1 - Review the Additional Data Fields

The Business Unit, Account, and User schemas in the CA Service Catalog database tables provide extra data fields. By default, these fields do not have labels. The fields do not appear on the CA Service Catalog user interface.

The additional data fields and their data types follow.

- The additional data fields (and their types) for business units in the usm_tenant table follow: data1: nvarchar(32)data2: nvarchar(32)data3: nvarchar(32)data4: nvarchar(64)data5: nvarchar (64)data6: nvarchar(128)data7: nvarchar(128)

- The additional data fields (and their types) for accounts in the usm_account table follow: data1: nvarchar(32)data2: nvarchar(32)data3: nvarchar(32)data4: nvarchar(64)data5: nvarchar (64)data6: nvarchar(64)data7: nvarchar(128)

- The additional data fields (and their types) for users in the usm_contact_extension table follow: data1: nvarchar(512)data2: nvarchar(512)data3: nvarchar(512)data4: nvarchar(512)data5: nvarchar(512)data6: nvarchar(512)data7: nvarchar(512)

Step 2 - Review the Sample custom.xml File

The custom.xml file lists all additional data fields for CA Service Catalog. Optionally expose an extra data field on the CA Service Catalog user interface by adding a label to the field.

The custom.xml file can be different based on the language that is chosen for the system. This file is located in a different folder for each language. For example, for English (icusen), the custom.xml file is located in the USM_HOME\view\webapps\usm\locale\icusen folder.

Step 3 - Expose Additional Data Fields

You can expose the data fields fields to add custom fields to the user interface.

Follow these steps:

1. Edit the custom.xml file for the language of your system. For example, for English, edit the USM_HOME\view\webapps\usm\locale\icusen\custom.xml file.

2. Type the label for the field between the start and end tags for the appropriate field (data1-data7) for the appropriate object: account, business unit (tenant), or user.
   This label appears on the user interface to help users identify the purpose of the field.

3. Save the custom.xml file.

4. Verify that the label appears as specified when you view the related object on the GUI. Examples include the associated add, edit, and profile pages.

Example: Expose Additional Fields in the User Interface

This example configures the account data1 and account data 5 fields in the custom.xml file to expose Cost Center and Department data on the GUI:

```
<account>
        <data1>Cost Center</data1>
        <data2></data2>
        <data3></data3>
        <data4></data4>
        <data5>Department</data5>
        <data6></data6>
        <data7></data7>
</account>
```

Note: To expose a field without specifying a new label on the user interface, specify a space as the value of the label.

Modify the Category, Class, and Subclass Lists

Each service option in the catalog has a category, class, and subclass assigned to it. CA Service Catalog assigns a value to each category, class, and subclass in the category.xml file.

Each <option> section in the category.xml file represents a separate category and contains one or more <class> sections. Each of these sections contains one or more <subclass> sections.

The category.xml file can be different based on the language that is chosen for the system. The file is located in a different folder for each language. For example, for English (icusen), the category.xml file is located in the USM_HOME\view\webapps\usm\locale\icusen\billing folder.

Each service option in the catalog has a predefined category, class, and subclass assigned to it. You can update the existing values or can add new values to meet the needs of your organization or customer.

Note: After you add a category, class or subclass value in the category.xml file, do *not* remove it. Ensure that you do not change the meaning of the category values, because business logic in the product is based on the category values.

Follow these steps:

1. Review the inline comments in the file. Verify that synchronized sections of the file remain synchronized. Verify that you do not use, certain status values.

2. Edit the appropriate category.xml file for the language of your system. For example, for English, edit the USM_HOME\view\webapps\usm\locale\icusen\billing\category.xml file.

3. Add a line or section for the category, class, or subclass you want to add. Select an unused numeric value for the category, class, or subclass you are adding.

   Note: To add a new category, add a new “option” section containing at least one class and subclass. To add a new class, add a new “class” section containing at least one subclass.

   Use a unique numeric value within the list of related objects. For example, suppose you add a new class to the Other category. In that case, you cannot use a value of 10, because the IT class already uses that value.

4. Update any existing values as needed; do *not* use the same value twice.

5. Save the category.xml file and test by using the CA Service Catalog user interface screens.

Example: Add a New Subclass

To add a new subclass named “Mouse” to the IT class of the Hardware category, modify the category.xml file as illustrated in the following example:

```
<option value="1" name="Hardware">
      <class value="10" name="IT">
          <subclass value="10" name="Desktop" />
          <subclass value="20" name="Laptop" />
          <subclass value="30" name="Monitor" />
          <subclass value="40" name="Memory" />
          <subclass value="50" name="Printer" />
          <subclass value="60" name="Server" />
          <subclass value="70" name="Storage" />
          <subclass value="71" name="Mouse" />
          <subclass value="999" name="Other" />
      </class>
    ...
  </option>
```

Modify the User and Service Approval Level List

Each user is assigned an approval level, in its user profile. Each service that requires approval is also assigned an approval level, in its service definition.

When a service uses the “System approval process,” the approver requires an approval level equal to or greater than the approval level of the service. Otherwise, the approver cannot approve or reject the service.

The approval level values are maintained in a file named approval_shared.xml. This file can be different based on the language that is chosen for the system. The file is located in a different folder for each language. For example, for English (icusen), the approval_shared.xml file is located in the USM_HOME\view\webapps\usm\locale\icusen folder.

You maintain the approval levels for users and services in a file named approval_shared.xml. You can add or change the values in this file to meet the needs of your organization.

Note: After you add an approval level to the file, do not remove it.

Follow these steps:

1. Edit the appropriate approval_shared.xml file for the language of your system, using an editor, such as Notepad. For example, for English, edit the approval_shared.xml file in the USM_HOME%\view\webapps\usm\locale\icusen folder.

2. Add a line for the approval level that you want to add. Select an unused numeric value for the approval level you are adding.

3. (Optional) Update an existing name or value in the file.

4. Save the approval_shared.xml file.

5. Verify that the new approval level appears as an option when you edit user profiles and service definitions on the product interface.

You have maintained the approval levels for users and services.

Example: Add a New Approval Level

This example illustrates a new approval level added to approval_shared.xml file. The name of the level is Director. The approval level value is 60.

```
<?xml version="1.0" encoding="UTF-8"?>
<shared>
    <approval_level>
        <option value='0'>Level 0</option>
        <option value='10'>Level 10</option>
        <option value='20'>Level 20</option>
        <option value='30'>Level 30</option>
        <option value='40'>Level 40</option>
        <option value='50'>Level 50</option>
        <option value='60'>Director</option>
    </approval_level>
</shared>
```

Modify the Request Status List

This article contains the following topics:

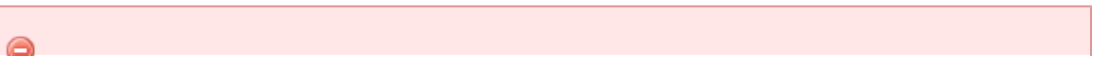
Each service and service option in a request has a status. In addition, the request has an overall status. CA Service Catalog supplies an extensive list of status values by default. Modify status values for the approval and fulfillment phases of the request life cycle, by editing the requestshared.xml file. You can also change the spelling of existing status values.

You maintain the request status values in the requestshared.xml file. This file can be different based on the language that is chosen for the system. The file is located in a different folder for each language. For example, for English (icusen), the requestshared.xml file is located in the USM_HOME\view\webapps\usm\locale\icusen\request folder.

The request status of the *entire* request is visible on the Pending Actions page. The request statuses of individual items in the request are visible in the Item Status drop-down list on the request-related user interface pages: Request Details, Approve Request, Fulfill Request, and Push Through Request. Updates that you make to the request status values in the requestshared.xml file are reflected in the options that users see on those pages.

Follow these steps:

1. Become familiar with the requestshared.xml file (see page 2007).
2. Back up the original requestshared.xml file and save it for reference.
3. (Optional) Modify existing status values or add additional request statuses (see page 2008).
4. (Optional) Hide request statuses (see page 2010).
5. (Optional) Restrict the status changes available for a request item based on its status (see page 2012).
   By default, all options (all statuses) are available for an item always, until the entire request is completed. In other words, you can change the status of request items to any value at any time. However, your organization can optionally restrict the menu options available for a request item that is based on its status.
6. Test your changes by verifying that they are correctly reflected on the request-related user interface screens.
   In the Item Status drop-down list on the request-related user interface pages, the status is designated with an asterisk (*).



Important! After you have added and used status numeric values to the default list, do *not* remove them.

Review requestshared.xml

Become familiar with the requestshared.xml file, as follows:

- Understand the purpose of the major sections (see page 2007) of the file: request_header, request_item, request_item_approval_action, and request_item_fulfillment_action.
- Understand that the status values in these sections must remain synchronized.
- Understand that the order of the statuses in the status drop-down lists on the GUI matches the order of the statuses in the requestshared.xml file. For example, suppose that the status 800 (Reject) is defined above the status 600 (Approved) in this file. In this case, the Reject status appears above the Approved status in the status drop-down lists on the GUI.
- Review the inline comments and note the *reserved* status values.
- Review the ranges for custom status values (see page 2008) to see which ranges are reserved for specific types of status values.

Important! Do *not* modify or delete the opening and closing lines that define the default statuses in the requestshared.xml file . Even when you modify statuses, these lines must remain as shown. This requirement applies to both the <request_item_approval> and <request_item_fulfillment> sections. These lines help ensure proper status behavior when the customizations are not used or are defined incorrectly.

```
- <custom_menu current_status_value="default">
status lines
</custom_menu>
```

Major Sections

The major sections of the requestshared.xml file are as follows:

- **request_header**
  Maintains all possible status values for the entire request.
- **request_item**
  Maintains all possible status values for a specific item (such as a service option element or service option group) in a request.
- **request_item_approval_action**
  Maintains all possible status values for a specific item in a request, when the request has been submitted but has not been approved or rejected.

- **request_item_fulfillment_action**
  Maintains all possible status values for a specific item in a request, when the request has been approved but has not yet been fulfilled.

The list of possible status values must be synchronized in the request_header and request_item sections: They must have the same values with same meaning.

Every value in the request_item_approval_action and request_item_fulfillment_action sections must have a matching value in both the request_header and request_item sections. The value in the request_item_approval_action and request_item_fulfillment_action sections must be a complete set or a subset of the values in the request_header and request_item sections.

Ranges for Custom Status Values

When adding a new request status in the requestshared.xml file, define it within the range that is specified for the custom statuses:

- 300 to 399 - custom *submit* status
- 500 to 599 - custom *pending approval* status
- 900 to 990 - custom *approved* status

Add an Additional Request Status

You can modify the request status list by adding request statuses. One common purpose is for approval or rejection of a request by a specific department. For example, the Finance department.

Follow these steps:

1. Edit the requestshared.xml file for the language of your system in a text editor. For example, for English, edit the file in the USM_HOME\view\webapps\usm\locale\icusen\request folder.

Add a line, including the number and text for the new status to the following sections: <request_header> and <request_item>.

- Select an unused numeric status value in the appropriate range for custom status values for the status you are adding.

  Note: If possible, limit the text of the status value to 40 characters. Text longer than 40 characters can be truncated in the drop-down status menu lists and request status fields. In such cases, the entire text string is displayed to catalog users *only* in the tooltip text.

- Copy that line to the custom section or sections where you want them to appear. Examples include <request_item_approval>, <request_item_fulfillment>, <request_item_stuck_approval_action>, and <request_item_stuck_fulfillment_action>.
- Delete the text from the line you copied and modify the line to include the statval="*value*" expression.

- Save the requestshared.xml file.
- Verify that the changes are correctly reflected on the request-related user interface screens (the Request Details, Approve Request, and Fulfill Request screens).

Example: Add New Approval Statuses

To add approval statuses 500, 700, and 900, all related to financial approval, add the new lines for these statuses to the request_header, request_item, and request_item_approval_action sections of the requestshared.xml file. Examples follow, in **bold**.

Specify the numeric value and text in the request_header and request_item sections. Specify only the numeric value (without the text) in the request_item_approval_action section.

```
<?xml version="1.0" encoding="UTF-8" ?>
...
- <request_header>
  <!--  status values must be synchronized with the status list in request_item,
request_item_approval_action and/or request_item_fulfillment_action   -->
  <st_1>Pending</st_1>
  <st_2>Completed</st_2>
...
  <!--  400 to 499 are reserved   -->
  <st_400>Pending Approval</st_400>
  <!--  500 to 599 can be used for custom pending approval status   -->
  <st_500>Pending Financial Approval</st_500>
  <!--  600 to 699 are reserved   -->
  <st_600>Rejected</st_600>
  <!--  700 to 799 can be used for custom rejected status   -->
  <st_700>Rejected by Financial Approver</st_700>
  <!--  800 to 899 are reserved   -->
  <st_800>Approved</st_800>
  <st_801>Approval Not Needed</st_801>
  <!--  900 to 990 can be used for custom approved status   -->
  <st_900>Approved by Financial Approver</st_900>
  !--  991 to 999 are reserved   -->
  <st_999>Approval Done</st_999>
...
 </request_header>
- <request_item>
  <!--  status values must be synchronized with the status list in request_header,
request_item_approval_action and/or request_item_fulfillment_action   -->
  <st_1>Pending</st_1>
  <st_2>Completed</st_2>
...
  <!--  400 to 499 are reserved   -->
  <st_400>Pending Approval</st_400>
  <!--  500 to 599 can be used for custom pending approval status   -->
  <st_500>Pending Financial Approval</st_500>
  <!--  600 to 699 are reserved   -->
  <st_600>Rejected</st_600>
  <!--  700 to 799 can be used for custom rejected status   -->
  <st_700>Rejected by Financial Approver</st_700>
```

```
  <!--  800 to 899 are reserved   -->
  <st_800>Approved</st_800>
  <st_801>Approval Not Needed</st_801>
  <!--  900 to 990 can be used for custom approved status   -->
  <st_900>Approved by Financial Approver</st_900>
  <!--  991 to 999 are reserved   -->
  <st_999>Approval Done</st_999>
...
  </request_item>
- <request_item_approval_action>
  <!--  status values must be synchronized with the status list in request_header and
request_item   -->
  <!--  A "default" value for the attribute "current_status_value" indicates these
statuses will be listed by default in the "item status" menu if no other custom
statuses are defined   -->
  <custom_menu current_status_value="default">
  <!--  400 to 499 are reserved   -->
  <!--  500 to 599 can be used for custom pending approval status   -->
    <st_500 statval="500"/>
  <!--  600 to 699 are reserved   -->
  <!--  700 to 799 can be used for custom rejected status   -->
  <st_700 statval="700"/>
  <!--  800 to 899 are reserved   -->
  <st_800 statval="800">Approve</st_800>
  <!--  900 to 999 can be used for custom approved status   -->
   <st_900 statval="900"/>
...
```

Hide Request Statuses

The default list of request statuses can include more options than you need for certain categories. You can hide some of the values in that category. So, users do not see these options on the GUI when they handle requests pending action.

Follow these steps:

1. Edit the requestshared.xml file for the language of your system using a text editor. For example, for English, edit the file in the USM_HOME\view\webapps\usm\locale\icusen\request folder.

2. Edit the line in the <request_header> and <request_item> sections for each status that you want to hide. Enter the comment characters before and after the original expression.

3. Hide the corresponding lines in all other sections that use it, such as the <request_item_approval> or <request_item_fulfillment> section.

   Note: Hide the exact same lines in all relevant sections of the file. Doing so is required for the status to appear correctly in the user interface.

4. Save the requestshared.xml file.

5. Test your changes by verifying that they are correctly reflected on the following request-related pages: Request Details, Approve Request, and Fulfill Request.

Example: Hide Request Statuses

To hide certain default fulfillment-related statuses, enter the comment characters before and after the original expression. Example in **bold**. Enter the comment characters in the request_header, request_item, and request_item_fulfillment_action sections of the requestshared.xml file.

In this example, *before* the comment markers are added, the following statuses are visible on the following request-related pages: Ordered, Shipped, Received, Order Cancelled, Staged, and Configured. *After* the comment markers are added, the following statuses are visible on those pages: Ordered, Shipped, and Configured.

```
- <request_header>
...
  <st_1004>Ordered</st_1004>
  <st_1006>Shipped</st_1006>
   <!--<st_1007>Received</st_1007>-->
   <!--<st_1008>Order Cancelled</st_1008>-->
   <!--<st_1017>Staged</st_1017>-->
  <st_1019>Configured</st_1019>
...
  </request_header>
- <request_item>
...
  <st_1004>Ordered</st_1004>
  <st_1006>Shipped</st_1006>
   <!--<st_1007>Received</st_1007>-->
   <!--<st_1008>Order Cancelled</st_1008>-->
   <!--<st_1017>Staged</st_1017>-->
  <st_1019>Configured</st_1019>
...
  </request_item>
- <request_item_fulfillment_action>
...
  <custom_menu current_status_value="default">
...
  <st_1004 statval="1004"/>
  <st_1006 statval="1006"/>
   <!--<st_1007 statval="1007"/>-->
   <!--<st_1008 statval="1008"/>-->
   <!--<st_1017 statval="1017"/>-->
  <st_1019 statval="1019"/>
...
</shared>
```

Restrict the Status Changes Available for a Request Item

You can restrict the status changes available for a request item that is based on its current status. For example, suppose that when an item is approved (Approved status), you no longer want users to be able to change the status *except* to a fulfillment-related status. You can configure the Item Status drop-down list to display *only* fulfillment-related options for items whose status is approved.

Follow these steps:

1. Edit the requestshared.xml file for the language of your system using a text editor. For example, for English, edit the file in the USM_HOME\view\webapps\usm\locale\icusen\request\requestshared.xml folder.

2. Locate the section of the file in which you want to restrict the available changes for one or more status values.
   You can restrict status changes in any section *except* the <request_item> and <request_header> sections.

3. Decide which status you want to restrict and the statuses to which you permit it to be changed.
   The list of all existing status values appears under the following line:

   ```
   - <custom_menu current_status_value="default">
   ```

4. Add a request status to permit in your list, if necessary. The statuses that you want to permit must exist already.

5. Locate the custom menu section. By default, this section is indented and commented out. Delete the opening and closing comment lines of this section.

   ```
   - <!--
           <custom_menu current_status_value="400">
           <st_400 statval="400"/>
           <st_600 statval="600"/>
           </custom_menu>
     -->
           <custom_menu current_status_value="400">
               <st_400 statval="400">/>
               <st_600 statval="600"/>
           </custom_menu>
           <custom_menu current_status_value="400">
               <st_400 statval="400"/>
               <st_600 statval="600"/>
                    <st_801 statval="801"/>
             </custom_menu>
   ```

6. Verify that the value in the current_status_value="*nnn*" expression in the first line of this section matches the status value that you want to restrict.
   For example, in the previous step, 400 corresponds to the Pending Approval status. Therefore, the status values shown appear on request-related pages when the status value is Pending Approval. If you want to restrict a different status, replace the current value with your new value.

7. Verify that the value in the current_status_value="*nnn*" expression is defined in one of the "<st_*nnn* statval=..." lines, as shown for Pending Approval in the previous example.

8. Copy and paste the additional status or statuses to which you want to allow the status to be changed. You can copy and paste it from the list of status values earlier in the section.
   For example, in the <request_item_approval> section, copy and paste the new "<st_801..." line to the custom_menu section for Pending Approval:

Now Approval Not Needed status is added to the statuses to which items in Pending Approval status can be changed.

- Restrict status changes for another status in the same section of requestshared.xml file, if necessary. Use these guidelines:

  1. Copy the entire custom_menu element and its children.

  2. Paste it after the element that you updated.

  3. Modify the newly copied element.

  4. Modify existing custom_menu element and children, if necessary. For example, in the <request_item_fulfillment> section, suppose you want to restrict items in Pending Fulfillment status to be changed to either Fulfillment Cancelled or Fulfilled. In that case, modify the existing custom_menu element as follows:

```
<custom_menu current_status_value="1000">
    <st_1000 statval="1000"/>
    <st_1999 statval="1999"/>
    <st_2000 statval="2000"/>
</custom_menu>
```

- Save the requestshared.xml file.

- Verify that the changes are correctly reflected on the request-related user interface pages (the Request Details, Approve Request, and Fulfill Request pages).

You have restricted the status changes available for a request item that is based on its current status.

Modify the Request Priority List

This article contains the following topics:

Every request has a priority that is assigned to it. CA Service Catalog supplies predefined priority values in the requestinfoshared.xml file. You can add or change the values in this file. You can also use this file to specify which user roles can assign specific priority values to requests. For example, you can add a new priority value "Immediate" that only the Service Delivery role can assign to a request.

The requestinfoshared.xml file can be different for each language and is located in a different folder for each language. For example, for English (icusen), the requestinfoshared.xml file is located in the USM_HOME\view\webapps\usm\locale\icusen\request folder.

You can modify the predefined priority levels:

- Add a new priority level for a specific role. (see page 2016)
- Add a new priority level for multiple roles. (see page 2015)

Priority Levels

The <priority_levels> section of the request and priority list in the requestinfoshared.xml file defines the numeric and text values for each priority. Each <levels> section defines those priority values that are available to the role code specified in the role attribute. The “default” role specification is used when no section exists for the role of the user.

The priority list appears in the order that is specified in the <priority_levels> section, regardless of role. You can use the defaultSel attribute to specify the default value for a new request according to role. The following table lists the roles and codes:

Role	Code
Catalog User	catalogenduser
Request Manager	requestmanager
Catalog Administrator	catadministrator
End User	enduser
SMA End User	smaenduser
Administrator	administrator
Service Manager	servicemanager
Super Business Unit Administrator	stadministrator
Service Delivery Administrator	spadministrator

You can edit this file to add values or change the spelling of existing values.

Suppose that a request uses a priority value that is *not* available to the role of the user editing the request. In that case, the user sees that priority in the list of priority values. Suppose that the request is set to another priority that *is* available the role of the user editing the request. In that case, the user can see *only* the priorities available to its role.

Example: Customizations for the requestinfoshared.xml File

If the Catalog End User role does not include priority 1 (High), a user who has that role does not see "High" listed in the priority list. Moreover, that user cannot set the priority of a request to High.

Suppose that the following situation occurs:

- A Request Manager who can use all the status values later sets the priority of the request to High.
- A user with the Catalog End User role later edits the request.

In this case, the status of High does appear in the priority list.

Thus, administrators *can* configure the product to prevent a certain role from using a particular priority value. Administrators cannot prevent users in that role from viewing and editing their requests when another user has set the priority.

Add a New Priority Level for Multiple Roles

If necessary for your organization, you can add a new priority level to the predefined priority levels.

Follow these steps:

1. Edit the requestinfoshared.xml file for the language of your system, using an editor, such as Notepad. For example, for English, edit the USM_HOME\view\webapps\usm\locale\icusen\request\ requestinfoshared.xml file.
2. Add a line in the priority_levels section for the priority you want to add. Specify a unique numeric value for the new priority level.
   The priority values are listed in the user interface in the order that they appear in this file section.
3. Perform *one* of the following actions:
   - Add a line in the levels section for each role that you permit to use the new priority.
   - Add a line in the levels section for the role. The line makes the new priority available to all users who do not have a role-specific priority list.
4. Save the file.
5. Log in to CA Service Catalog as a user with the role that you modified. Verify your updates on the request-related pages.

Example: Add a New Priority for All Roles

This example adds the following **bold** line to the requestinfoshared.xml file. This example adds a new priority named “Urgent” and makes it available to all users who do not have a role-specific priority list.

```
<priority_levels>
    <priority_6 propval="6">Urgent</priority_6>
    <priority_1 propval="1">High</priority_1>
    <priority_2 propval="2">Medium-High</priority_2>
```

```
    <priority_3 propval="3">Medium</priority_3>
    <priority_4 propval="4">Medium-Low</priority_4>
    <priority_5 propval="5">Low</priority_5>
    </priority_levels>
    <priority_level_roles>
<levels role="default">
    <level propval="1" />
    <level propval="2" />
    <level propval="3" defaultSel="true"/>
    <level propval="4" />
    <level propval="5" />
    <level propval="6" />
</levels>
</priority_level_roles>
```

Add a New Priority Level for a Specific Role

If necessary for your organization, you can add a new priority level to the predefined priority levels. You can add a new priority level for a specific role only.

Follow these steps:

1. Edit the requestinfoshared.xml file for the language of your system, using an editor such as Notepad. For example, for English, edit the USM_HOME\view\webapps\usm\locale\icusen\request\ requestinfoshared.xml file.

2. Add a level section for the affected role.

3. Perform *all* of the following actions in that section:

   - Specify the role code in the role attribute.

   - Include only the lines from the priority_levels section that you want users in the role to see.

   - Specify the default priority for new requests by using the defaultSel attribute.

4. Save the file.

5. Log in to CA Service Catalog as a user with the role that you modified. Verify your updates on the request-related pages.

Example: Add a New Priority Level for a Specific Role

This example adds a new priority list for users with the Catalog User role. This example sets the default priority to Medium-Low and does *not* allow users to set the priority to High. This example achieves these goals by adding the new section that is shown in **bold**:

```
<priority_levels>
        <priority_1 propval="1">High</priority_1>
        <priority_2 propval="2">Medium-High</priority_2>
        <priority_3 propval="3">Medium</priority_3>
        <priority_4 propval="4">Medium-Low</priority_4>
```

```
        <priority_5 propval="5">Low</priority_5>
    </priority_levels>
    <priority_level_roles>
        <levels role="default">
            <level propval="1" />
            <level propval="2" />
            <level propval="3" defaultSel="true"/>
            <level propval="4" />
            <level propval="5" />
    </levels>
        <levels role="catalogenduser">
            <level propval="2" />
            <level propval="3" />
            <level propval="4" defaultSel="true"/>
            <level propval="5" />
    </levels>
</priority_level_roles>
```

Modify the Typefaces Available for Notes in Requests

Users can add notes to requests by accessing the Request Details page and clicking Add in the Notes section. The Add Notes dialog appears and presents several type faces and type sizes as options. For these notes, the default typeface is Arial, and the default type size is 8-point. In addition, users can apply several formatting and highlighting options to these notes.

By default, all supported type faces are enabled. The Add Notes dialog displays all type faces listed in the <fonts> section of requestshared.xml file. Administrators can optionally limit or expand the typefaces that appear to users in the drop-down list of the dialog.

Users can select a typeface in the drop-down that the local computer being used to display or print the request does not support. In that case, the typeface changes to the default typeface, Arial.

Follow these steps:

1. Open the requestshared.xml file and move to the <fonts> section of the file.

2. Leave the type faces that you want to be available to users for notes in request. Comment out the type faces that you do not want to appear in the dialog.
   Comment the lines whose font you want to exclude from the Add Notes dialog.
   For example, to comment out the Courier New and Bookman Old Style type faces, modify their lines as follows:

   ```
   <!--<courier_new>Courier New</courier_new>-->
   <!--<bookman_old_style>Bookman Old Style</bookman_old_style>-->
   ```

3. Add a new typeface to the list that appears in the drop-down list in the dialog: Enter a new line and specify the new typeface. Use the following convention: If the font name is X Y, use the format <x_y>X Y</x_y>.
   For example, to add a typeface, "my company font", add the following line to the <fonts> section:

   ```
   <my_company_font>my company font</my_company_font>
   ```

The fonts that you added become available to users for notes in requests.

4. Save and close the requestshared.xml file.

Verify that the local computer being used to display or print the request supports the font.

- Verify your changes by adding a note to a request and reviewing the available typefaces.

You have modified the typefaces available to users for notes in requests.

Modify XSL, XML, JavaScript, and Image Files

CA Service Catalog includes several XSL, XML, JavaScript, and image files. Together, they are used to form every page and every page element in the product. Each file represents one page or a part of a page. For example, a dialog, menu option, form field control, message, or picture.

You can optionally modify any of these files to meet your requirements. To modify XSL, XML, JavaScript, and image files, follow this process:

1. Determine the specific page or part of a page that you want to modify.
2. Locate the file whose name matches the element you want to change. For example:
   - To modify the configuration information of any of the integrated products, locate the toolsconfig.xsl file.
   - To modify the states of request life cycle, locate the requestshared.xml file.
   - To modify the messages that appear when a user tests the connection for a new administration configuration setting, locate the toolsconfig.js and toolsconfig.xsl files.
   - To modify the edit button of the Administration, Configuration page, locate the modify.gif and toolsconfig.xsl files.
   - Modify the request status list by editing the requeststatus.xml file.
3. Open the file, review its contents, and verify that it controls the element or behavior that you want to change.
4. Copy the file from its original location to the custom location. Use the table as a reference.
5. Modify the file according to your requirements.
6. If you modified a JavaScript or image file, perform this step. Otherwise, skip it.
   a. Copy the modified JavaScript file to the \FileStore\custom\explorer\scripts folder.
   b. Copy the modified images to the \FileStore\custom\images folder.
   c. Locate the XSL file in the custom location in which the JavaScript or image file is used.

d. Update this XSL file and specify the new custom path name of the JavaScript or image file. To do so, prepend "FileStore/" to the relative path of the JavaScript or image file. Use the following example as a model:

```
<script src="FileStore/custom/explorer/scripts/custom_form_example.js"><
/script>
```

This action is required because the XSL file references the filestore location for the modified script files.

Important! If you are using multiple Catalog Component computers, verify that the filestore is shared among *all* of them.

7. Clear the USM_HOME\view\translets folder on all Catalog Component computers: Delete all files in this folder, but do *not* delete the folder itself.

8. Restart all Catalog Component computers.

9. Verify that the changes are working in CA Service Catalog as you intended.

In the following table, the parent folder is USM_HOME/view/webapps/usm. The filestore folder is % USM_HOME/filestore. The folder entries, such as /explorer and /custom/explorer, are subfolders under the parent and filestore folders.

File Type	Original Location in Parent Folder	Custom Location in Filestore Folder
XSL	/explorer	/custom/explorer
XSL	/explorer/request	/custom/explorer/request
XML	/locale/icusen*	/custom/locale/icusen*
XML	/locale/icusen*/request	/custom/locale/icusen*/request
image	/images	/custom/images
image	/images/billing	/custom/images/billing
JS	/explorer/scripts	/custom/explorer/scripts

*The folder name *icusen* applies to English-language implementations only. If you are using a non-English implementation, your locale-specific folder name is different. In such cases, use your locale-specific folder name instead of *icusen*.

Increase the Number of Values for a Drop-Down Variable

An administrator can add a query runtime variable that appears as a drop-down list to users. The limit for the number of values in the list is 1000. If the report query returns more than 1000 values, the system truncates these additional values. So, the user cannot view them in the drop-down list. You can increase the number of values that appear in the drop-down list to be greater than 1000.

Follow these steps:

1. Verify that your implementation has set up a filestore, a single location for shared files.
2. Copy the reportsgenericgetvariables.xsl file from its *parent* folder (USM_HOME\View\webapps\usm\explorer\reports) to the *filestore* folder.
3. Open the reportsgenericgetvariables.xsl file in the filestore and locate the following line:

   ```
   <input type="hidden" name="Args" value="1000"/> <!---1-->
   ```

4. Increase 1000 to the value you want.
5. Save the file.
6. Restart all Catalog Component computers.
7. Run a report and test the increased limit and verify the results.

You have increased the number of values for a drop-down variable.

Modify the Branding

As an administrator, you can modify the look-and-feel of the CA Service Catalog UI. The following are the main categories of look-and-feel elements that you can modify:

- Logos are image files that uniquely identify a company, business unit, or super business unit. These logos include the login logo (see page), global logo (see page), and business unit logo (see page).
- The login page (see page 2024) enables a user to access the product.
  The same login page (including the login logo) applies to all users in all business units. For example, images and icons (*except for* logos), menus, and tabs. When applicable, these elements include colors, font name and point size, highlighting, and related specifications. You modify these look-and-feel elements by editing the Cascading Style Sheet (CSS) files for the login page.
- *A theme* (see page 2026)specifies the settings for several look-and-feel elements. For example, images and icons (*except for* logos), menus, and tabs. When applicable, these elements include colors, font name and point size, highlighting, and related specifications. You modify these look-and-feel elements by editing the CSS files for the theme.
  The look-and-feel of the UI matches the theme of the business unit that you are logged in to. If theme is not set for a business unit, CA Service Catalog checks the business unit hierarchy and it finds a theme. Thus, if a business unit does not have its own theme, it uses the theme of its closest parent business unit. You can use the same theme for all business units. Alternatively, you can optionally create and use different themes for different business units.
- Global page elements appear on several or all product pages. They include the product name, shopping icon, and footer. Global page elements are always the same, on every product page where they appear.
  Like the elements of the login page, global page elements apply to all users, regardless of their

business unit. You *cannot* override them with business unit-specific settings. The global page elements also apply regardless of whether you have modified the themes of one or more business units.
You modify global page elements (see page 2030) by editing the includes_shared.xml file.

You can modify any, all, or none of the items in this list. This separation provides flexibility.

Important! Verify that the changes you plan to make to each one are compatible with each other. Such consistency helps provide a consistent look-and-feel to users. For example, use similar colors and elements on both the login page and the product pages.

Upgrade Considerations

Depending upon your implementation and if you have customized any of these elements in previous releases, perform *one* of the following actions:

- Verify that the modified files reside in a *custom* subfolder of the USM_HOME\FileStore folder.
- Recreate your changes by following the instructions in this section to:
  - Change the Logos (see page 2021)
  - Modify the Login Page (see page 2024)
  - Modify the Theme (see page 2026)
  - Modify Global Page Elements (see page 2030)

Change the Logos

This article contains the following topics:

Logos are image files that uniquely identify a company, business unit, or super business unit. As a service delivery manager, you can modify the logos that are used on the CA Service Catalog UI. Using custom logos helps reinforce branding or other messaging in your organization.

Note: We recommend that you size your custom logo to be approximately the same size as the predefined logo.

Change the Login Logo

CA Service Catalog includes a predefined login logo that you can optionally replace with a custom login logo. The login logo *always* applies to the login page, regardless of whether you have specified different logos for different business units.

Follow these steps:

1. Determine the custom login logo that you want to use.
2. Access the USM_HOME/FileStore/themes/common/images/logo folder on your filestore computer.
3. Copy and rename the predefined login logo (login_logo.png).
4. Copy the custom logo to the same folder. Rename it to the name of the original logo.
5. Access the login page for CA Service Catalog.
6. Verify that the predefined login logo no longer appears and that the custom login logo appears correctly.

You have changed the login logo.

Change the Global Logo

CA Service Catalog includes a *predefined* global logo that applies to all users. You can optionally replace it with a *custom* global logo. The global logo appears in the heading of all product pages (except the login page) and request emails.

Note: If a business unit has its own logo, users who log in to it see the business unit logo instead of the global logo.

Follow these steps:

1. Determine the custom global logo that you want to use.
2. Access the USM_HOME/FileStore/themes/common/images/logo folder on your filestore computer.
3. Copy and rename the predefined global logo (header_logo.png).
4. Copy your custom logo to the same folder. Rename it to the name of the original logo.
5. Log in to CA Service Catalog.
6. Verify that your custom global logo is legible on the UI and in request emails.

You have changed the global logo.

Change the Business Unit Logo

For each business unit, you can optionally specify a *business unit* logo. If you specify this logo, it replaces the *global* logo in the heading on product pages and request emails for users of the business unit. You can update the logos for every business unit or only for specific business units. For example, you can decide to customize logos only for super tenants directly under the root business unit.

Important! If you have enabled multi-tenancy with CA Service Desk Manager, CA Service Catalog ignores any of its settings for business logos. Instead, CA Service Catalog uses the logo or logos that the CA Service Desk Manager setup specifies, if applicable. If no CA Service Desk Manager logo applies, then each business unit uses the CA Service Catalog global logo.

Follow these steps:

1. Determine the business unit logo that you want to use.
2. (Optional) Perform the following actions:
   - Rename the custom logo file intuitively to match its business unit. For example, for a business unit that is named Vienna_123, name the logo Vienna_123_header_logo.png.
   - Create a subfolder that is named "custom logos" in USM_HOME/FileStore/themes /common/images/logo directory.
3. Copy your custom logo to the USM_HOME/FileStore/themes/common/images/logo folder on your filestore computer.
4. Perform *one* of the following actions, whichever applies to your level of administrative access:
   - Log in to the business unit whose logo you want to change.
   - Log in to the root business unit:
     a. Select Administration, Business Units.
     b. Drill down the tree to the business unit whose logo you want to change.
5. Edit the business unit.
6. Enter the URL of the logo that you copied in the Logo field and save your changes.
7. Refresh your browser.
8. Verify that your business unit logo is legible on the UI and in request emails.
9. (If the business unit has child business units) Verify:

- If the child business unit has its own logo, users who log in to it see the child logo, not the parent logo.
- If the child business unit does not have its own logo, users who log in to it see the global logo.

Thus, users with access to multiple business units can see different header logos when they log in to each business unit.

You have specified a business unit logo.

Modify the Login Page

You can modify the login page, as follows:

- Modify the login logo (see page).
- Modify the *content* or *text* of the Predefined Login Page (see page 2024).
- Modify the *look-and-feel* of several elements of the login page by editing the logon.css file (see page 2024).

You can modify the login page *without* changing the theme for one or more business units. The same login page applies to all users, regardless of whether you have changed any theme. This separation provides greater flexibility to your organization. This separation also enables you to update the login page alone more quickly and efficiently.

As an administrator, ensure that you have expertise in the following areas before modifying the login page:

- UI design, especially look-and-feel elements
- Standard specifications for CSS files
- Customization of the CSS files, using a CSS file editor for your web browser

Predefined Login Page

The following table lists the elements of the login page that you can customize, except for the login logo. When applicable, each row lists the section of the login.css file that affects the look-and-feel of the element.

GUI Element	File Location under USM_HOME*	Section in Logon.css File
Text for the browser window title and title bar	view\webapps\usm\locale\icusen\logon.xml	.loginpage
Text for product name	view\webapps\usm\locale\icusen\logon.xml	. loginproductname
Login input text		.logininputtext

GUI Element	File Location under USM_HOME*	Section in Logon.css File
	view\webapps\usm\locale\icusen\logon.xml **Note:** This text supplies the User Name, Password, and Advanced-Business Unit fields.	
Copyright text and date	view\webapps\usm\locale\icusen\logon.xml	.loginpagecopyright

USM_HOME is the documentation convention that specifies the local CA Service Catalog installation directory. For 32-bit computers, the default path name is C:\Program Files\CA\Service Catalog. For 64-bit computers, the default path name is C:\Program Files (x86)\CA\Service Catalog for 32-bit installations or C:\Program Files\CA\Service Catalog for 64-bit installations.

Note: The favorites icon appears in the browser address bar and the product title bar of every product page, including the login page. The favorites icon is a global page element that you can modify.

Note: For the Text elements, the File Name column displays the folder location for an English system (icusen). For other languages, the location is different.

Edit the logon.css file

Modify the look-and-feel of the login page to reinforce branding or other messaging. The same login page applies to all users, regardless of business unit that they are logging in to.

Follow these steps:

1. Open your web browser and access the login page for CA Service Catalog.
2. Back up the USM_HOME\filestore\themes\common\css\logon.css file. *Always* back up CSS files and other configuration files before editing them.
3. Open the file, using the CSS editor for your web browser.
4. Find the lines that control the look-and-feel specification that you want to update.
   For example, to configure the look-and-feel of the product name, find the following line:

```
.loginproductname {
  text-align: left;
  font-family: CAlibri, Verdana, Arial, Helvetica, sans-serif;
  color: #ffffff;
...
```

   To change the color of the product name from the current color to blue, update the lines:

```
.loginproductname {
  text-align: left;
  font-family: CAlibri, Verdana, Arial, Helvetica, sans-serif;
  color: blue;
...
```

5. Repeat the previous step for other look-and-feel changes that you want to make.
   For example, to configure the background color of the login page, find the following lines:

   ```
   .login_page {
     background-color: #00174A;
     text-align: center;
   ...
   ```

   To change the background color of the login page to yellow and align the affected text to the right, update the lines:

   ```
   .login_page {
     background-color: yellow;
     text-align: right;
   ...
   ```

6. Refresh your browser and verify your updates on the login page.

7. Update the elements of the login page (see page 2024) to meet your requirements. Verify each change by saving the file and refreshing the login page.

You have modified the login page.

Modify the Theme

A theme specifies the settings for the following look-and-feel elements:

- Images and icons (*except for* logos)
- Menus
- Tabs
- Toolbars
- Wizards

When applicable, these elements include the following specifications:

- Colors (especially background colors)
- Font name and point size
- Highlighting, such as bold or underline
- Position on a page or dialog

You modify these look-and-feel elements by editing the Cascading Style Sheet (CSS) files for the theme. Each theme includes the following CSS files:

- logon.css, which applies to the login page *only*
- main.css, which applies to other product pages

A theme is organized in folders, with one top-level folder for each theme. In addition to the CSS files, a theme includes several other supporting files and several folders. You do not need to edit these additional files and folders. However, you copy them as a group when you copy and modify a CSS file.

The look-and-feel of the UI matches the theme of the business unit that you are logged in to. If theme is not set for a business unit, CA Service Catalog checks the business unit hierarchy until it finds a theme. Thus, if a business unit does not have its own theme, it uses the theme of its closest parent business unit. You can use the same theme for all business units. Alternatively, you can optionally create and use different themes for different business units.

As an administrator, edit the theme for one or more business units *only* if you have expertise in:

- UI design, especially look-and-feel elements
- Standard specifications for CSS files
- Customization of CSS files, using a CSS file editor for your web browser

To customize a theme:

- Step 1 - Understand Predefined and Custom Themes (see page 2027)
- Step 2 - Create a Custom Theme (see page 2028)
- Step 3 - Change the New Theme (see page 2029)

Step 1 - Understand Predefined and Custom Themes

A theme is organized in folders, with one top-level folder for each theme. In addition to the CSS files, a theme includes several other supporting files and several folders. You do not need to edit these additional files and folders. However, you copy them as a group when you copy and modify a CSS file.

In the USM_HOME\filestore\themes folder, CA Service Catalog includes the following top-level folders for each predefined theme:

- **CA_Technologies_R7**
  Specifies the predefined look-and-feel elements of CA Service Catalog.
- **common**
  Contains look-and-feel elements that apply to *all* predefined and custom themes.

  Important! Do *not* copy and modify the *common* folder.

If you have already created custom themes, your top-level folders for those themes also appear in the USM_HOME\filestore\themes folder.

To create a custom theme, you copy either a predefined folder (such as CA_Technologies_R7) or a custom folder that you created earlier. Afterwards, you modify the CSS file of interest in the folder that you copied.

You store all custom theme folders under the filestore folder. You store them on the same folder level as the CA_Technologies_R7 folder.

Each top-level folder name becomes the name of an option for a theme. When you edit a business unit, you can select a theme for it.

If you update a theme for a specific business unit, the change affects the users who belong to that business unit. The change also affects any child business units that do not have their own theme specified. Child business units inherit the theme of their parent business unit. However, they can optionally override the inherited theme by specifying their own theme.

Step 2 - Create a Custom Theme

You create a custom theme by copying and modifying an existing theme. You can copy and modify either a predefined CA Service Catalog theme or another existing theme that you created earlier.

Important! As a best practice, do *not* modify a predefined CA Service Catalog theme directly. Instead, copy and modify it, so that you can efficiently return to the original version, if necessary. *Always* back up the CSS files before editing them.

Follow these steps:

1. Access the computer on which the filestore resides.
2. Find and expand the USM_HOME folders. Expand the \filestore\themes folder. Review the organization of the predefined and custom themes (see page) in that folder.

   Note: The name of each top-level folder is an option that you can select when you select a theme for a business unit.

3. Copy the top-level folder of existing theme that you want to use as a starting point for your new theme.
4. Rename the new theme.
   For example, suppose that the existing theme was named Rome_Super_Tenant_A. If the new theme is for a second super tenant, you can name it Rome_Super_Tenant_B. Conversely, if the new theme is for a new child business unit of the parent super tenant, you can name it Rome_Super_Tenant_A--Child-1.
5. Add or edit the business unit for which you want to use this theme. In the Available Branding field, select the new theme that you created.
   For example:

- To apply the theme to all business units that do not have their own theme, edit the root business unit and apply this theme.
- To apply the theme to a specific business unit, add or edit the business unit and apply the theme.
  The theme also applies to all child business units that do not have their own theme.

6. Change the new theme (see page 2026) by editing its main.css file.

The new theme is ready for modifications.

Step 3 - Change the New Theme

After you have created a theme, you can change it, to give it a unique look-and-feel.

Follow these steps:

1. Log in to CA Service Catalog and note the look-and-feel of the home page.
2. Back up the main.css file in the custom theme folder that you created (see page). A sample path name is USM_HOME\filestore\themes*custom_theme*\css\main.css file.
3. Open the main.css file of your custom theme. Use a suitable CSS editor for your web browser.
4. Find the lines that control the look-and-feel specification that you want to update.
   For example, To change the background color globally on product pages, perform the following actions:
   a. Find the following default setting:

      ```
      td.pagebg{background-image:url(../images/grid/page-bg.png);background-repeat:repeat-x;background-color:#D9E2F3;}
      ```

   b. Delete the following phrase:

      ```
      background-image:url(../images/grid/page-bg.png);
      ```

      The line now appears as follows:

      ```
      td.pagebg{background-repeat:repeat-x;background-color:#D9E2F3;}
      ```

   c. Change the background-color:#D9E2F3 to the color of your choice, for example, background-color:red.
   d. Save the file.

> **Note:** The setting in this example *does* affect the background color of the *entire* product page. However, the background colors of specific sections of the page *override* the background color of the entire page.

5. Refresh the CA Service Catalog UI. Verify the changes to the product pages.

6. Update other elements of the theme to meet your requirements. Verify each change by saving the file and refreshing the login page. For example, you can customize the look-and-feel of the top-level menu tabs (Home, Service Builder, Accounting, and Administration).

Modify Global Page Elements

Global page elements include both text and icons. The same global page elements apply to all users, regardless of business unit that they are logging in to. The global page elements also apply regardless of whether you have modified the themes of one or more business units.

Global page elements appear on several or all product pages. They include the product name, shopping icon, and footer.

Follow these steps:

1. Back up the USM_HOME\view\webapps\usm\locale\icusen\ includes_shared.xml. *Always* back up XML files and other configuration files before editing them.

2. Open the includes_shared.xml file, using an XML editor.

   Note: The folder location is for an English system (icusen). For other languages, the location is different.

3. Find the line that controls the text that you want to update. For example,

   - Text for the product name: <product_title> value
     Default: CA Service Catalog

4. Update the lines to the values you want, and save the file.

5. Access the folder that contains the icons that you want to update. For example, USM_HOME\view\webapps\usm\images or USM_HOME\view\webapps\root folders contain icons.

   Note: To view an icon, double-click its file name.

6. Perform the following steps for each icon that you want to change:

   a. Rename the original file to filename_OLD.png.

   b. Copy your new file to the folder, and rename it to the original file name.

7. Log in to CA Service Catalog and verify your updates on the product UI.

8. Copy the icons that you customized to the USM_HOME\filestore\custom\images folder.

Important! This step is required to help ensure that your updates apply to all users in your organization.

You have modified the global page elements.

Add a Custom Time Zone

You select the time zone for a business unit when you create or edit it. The time zone selection determines the date and time settings for the business unit, including the following components: the Scheduler, outage calendars, and business hours, date and time fields in forms, and the availability dates for services. You can also select a time zone for conditions in policies. CA Service Catalog supplies several predefined time zones that you can use in these settings. You can add a custom time zone.

Follow these steps:

1. Verify that you have set up the filestore.
2. Copy the appropriate sharedxml.xml file for the language of your system to the filestore. For example, for English, copy the file USM_HOME% \view\webapps\usm\locale\icusen\sharedxml.xml to the filestore.
3. Edit the sharedxml.xml file in the filestore using a text editor. Locate the <timezones> tag and the existing time zone entries under it.
4. Enter the custom time zone under the existing entries. Use the format that is shown in the following example:

```
<t53>
        <id>GMT-06:00 America/North_Dakota/Center</id>
        <text>(GMT-06:00) Central Time (US&amp;Canada)</text>
</t53>
```

5. Verify that the new custom time zone is implemented, as follows:
   - Edit a business unit and verify that the available time zones include the new custom time zone.
   - Set the business unit to this time zone. Verify that the time zone is used in affected components.
   - Verify that this time zone works accurately in conditions in policies, if applicable.

Note: If You have implemented CA Service Catalog in multiple languages, repeat steps 2 through 5 for all other languages.

You have added a custom time zone.

Customize the Online Help

Service delivery administrators can optionally replace the predefined online help with custom online help, for some or all roles. Here, the predefined online help refers to the *CA Service Management Wiki* . Custom online help appears instead of the predefined online help when users with the specified roles click the **Help** button.

Note: If the user selects Administration, Tools, Links, CA Service Management Wiki, the predefined online help *always* appears. Customization for online help does not affect the menu selection that appears when users click the **Help** button.

Follow these steps:

1. Create your custom online help file files and copy them to the USM_HOME\filestore\custom\help\<***language***> folder.

   - ***language***
     Specifies the language of the operating system on which you installed CA Service Catalog. For example, specify en_US for U.S. English or ja_JP for Japanese.
     For example, the file location for your custom English help files must be USM_HOME\filestore\custom\help\en_US folder.

   Note: The folder must include an index.html file that, when clicked, opens the custom online help.

2. Click **Administration**, **Configuration**, **Filestore**.
3. Select the option that is named **Enable Custom Help**.
4. Specify the roles that must see the custom help rather than the predefined online help.
5. Restart Catalog Component.
6. Verify that CA Service Catalog functions as expected when users with the specified roles click the **Help** button:

   - If applicable, the custom online help opens instead of the predefined online help.
   - If the index.html file does *not* exist in the USM_HOME\filestore\custom\help\<***language***> folder, the index.html file in the USM_HOME\filestore\custom\help\default folder runs. The predefined online help opens.

- If the custom online help is disabled, the predefined online help opens.

Use Web Services to Automate Business Processes

Administrators can use the CA Service Catalog web services to automate business processes and to reduce manual input by catalog users. You can access the web services from any client that uses standard web service protocol.

A web service is any collection of software operations or methods that is available over the Internet. A web service uses a standardized XML messaging system. The web services use XML to encode all communications: A client invokes a web service operation by sending an XML message and then waits for a corresponding XML response.

CA Service Catalog includes several predefined web services. For example, the UserService web service provides a *getUser* method and an *editUser* method that you can use to manage information about users. The BusinessUnitService web service provides similar functionality for business units. This set of web services constitutes an application programming interface (API) for CA Service Catalog.

The web services use Simple Object Access Protocol (SOAP). SOAP is a lightweight, XML-based communication protocol and encoding format for inter-application communication.

The CA Service Catalog implementation of SOAP is Axis-compliant. You can access the web services from any Axis-compliant client. Implementers can use any programming language with which they are familiar to call exposed methods, using method call syntax. Implementers must be skilled users of the web services of the programming language they select.

The web services support the Web Service Description Language (WSDL). You can use WSDL to build stubs to access remote services. You can also use WSDL to export automatically machine-readable descriptions of CA Service Catalog deployed services from Axis.

Important! For more information about how to use the web services, log in to CA Service Catalog and click Administration, Tools, Links, Web Services API. The API documentation is automatically generated Java documentation that is based on the CA Service Catalog web service methods. Alternatively, to access this documentation, click Start, Programs, CA, Service Catalog, Documentation, Web Service API on the Catalog Component computer.

Follow these steps:

Step 1 - Verify the Prerequisites for Clients

Clients must meet the following prerequisites to call CA Service Catalog web services:

- Verify that you are using apache Axis 1 for your web service implementation.
- Axis clients require a Web Service Description Language (WSDL) file for the initialization.
- Verify that a WSDL file is generated for each web service when the Axis server is initialized. The WSDL file for a web service is updated each time when the service is dynamically deployed or undeployed successfully.
  A WSDL file is required for each web service. Typically, when a web service is made available using Axis, a unique URL is associated with that web service. The URL name is typically http://localhost:8080/usm/services/*webservice*. An example is http://localhost:8080/usm /services/UserService for the web service named UserService.
  Name your WSDL files using the convention *webservice*.wsdl, where *webservice* is the name of the web service.
- Verify that each WSDL file contains the information, including method signatures, required to call currently deployed services. The WSDL files help you to differentiate the following parts of a service:
  - Abstract functionality description
  - Concrete details description, such as message format and communication protocol. Examples include SOAP, HTTP, and MIME.

  Thus, you can reuse a WSDL file for different types of clients.
- If you use a Java program to call the methods, verify that the following jar files are in the class path. These files are installed in USM_HOME/webapps/usm/WEB-INF/lib:
  - axis.jar
  - jaxrpc.jar
  - commons-logging.jar
  - commons-discovery.jar
  - wsdl4j.jar
  - mail.jar

Step 2 - Deploy Web Services

To make a web service accessible to a client application, deploy the web service. After you deploy, enable the method on the server. An authenticated user with proper permissions can deploy and undeploy services dynamically when the server starts.

By default, the Catalog system deploys all web services and their methods. With the proper login credentials, a client application has access to all web services functionality. If you decide to undeploy a web service, check if any client applications use it. Therefore, undeploying a web service can affect request approval and fulfillment business processes.

When a web service is deployed or undeployed, the WSDL file for the web service is updated. Each web service has its own WSDL that contains the information about currently deployed services, including method signatures. The URL format for the web service follows:

```
http://hostname:port/usm/services/servicenameService?wsdl
```

- ***hostname*:*port***
  Specifies the Catalog Component server name and port number.

- ***servicename***
  Specifies the web service name.

For example, in your browser address field, you enter:

```
http://prod123:8080/usm/services/UserService?wsdl
```

The results display the following data:

- The WSDL contents for a Catalog Component server named “prod123” on port 8080
- All web service methods and data structures for the User web services, in XML format

Note: You can also remotely invoke methods of the Axis server at runtime through an Axis-compatible client.

Step 3 - Generate the WSDL File

Generating the WSDL file for each web service is required when you call web services with a Java client.

Follow these steps:

1. Access the web service URL in a browser.
   You typically see a message referencing an Axis service and SOAP access.

2. Append **?wsdl** to the URL.
   Axis generates a service description for the deployed service and returns it as XML in the browser, for example:

   ```
   http://localhost:8080/usm/services/AccountService?wsdl
   ```

3. Save the output as a file named *webservice*.wsdl. Record the path name for future reference.

Use the webservice.wsdl file as input to web service calls (proxy-generation) when you generate java stubs for each web service.

Step 4 - Generate Java Stubs

Generating Java stubs for each web service is required when you call web services with a Java client.

Follow these steps:

1. Verify that you are using the Axis WSDL2Java tool for generating the Java stubs.

   Note: You can obtain the Axis tools from the Apache Axis website (apache.org).

2. Open a command prompt and enter the command to generate Java stubs. Use the following command as a model.

   ```
   java org.apache.axis.wsdl.WSDL2Java -o . -ptesting.soap AccountService.wsdl
   ```

   This action generates the following files in the package named testing\soap:

   - *web_service_name*Impl.java
     This new interface file contains the appropriate java.rmi.Remote usages.
   - *web_service_name*ImplService.java
     This file is the Service Interface of the web service. The Service Locator implements this interface.
   - *web_service_name*ImplServiceLocator.java
     This file is the Helper factory to retrieve a handle to the service.
   - *web_service_name*SoapBindingStub.java
     This file is the client-side stub code that encapsulates the client access.
   - Serialized beans
     These beans function as input and return types. They also catch exceptions.

3. Verify that the command generated files like the ones in the previous step.

Step 5 - Call each Web Service

This article contains the following topics:

Use a Java Program to Call a Web Service

The Java-related specifications and parameter-related specifications are specific to your program. For more information, see the Axis and web service related-related sections of apache.org website.

Use a JavaScript Program to Call a Web Service

Developers can access web services directly through JavaScript programs. This ability enables web programmers and system administrators to invoke methods remotely through DHTML or Windows Scripting Host. The ability to call web services through client-side scripting gives web developers greater flexibility to create dynamic web sites.

For more information, see the web service-related portions of the workshop sections of the Microsoft Developer Network (MSDN).

Follow these steps:

1. Review the following sample files and use them as models to create your own programs. These files reside at:
   USM_HOME\ view\webapps\usm\admin
   - soapTest_index.html
   - soapTest_bottom.html
   - soapTest.html. This file contains the JavaScript code to call web service.

   The sample files provide a sample HTML that gets the list of all accounts for a business unit, using synchronous method calls.

   Note: The sample files support both synchronous and asynchronous method calls. When you use asynchronous calls, the web browser does not lock during calls and responds to user input.

2. Open the soapTest_index.html file in your browser.

3. Complete the fields and run the file.
   The file runs and calls the web service. The page dynamically creates an HTML table with the list of accounts.

Step 6 - (Optional) Specify Special Characters

If necessary, your web service calls can include special characters, as explained in the sections that follow.

Select Special Characters

Important! This section applies only if the special character does *not* function as a separator for the parameter in the web service call.

You can use the following XML character entities to specify special characters in web service calls:

- & (ampersand)
- ' (apostrophe)
- " (double quotation mark)
- < (less than)
- > (greater than)

For example, use the following entities to specify the business unit named Smith&Jones Hardware&Software Supplies:

```
Smith&amp;Jones Hardware&amp;Software Supplies
```

Special Characters Other Than Separator Characters

Important! This section applies only if the special character does *not* function as a separator for the parameter in the web service call.

To use CDATA tags to specify special characters in web service calls, use the following format:

```
<![CDATA[...]]>
```

For example, use the following expression to specify the business unit named Smith&Jones Hardware&Software Supplies:

```
<![CDATA[Smith&Jones Hardware&Software Supplies]]>
```

Separator Characters

The following special characters are typically used as separators:

- | (vertical bar)
- ! (exclamation point)

If the special character functions as a separator for the parameter in the web service call, specify the special character as a dynamic variable:

1. On the CA Service Catalog UI, enter the special character or characters in the field that you reference in the web service call. For example, in the Description field for the current business unit, enter !&.

Note: Dynamic variable can also handle other special characters (for example, & and ,) although they are not separators for web service methods.

2. In the web service call, replace the special character with the dynamic variable for the field of previous step. For example, $bu.description$.

The following sample web service call uses the example from the previous steps:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="
http://www.w3.org/2001/XMLSchema" xmlns:soapenv="http://schemas.xmlsoap.org/soap
/envelope/" xmlns:ser="http://services.soap.usm.ca.com">
   <soapenv:Header/>
   <soapenv:Body>
      <ser:saveRequestForm soapenv:encodingStyle="http://schemas.xmlsoap.org/soap
/encoding/">
         <sessionID xsi:type="xsd:string">e2f6b05b85247d35b4d7371edc9c6fe398fba60d<
/sessionID>
         <subscriptionDetailID xsi:type="xsd:int">10009</subscriptionDetailID>
         <formValuesData xsi:type="xsd:string">text1:M$bu.description$<
/formValuesData>
      </ser:saveRequestForm>
   </soapenv:Body>
</soapenv:Envelope>
```

Step 7 - Clients Invoke Login and Logout Methods

When you call web services with a Java client, a required process is clients invoking login and logout methods for each web service. A typical process follows:

1. The client uses a method for login and authentication.
   Each web service has a set of login methods. The client applications can use several login methods for authentication. For example, the *logIn* method takes the same parameters as the Login window: User ID, Password, and Business Unit.
   To view the method parameter information, including signatures, use the following resources:

   - Web Services API documentation.
     To access the Web Services API documentation, log in to CA Service Catalog, click Administration, Tools, Links, Web Services API.

   - SOAP administration interface for deploying or undeploying web services

2. The Catalog system authenticates the user and determines its role.
   Subsequent method calls operate within the scope of the access rights of the user.

3. The client:

   - States the service that it is calling.

   - Provides the method name and its corresponding parameters before initiating the remote procedure call.

   - Checks the WSDL file for this information, if it is unknown.
     Typically, the client already has this information.

4. The web service returns a session ID. This session ID is a required parameter that the client uses for the remaining web service calls. Because the underlying transport protocol can be either HTTP or non-HTTP, the authentication uses a common logIn web service.
   You can share the session ID across web services. For example, you can use the UserService logIn method to obtain a session ID. You can then use the session ID in a call to a Business Unit web service method.

5. This session ends when one of the following events occurs:

   - The client calls the logOut web service method.
     Once you are finished using a session ID, you call the *logOut* web service to terminate the session. The *logOut* web service also invalidates the session ID. Managing the sessions efficiently in this manner helps you obtain the best product performance.

   - The client is idle for a period longer than the session timeout value.
     The client can use the session ID repeatedly within the timeout period. If the session times out, the session ID becomes invalid.
     To change the timeout value, update the administration configuration setting named User Default: Session Timeout.

Step 8 - Add Attachments to Requests

Administrators can use the addRequestAttachmentWithPath web service as an automated, efficient, and reliable mechanism for adding attachments to requests.

Use the following options to use this web service to add attachments to requests:

- Add attachments stored by CA Service Catalog (see page 2040).
- Add attachments stored by a WEBDAV (see page 2042).
- Add attachments using an absolute path (see page 2043)

Add Attachments Stored by CA Service Catalog

You can optionally attach files to requests when the files are stored using the Document Management feature of CA Service Catalog. To do so, follow this process:

1. Enable the Document Management feature.

2. Attach the file.

Enable the Document Management Feature

Perform this procedure once.

Follow these steps:

1. Disable the following policies in CA EEM : ACL_deprecated_features_launchpads and ACL_deprecated_features_guinodes.

Note: For more information about how to disable policies in CA EEM, see your CA EEM documentation.

2. Restart CA Service Catalog.

3. Verify that the Home, Documents menu is enabled.

Note: The following menu options are also enabled when you disable the CA EEM policies: Home, Reports and *both* Offline Data Views *and* Offline Layouts under Administration, Report Builder.

Attach the File

Perform this procedure each time that you want to attach a file to a request using web services.

Follow these steps:

1. Click Home, Documents. Upload the file that you want to use as an attachment.

2. Call the web services that use addRequestAttachmentWithPath and pass the values that you want to the input parameters.
   Use the following format for the attachmentPath parameter:

   ```
   http://username:password@computername:port/usm/documents/pathname
   ```

   - ***username* and *password***
     Specifies one of the following options:

     - The user name and password of the user who uploaded the documents
     - A user with the Service Delivery administrator role

   - ***pathname***
     Specifies the subfolder pathname (under the documents folder) of the file being uploaded, including its extension.

Examples

The following example attaches a file from the Documents folder:

```
http://spadmin:spadmin@computer-abc:8080/usm/documents/test.txt
```

The following example attaches a file from a subfolder of the Documents folder:

```
http://spadmin:spadmin@computer-xyz:8080/usm/documents/WSAttachments/test.txt
```

Add Attachments Stored by a WEBDAV

You can attach files to requests when the files are stored using a third-party web-based distributed authoring and versioning (WEBDAV). A sample WEBDAV is Microsoft Internet Information Server (IIS). To do so, follow this process:

1. Enable WEBDAV functionality.
2. Attach the file.

Enable WEBDAV functionality

Perform this procedure *once*.

Follow these steps:

1. Edit the following section in the web.xml file:

```
<init-param>
  <!-- web dav is disabled as of 12.8 to enable change the flag and restart -->
  <param-name>disableWebDav</param-name>
  <param-value>true</param-value>
</init-param>
```

2. Change the value of the WebDav parameter from *true* to *false*.
3. Restart CA Service Catalog.

Attach the File

Perform this procedure *each time* that you want to attach a file to a request using a WEBDAV.

Follow these steps:

1. Pass the HTTP URL of the attachment.
2. Call the web services that use addRequestAttachmentWithPath and pass the appropriate values to the input parameter.
3. Use the following format for the attachmentPath parameter:

```
http://computername/websharefoldername/filename
```

   - ***computername***
     Specifies the name of the computer from which you are adding the attachments.
   - ***websharefoldername***
     Specifies the name of the new folder.
   - ***filename***
     Specifies the file name of the attachment, including the extension for example, test.txt.

Add Attachments Using An Absolute Path Name

You can optionally attach files to requests by using the absolute path name of the file.

Follow these steps:

1. Verify that the attachment is stored on the CA Service Catalog computer. If necessary, copy or move the attachment to meet this requirement.

2. Call the web services that use addRequestAttachmentWithPath and pass the values that you want to the input parameters. Pass the absolute path name of the attachment, for example: C:\\TEST\\test.txt.

Use API Plug-ins to Load Data into Policies and Forms

This article contains the following topics:

Administrators and service designers work together to write API plug-ins that dynamically load data into policies and forms, as follows:

- For a policy, this data specifies the assignees (approvers) for a request. You use the plug-in instead of specifying assignees manually using the Action Builder. When a user submits a request, the API plug-in dynamically specifies the assignees.

- For a form, this data specifies the value for any of the following fields: dynamic tables, dual lists, or select boxes and their options. For example, when a user completes a form to reserve a virtual computer, the report data object populates the list of available computers. You can also write other report data objects to populate related fields, for example, options for RAM and disk space.

API plug-ins query the MDB or another data source. The API plug-in returns the number of objects that meet the criteria that you specify. You can either write your own API plug-ins or copy and modify the predefined plug-ins to meet your requirements. In both cases, you meet the prerequisites and compile your plug-ins *before* you can use them.

API plug-ins are deployed as jar files in the plugins directory of the filestore. API plug-ins run in the same Java Virtual Machine instance as CA Service Catalog.

Perform the tasks that apply:

- Use API plug-ins for policies (see page)

- Use API plug-ins for forms (see page)

Use API Plug-ins for Policies

To write and use an API plug-in for policies, follow this process:

1. Define the purpose or goal of the plug-in.
   An API plug-in is useful when you query an external system for data to specify the assignees. An API plug-in is also useful when the identities vary according to the data in the request. Based on this data, the plug-in dynamically creates the assignee list and specifies the assignee levels.

2. Meet the prerequisites:

3. Be able to do the following proficiently:

   - Program in Java.
   - Create policies, including conditions, and understand the types of assignees required.

4. Review the API Plug-in documentation, as follows:

   a. Select Administration, Tools, Plug-ins.

   b. Click API Documentation.

   c. Review the com.ca.usm.plugins.apis.policies package.

   The API documentation is automatically generated Java documentation from the Java class methods for the plug-ins. You use the interfaces, classes, methods, and so on, to implement your plug-in.

5. Download and review the sample API plug-in for policies, as follows:

   a. Select Administration, Tools, Plug-ins.

   b. Click the Sample Policy Plug-in, review the details, and download the source code.

   c. Open and review the SamplePolicyPlugin.java file in the \src\java\com\ca\usm\plugins\samples\policy folder. Use this sample policy plug-in as a model.

6. Create a Java class that implements the interface, com.ca.usm.plugins.apis.policies. AssignmentPolicyPlugin. The sample policy plug-in illustrates how to implement this interface.

7. (Optional) If you use content configuration forms, retrieve values from the fields on these forms. Use the forms as needed.

8. Create a properties file for the plug-in. You can use the plugin.properties file in the sample policy plug-in as a model for your properties files.

9. Create a folder to store the properties file and any JAR files that provide the classes and supporting libraries.

Important! Store the properties file at the *top* level of the folder. Do *not* store the properties file in a subfolder.

10. Activate the plug-in:
    a. Stop the CA Service Catalog Windows service.
    b. Copy your folder (including all subfolders, if any) to the USM_HOME\filestore\plugins folder.
11. Start the CA Service Catalog Windows service.
12. Verify that the plug-in was successfully adopted:
    a. Select Administration, Tools, Plug-ins.
    b. Verify that the plug-in is listed and that its details appear properly.
13. Test this plug-in:
    a. Use it to specify assignees for a policy.
    b. Submit a request that activates the policy and verify that the policy assigns approvers dynamically as intended.

Use API Plug-ins for Forms

To write and use an API plug-in for use in a form, follow this process:

1. Define the purpose of the plug-in. For example, to populate a select field with meeting rooms that a user can reserve for a specified time period. Other examples include options for the meeting room, such as projectors, video conferencing units, and microphones.
2. Meet the prerequisites. Be able to do the following proficiently:
   - Program in Java.
   - Create forms using the Form Designer.
   - Create the following fields in Form Designer forms:
     - Single select, multi-select, and dual list fields
     - Dynamic table fields
3. Review the API Plug-in documentation, as follows:
   a. Log in to CA Service Catalog and select Administration, Tools.
   b. Select Links.

c. Click Plug-in Documentation.

The API documentation is automatically generated Java documentation from the Java class methods for the plug-ins. You use the interfaces, classes, methods, and so on, to implement your plug-in.

4. Create a Java class for the type of Form Designer field for which the plug-in applies, as follows:

   - For single select, multiselect, and dual list fields: Create a Java class that implements the com.ca.usm.plugins.apis.forms.FDSelectDataProvider interface. A sample implementation of this interface is provided in the Sample Select Plug-in, with id ca.catalog.samples.select-plugin.

   - For dynamic table fields: Create a Java class that implements the com.ca.usm.plugins.apis.forms.FDTableDataProvider interface. A sample implementation of this interface is provided in the Sample Table Plug-in, with id ca.catalog.samples.table-plugin.

   To access Java documentation for the interfaces, click Administration, Tools, Plug-ins, and click API Documentation.
   To download sample source code, click the sample plug-ins on the same page and click Download Source Code.

5. Create a properties file for the plug-in, as follows:

   - Use the sample plug-ins as models for your properties files. In that case, change the plug-in id property in the plugin.properties file.

   - Use the Java Development Kit 1.6 (or higher) and Apache Ant 1.8 (or higher) to use the included build file to compile the plug-in.

   - Use a private classloader for your plug-ins. To use a private classloader, add the following line to your plugin.properties file:

     ```
     classloader.type=private
     ```

     Note: Custom plug-ins from CA Service Catalog Release 12.7 do *not* require any updates after you upgrade CA Service Catalog. These plug-ins continue to function as they originally did.

6. (Optional) If you use content configuration forms, retrieve values from the fields on these forms. Use the forms as needed.

7. Perform the actions that apply:

   - Configure Pagination Parameters for Select Fields.

   - Configure Attributes for Select Boxes Only.

   - Configure Sorting and Pagination Parameters for Dynamic Tables.

8. Create a folder to store the properties file and any JAR files that provide the classes and supporting libraries.

   Important! Store the properties file at the *top* level of the folder. Do *not* store the properties file in a subfolder.

9. Activate the plug-in:

   a. Copy your folder (including all subfolders, if any) to the plugins folder of the filestore.

   b. Select Administration, Tools, Plug-ins, and click the Reload Plugins method.

10. Verify that the plug-in was successfully adopted:

    a. Log in to CA Service Catalog and select Administration, Tools.

    b. Select Plug-ins.

    c. Verify that the plug-in is listed and that its details appear properly.

You are ready to test this API for use in a form field.

Configure Pagination Parameters for Select Fields

Your plug-in can return a large amount of data in a select field on a form. In that case, you often specify the page size of the results in the select field. An example is displaying ten results per page in the select field. To accomplish this task, configure the parameters for pagination in the related Java class and object.

Follow these steps:

1. Edit the Java class that implements the interface, com.ca.usm.plugins.apis.forms. FDSelectDataProvider. Implement the following method in FDSelectDataProvider:

   ```
   List<FDOption> getOptions(int start, int numToReturn);
   ```

   - **start**
     Specifies the first row to return. This parameter is an integer.

   - **numToReturn**
     Specifies the number of rows to return. This parameter is an integer.

   This method returns a list of FDOption objects:

   - The key value pair (id and value) in a report data object for the options of the select field.

   - Data that complement the key value pair. You can optionally display this additional data in other fields (except the select field) on the form.

The value of the _id attribute of each field must match the one of the keys in the additional data.

2. Also in FDSelectDataProvider, implement the following method:

```
int totalCount();
```

This method returns the total number of rows that exist.

Note: For more information and examples, see the API plug-in documentation.

Configure Attributes for Select Boxes Only

Some HTML Attributes apply to select boxes only. For more information, see the Attributes for Select Boxes Only (see page 2934) section.

Configure Sorting and Pagination Parameters for Dynamic Tables

Your plug-in can return a large amount of data in a dynamic table in a form. In such a scenario, you specify the page size of the results. An example is displaying ten results per page on the form. Similarly, you often want to let users sort the results on each page in ascending or descending order. To accomplish both tasks, configure the parameters for sorting and pagination in the related Java class and object.

Follow these steps:

1. Click Catalog, Forms, and open the form of interest.

2. Open the table and verify that the attribute named Sortable is set to True.
If this attribute is enabled (True), then users can click arrows on the table column headers to sort the results.

3. Edit the Java class that implements the interface, com.ca.usm.plugins.apis.forms.FDTableDataProvider. Implement the following method in FDTableDataProvider:

```
List<FDTableRow> getTableRows(int start, int numToReturn, String sortField,
boolean sortAscending);
```

Users determine these values by interacting with the form, for example, by clicking to view the next page.

- **start**
Specifies the first row to return. This parameter is an integer.

- **numToReturn**
Specifies the number of rows to return. This parameter is an integer.

- **sortField**
  Specifies the rows to sort. When the value is null, no sorting occurs. This parameter is a string.

- **sortAscending**
  Specifies whether to sort the results in ascending or descending order. This parameter is Boolean.

This method returns FDTableRow objects, which are described in a later step.

4. Also in FDTableDataProvider, implement the following method:

```
int totalCount();
```

This method returns the total number of rows that exist.

5. Use the FDTableRow object and its methods to return table row data. You can use the following methods:

- **public void setColumnValue(String columnId, String data)**
  Specifies the following to set the value for a column:
  - String columnid - Specifies "_id" attribute of a component of a table.
  - String data - Specifies a value that you can parse and place into the field on the table.
- **public String getColumnValue(String columnId)**
  Specifies the matching GET function for the previous SET function (public void setColumnValue).
- **public Set getColumns()**
  Returns the set of column IDs stored in this object.

Note: For more information and examples, see the API plug-in documentation.

Using

Audience: IT Analysts, Knowledge Managers, Configuration Administrators, Configuration Managers, Asset Managers, Service Designers

CA Service Desk Manager

CA Service Catalog

CA Asset Portfolio Management

Vendor Management (see page 2457)

Common Capabilities

Reporting (see page 3180)

Mobility (see page 3156)

Self-Service (see page 3244)

Working with Problems

This article contains the following topics:

Problems are difficulties encountered when following normal procedures. Records of problems are recorded, along with the steps taken to correct the problems. If you create a ticket as a copy of another ticket, the Status field displays all Status values.

Important! Unless otherwise noted, all the CA SDM Request features are also available for Incidents and Problems.

Note: Depending on your role, you may not have access to all the functionality described in this section. For example, some predefined roles can edit records but cannot create records.

Create a Problem

You can create a new problem either using a template or without using a template.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. Do one of the following steps:
   - On the Service Desk tab, select File, New Problem.
   - On the Service Desk tab, select File, New Problem from Template.
2. Complete the Problem Fields (see page 2052) as appropriate for the problem.
3. Use the controls available on the problem tabs (see page) to process the problem as appropriate.
4. Click one of the following buttons:
   - **Use Template** -- Displays a list of available problem templates. Select the template you want to use for creating this problem.
   - **Quick Profile** -- Displays the contact information for the user entered in the Affected End User field. If you are creating a new problem, a list of available users appears. Select the user that is the Affected End User.
   - **Find Similar** -- Opens the Find Similar page to search for similar problems.
   - **Create Change Order** -- Opens the Create New Change Order window so you can create a change order ticket associated with this problem.

Problem Fields

The following fields require explanation to create or update a problem:

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

- **Problem Reference Number**
  This is a unique reference number assigned by CA Service Desk Manager for all problem tickets. This is used by analysts and customers to refer to a particular problem ticket.
- **Requester**
  Specifies the name of the person who initiated the ticket. This person must be a defined contact. You can enter a value directly or click the magnifier to search for the name.
- **Affected End User**
  Specifies the contact name of the person who is affected by the record. If the contact is assigned to a special handling type, special handling indicators are displayed. You can enter a value directly or click the magnifier to search for a contact name.
- **Problem Area**
  Indicates the general area of your IT environment that is affected by the problem (for example, Applications, E-mail, Hardware, and Software). A problem area provides default values that are

entered automatically on all problem tickets that are assigned to the area. In addition to the predefined problem areas, your system administrator can define custom problem areas. You can enter a value directly or click the magnifier to search for a problem area.

Note: Your system administrator has the option of adding custom properties to problem areas. If custom properties have been added, they are displayed on the Properties tab when you create, edit, or view a problem. Some custom properties require that you enter a value.

- **Status**
  Specifies the status code of the record. For example, you can list only the tickets with a status code of Fix in Progress, or can Close Requested. You can enter a value directly or click the magnifier to search for a status. The blue button (on the left side of the Status field) lets you change the current status to the next default status.

- **Priority**
  Specifies the priority ranking of the record. The ranking determines the amount of attention the ticket receives. The predefined priority levels are 1 (highest) through 5 (lowest). Your system administrator or an active priority calculation can generate the appropriate Priority values for various installations and tenants. When priority calculation is enabled, this field updates based on Impact, Urgency, Affected Service, and Affected User settings. When your administrator disables priority calculation and uninstalls the urgency_on_employee option, Self Service Users see the Priority field on the Request Detail page.

Detail Fields

- **Reported By**
  Specifies the name of the person reporting the record.

- **Assignee**
  Specifies the name of the person who is assigned to handle the record. You can enter a value directly or click the magnifier to search for a name. Selecting an assignee populates the groups that the assignee belongs to in the **Group** field.

- **Group**
  Specifies the group that is responsible for this record. Your system administrator defines groups of contacts that are responsible for different types of issues, requests, incidents, or problems. Any contact who is part of the group can handle the record after it is assigned to the group. You can enter a value directly or click the magnifier to search for a group. Selecting a group populates the **Assignee** field with the corresponding assignee name, which belong to the group.

- **Urgency**
  Specifies the urgency of the record. The urgency is determined by the importance of the user tasks that are affected by the record. Urgency codes indicate the importance of a ticket based on the degree to which it affects user tasks. For example, a network outage is more urgent than a printer failure. Your system administrator can modify the default urgency codes, so they can vary from one installation to another. Urgency values can update automatically based on an active priority calculation.

- **Impact**
  Specifies an impact code, such as 1 - Entire Organization, that indicates how a ticket affects the work being performed. For example, a ticket that requires a network outage for several hours would have a higher impact than a ticket that takes a printer off-line. Your system administrator can modify the default impact codes, so they can vary from one installation to another.

- **Active**
  Indicates whether the record is Active or Inactive. This value applies to the current record only, not the associated template.

- **Configuration Item**
  Specifies the hardware, software, or service that is affected by the record. Your system administrator creates a record that uniquely identifies each configuration item for your organization and indicates its precise location. You can enter a value directly or click the magnifier to search for an item.

- **Charge Back ID**
  Specifies the ID that is charged for the service.

- **Call Back Date/Time**
  Specifies the date and time to follow up on this record. You can enter the date and time in the format mm/dd/yyyy hh:mm am | pm, or click the calendar icon to open a calendar window where you can select the date and time for follow-up.

- **Symptom**
  Specifies a code that describes a primary symptom of the record. For example, Slow Response.

- **Root Cause**
  Identifies the code associated with the core reason why the ticket was opened. Your service desk can use generic root cause codes, such as Hardware Failure or Software Failure, or more specific codes, such as Network.Cable, Network.Card, or Network.Response. You can enter a value directly or click the magnifier to search for a code.

- **Change**
  Specifies the number and name of the change order that is associated with this record. Enter the number or name of the change order directly in this field.

- **Caused by Change Order**
  Specifies only tickets that were opened as a result of a specific change order ticket. You can enter a value directly or click the magnifier to search for a change order ticket.

- **External System Ticket**
  Specifies an identification for a ticket that belongs to an external system that integrates with CA SDM. This field stores hyperlinks and displays functional links in read-only mode.

- **Timer**
  Tracks the incremental amount of the time spent working on various phases of ticket processing. The timer is reset to 00:00:00 each time you open the ticket record for updates. You cannot edit this field.

> **Note:** The amount of time that is spent on each activity is shown on the Activities tab of the ticket record.

- **Action**
  Sets or resets the Actual Date/Time to the current date and time.

- **Target**
  Specifies the current Service Target.

- **Target Date/Time**
  Specifies date and time when this Service Target is due. If the ticket is in a Hold status, this value is blank.

- **Actual Date/Time**
  Specifies the time when the target condition was met. If no value appears, the target condition has not been met.

- **Time Left**
  Specifies the amount of remaining time for the service target when the ticket is on hold. If the Service Target has been met, Time Left shows the unused time. A negative value indicates the time that elapsed since the missed target date.

- **Violation Cost**
  Specifies the incurred cost when the service type time limit is violated.

- **Affected Service**
  Specifies the primary service that affects the problem or incident. The CIs of type Service have a class that is defined in the Enterprise Service Family field. The ticket stores the currently affected service information in the ticket for reporting. You can enter a value directly or click the magnifier to search for a CI.

- **Affected End User**
  Specifies the contact name of the person who is affected by the record. If the contact is assigned to a special handling type, special handling indicators are displayed. You can enter a value directly or click the magnifier to search for a contact name.

- **Priority**
  Specifies the priority ranking of the record. The ranking determines the amount of attention the ticket receives. The predefined priority levels are 1 (highest) through 5 (lowest). Your system administrator or an active priority calculation can generate the appropriate Priority values for various installations and tenants. When priority calculation is enabled, this field updates based on Impact, Urgency, Affected Service, and Affected User settings. When your administrator disables priority calculation and uninstalls the urgency_on_employee option, Self Service Users see the Priority field on the Request Detail page.

- **Summary**
  Provides a brief description of the record.

- **Description**
  Describes the record in detail.

- **Last Modified Date/Time**
  Displays the date that this ticket was last modified.

- **Last Modified By**
  Displays the name of the last person who edited the ticket.

- **Ticket Open Date/Time**
  Displays the date and time the ticket was opened.

- **Ticket Resolved Date/Time**
  Displays the date and time the ticket was resolved.

- **Ticket Closed Date/Time**
  Displays the date and time the ticket was closed.

- **Created Via**
  Specifies the component reporting the record (detail_pr.htmpl).

Problem Tabs

The following tabs are available on the Create New Problem, Problem Detail, and Update Problem pages:

- **Activities:** Displays a log of the activities performed to resolve the problem. For more information, see Add an Activity from the Ticket Management (see page 2308) topic.

- **Event Log:** Displays a record of significant actions that occur regarding the problem.

- **Attachments:** Allows you to attach a document or a link to a URL to the problem.

- **Workflow Tasks:** Lists the process instance and related audit trail messages for a CA Process Automation, or Classic Workflow that is associated with the ticket. The Workflow Tasks tab shows fields that apply to an attached workflow. The workflow may require some of the work items to complete before the ticket can close. The Workflow Tasks tab appears only if your administrator configured workflows for the ticket area or category. For more information, see Define a Category or Area (see page 1054) topic.

- **Service Type:** Allows you to attach a service type event (see page 2313) to indicate the level of support for the ticket.

- **Attached Incidents:** Allows you to view a list of any incident tickets attached to the problem ticket.

- **Knowledge:** Allows you to search for or submit information to the CA SDM Knowledge Base to help resolve problems. The Federated Search capability helps you to get the knowledge search results from multiple sources. For example, Google, SharePoint, CA Open Space, and so on.

- **Solutions:** Allows you to store information about the problem solution with the problem record for future reference.

- **Parent / Child:** Allows you to create a parent/child relationship between the problem and another CA SDM record.

- **Properties:** Your CA SDM administrator can add custom properties to problem areas.
- **Templates:** Allows you to create a template (see page 2315) using the current ticket as a model.

Create a Problem from an Incident

From an incident, you can create an associated problem if necessary.

Follow these steps:

1. From the Incident Detail Page, click Create Problem.
   The Create New Problem page displays. The fields are filled with the values from the original incident, but they can be edited for the problem. See the Problem Fields (see page 2052) as appropriate for the problem.

2. Use the controls available on the problem tabs (see page) to process the problem as appropriate.

3. Click one of the following buttons:

   - **Use Template** -- Displays a list of available problem templates. Select the template you want to use for creating this problem.
   - **Quick Profile** -- Displays the contact information for the user entered in the Affected End User field. If you are creating a new problem, a list of available users appears. Select the user that is the Affected End User. For more information about Quick Profile, see the Ticket Management (see page 2308) topic.
   - **Find Similar** -- Opens the Find Similar page to search for similar problems.
   - **Create Change Order** -- Opens the Create New Change Order window so you can create a change order ticket associated with this problem.

Issue Management

Contents

Issues are entered by customers when they encounter questions or difficulties when following normal procedures. Records of issues are recorded, along with the steps taken to correct the issues. If you create a ticket as a copy of another ticket, the Status field displays all Status values.

Create an Issue

You can either create an issue from scratch or use an existing template.

Important! Depending on your role, you do not have access to all the functionality described in this section. For example, some predefined roles can edit records but cannot create new ones.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Service Desk tab, select File, New Issue.
2. Fill in the issue fields (see page)as appropriate for the ticket.
3. Use the controls available on the tabs (see page)to process the ticket as appropriate.
4. Click one of the following buttons:

   Auto Assign -- Triggers an auto assignment task, and updates the activity log. This button appears only when the ticket specifies a category or area that has auto-assignment enabled.

   Find Similar -- Opens the Find Similar page to search for similar problems.**Quick Profile --** Displays the contact information for the specified user in the **Affected End User** field. You can also view their environment details and their entire ticket history.

   Use Template -- Displays a list of available templates for the selected ticket type. You can select the template that you want to use for creating this ticket.

Note: You can use the Quick Profile to identify a contact to be the affected end user of your new ticket. Quick Profile allows you to search for a contact, and view the history of the issues, requests, change orders, incidents, and problems that are assigned to that contact. When you have identified a contact, you can create the incident ticket directly from the Quick Profile.

Issue Fields

The following fields require explanation:

- **Affected End User**
  Specifies the name of the person affected by the record. You can enter a name directly or click the magnifier to search for a contact.

- **Category**
  Indicates the general category of the issue within your IT environment (for example, Hardware.pc. install and Software.pc.install). Issue categories provide default values that are entered automatically on all issue tickets assigned to the category. In addition to the predefined issue categories, your system administrator may define custom issue categories. You can enter a value directly, or click the Lookup icon to select from the defined categories. When you edit the Category and a CA Process Automation workflow is already running, the workflow cancels.

- **Status**
  Specifies the status of the record. You can enter the status directly or click the magnifier to search for a status.

- **Priority**
  Specifies the priority ranking of the record, determined by the amount of attention it should receive. Your system administrator can modify the default priority codes, so they can vary from one installation to another.

- **Product**
  Indicates the product that is associated with this issue. Select a product from the drop-down list.

Detail Fields

- **Organization**
  Specifies the name of the organization responsible for submitting the issue. You can enter a value directly or click the magnifier to search for an organization.

- **Position**
  Specifies the job title of the contact within the organization that submitted the issue, such as CEO, Director, or Manager.

- **Role**
  Indicates the role of the person submitting the issue to your service desk. For example, the person might be a customer or a potential customer.

- **On**
  Displays the date and time the record was created, in the time zone of the server. This field is read-only and is automatically filled during creation. The date and time display in mm/dd/yyyy hh: mm am | pm format.

- **Reason**
  Identifies the basic reason for opening the issue. For example, the reason might be a complaint, inquiry, or suggestion from a customer. Select a value from the drop-down list.

- **Reporting Method**
  Indicates the reporting method used to submit the current issue. Select a value from the drop-down list.

- **Assignee**
  Specifies the name of the person assigned to handle the record. You can enter the name of the person directly, or click the magnifier to search for a name. Selecting an assignee populates the groups that the assignee belongs to in the **Group** field.

- **Group**
  Specifies the group that is responsible for the record. Your system administrator defines groups of contacts that are responsible for different types of issues, requests, incidents, or problems. Any individual contact assigned to the group can handle the record once it has been assigned to the group. You can enter the group name directly, or click the magnifier to search for the group. Selecting a group populates the **Assignee** field with the corresponding assignee name, which belong to the group.

- **Service #**
  Specifies an issue number for an on-site service call.

- **Service Date**
  Specifies the date of the last on-site service call. You can enter the date and time in mm/dd/yyyy hh:mm am | pm format or click the calendar to select a date.

- **Need By Date**
  Specifies the date that the issue needs to be completed by. You can enter the date and time in mm/dd/yyyy hh:mm am | pm format or click the calendar to select a date.

- **Call Back Date/Time**
  Specifies the date and time to follow up on this record. You can enter the date and time in the format mm/dd/yyyy hh:mm am | pm, or click the calendar icon to select the date and time for follow up.

- **Root Cause**
  Specifies the code associated with the core reason why the ticket was opened. Your service desk can use generic root cause codes, such as Hardware Failure or Software Failure, or more specific codes, such as Network.Cable, Network.Card or Network.Response. You can enter the root cause directly into the field, or click the Lookup icon to display the defined root causes and select one.

- **External System Ticket**

  Specifies an identification for a ticket that belongs to an external system that integrates with CA SDM. This field stores hyperlinks and displays functional links in read-only mode.

Summary Information Fields

- **Issue Summary**
  Describes the record briefly.

- **Spelling**
  Checks the spelling of the text you enter in the Issue Summary field.

- **Issue Description**
  Describes the record.

- **Spelling**
  Checks the spelling of the text you enter in the Issue Description field.

- **Open Date**
  Displays the date and time when the issue was started in mm/dd/yyyy hh:mm am | pm format.

- **Resolve Date**
  Displays the date and time when the issue was resolved in mm/dd/yyyy hh:mm am | pm format.

- **Close Date**
  Displays the date and time when the issue was closed in mm/dd/yyyy hh:mm am | pm format.

- **Timer**
  Tracks the incremental amount of the time spent working on various phases of ticket processing. The timer is reset to 00:00:00 each time you open the ticket record for updates.

  Note: The amount of time spent on each activity is shown on the Activities tab of the ticket record.

Issue Tabs

The following tabs are available on the Create Issue, Issue Detail, and Update Issue pages:

- **Properties:** Administrators have the option of defining custom properties for issue categories, to provide additional detail on issue tickets assigned to that category. When you select an issue category while creating or editing an issue, if any custom properties have been defined for that category, they appear on the Properties tab.

- **Workflow Tasks:** Lists Workflow tasks associated with the issue. For more information, see Define a Category or Area (see page 1054) topic.

- **Config Items:** Links configuration items (CIs) to an issue or change order in order to give analysts information about the system that is affected by the ticket.

- **Knowledge:** Searches for or submits information to the knowledge base to help resolve issues. The Federated Search capability helps you to get the knowledge search results from multiple sources. For example, Google, SharePoint, CA Open Space, and so on.

- **Solutions:** Stores information about the issue solution with the issue record for future reference.

- **Resolution:** Displays a text description of the resolution to the issue.

- **Related Issues:** Create a parent/child relationship between the issue and another issue.

- **Activities:** Displays a log of the activities performed to resolve the issue. For more information, see Add an Activity from the Ticket Management (see page 2308) topic.

- **Event Log:** Displays a record of significant actions that take place regarding the issue.

- **Attachments:** Attaches a document or a link to a URL to the issue.

- **Service Type:** Attaches a service type event (see page 2313) to indicate the level of support for the ticket.
- **Time / Cost:** Calculates the estimated cost and duration of the entire issue by adding together the estimated cost and duration of each task.
- **Custom Fields:** Defines custom fields for tracking information about the issue.
- **Templates:** Create a template (see page 2315) using the current ticket as a model.
- **Support Automation:** Displays the assistance session log and lets you invite the end user to an assistance session.

Note: If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

Accumulate Costs and Time to an Issue

The accumulate feature allows you to calculate the estimated cost and duration of the entire issue by adding together the estimated cost and duration of each task. You can also choose to accumulate the issue and all of its children. Children are additional records entered as a result of attempting to resolve the original issue.

Follow these steps:

1. Select Issues, Assigned or Unassigned, and a priority level.
   The Issue List appears.
2. Select the issue of interest.
   The Issue Detail page appears.
3. Select Actions, Accumulate Issue on the menu bar.
   The Accumulate Issue page appears.
4. Click one of the following buttons:
   - **Accumulate this Issue and All Children**
     Calculates the estimated cost and duration of the issue by adding together the estimated cost and duration of tasks for this issue and all of its children.
   - **Accumulate Only this Issue**
     Calculates the estimated cost and duration of the issue by adding together the estimated cost and duration of tasks for only this issue.
   - **Cancel**
     Closes the Accumulate Issue page without accumulating the issue.

The estimated cost and duration are accumulated and you are returned to the Issue Detail page.

5. Select the Time/Cost tab on the Issue Detail page.
   The tab displays the estimated cost and duration for the issue based on the values accumulated.

Expedite an Issue

You can use the Expedite Issue command to change the status of unnecessary tasks to Skip so the issue can be completed quickly.

Note: Skip must be defined as a valid status for the task.

Follow these steps:

1. Select Issues from the Scoreboard.
   The Issues folder expands to reveal nested folders for Assigned, Unassigned, and All Scheduled issues.

2. Select the appropriate folder under Assigned, Unassigned, and All Scheduled for the issue whose children you want to close.
   The Issue List page appears.

3. Click the issue number.
   The Issue Detail page appears.

4. Select Expedite Issue from the Actions menu.
   The Expedite Issue page appears.

5. (Optional) Enter comments in the Remarks field to explain the action.

6. Click OK.
   The Expedite Issue page closes and the Workflow Tasks tab on the Issue Detail page shows all unnecessary tasks with status of Skip.

Status Transitions

You can define a subset of the full status list and determine the next status of the ticket as it continues through its lifecycle. You can also specify how strictly the system enforces status transition policies by configuring the Status Policy Violations option in Options Manager (General Options).

Note: Because status transitions can be shared between integrations such as Events and Macros, do not inactivate predefined status transitions unless explicitly requested.

Follow these steps:

1. On the Administration tab, select Service Desk, Requests/Incidents/Problems, and specify one of the following:

   - Incident Transitions
   - Problem Transitions
     Request Transitions

   The Transition List page appears.

2. Click Create.
   The Update Status Transitions page appears.

3. Complete the fields as appropriate. The following fields require explanation:

   - **From Status**
     Defines the current status of the ticket, for example, Open.
   - **To Status**
     Specifies a valid next status of the ticket, for example, Assigned.
   - **Default Transition**
     Specifies the default status transition. CA SDM uses the default transition when a user clicks the default transition button on the ticket detail page, or when a user (including a web services user) updates the status to a <d> value. You can only configure one default transition for each status (or one for each tenant in a multi-tenanted system).
   - **Must Comment**
     Indicates that a comment for the transition must be supplied. Specifying this option indicates that an analyst must supply an activity log comment when changing the status on a request.
   - **Condition**
     Specifies the condition by which the transition is allowed. For example, when the condition "nonprty 1&2 assigned req" is associated with the Request Transition of Acknowledged to Hold, the condition verifies if the transition to move the status from Acknowledged to Hold is allowed.
   - **Transition Type**
     Links a transition type to this transition. Transition types and their corresponding statuses control when employees can close and reopen Incidents and Requests using self-service. This field only displays for Incident and Request status transitions.
   - **Condition Error Message**
     Specifies the message returned to the user if the transition is rejected.

The transition is defined.

4. Click Save, Close Window.
   The transition appears in the Transition List when you refresh the page.

Status Transitions and Dependent Attribute Controls

This article contains the following topics:

You can use the following configurable controls to restrict ticket status flows for change orders, issues, incidents/problems/requests, and determine which fields are shown or required for each ticket status:

- **Transitions**
  Controls how users select available statuses on the incident/problem/request, issue, or change order form. For example, a problem is in a status of Open, and the transition flow only allows the analyst to update the status to Closed. In this example, the analyst has no other status options, which reinforces the problem management process.
  Transitions let you define a subset of the full status list and specify the default new (or next) status of a ticket based on the current status. You can define unique status transitions for each ticket type. Consider using transitions when you want to restrict status workflows for your end users.

- **Dependent Attributes**
  Controls how attributes are designated as required (must supply) or locked (cannot update) depending on ticket status. For example, the Change Manager can prevent an analyst from editing the Summary attribute after a change order is approved. Consider using attribute controls when you want to restrict certain attributes based on the status.

Note: You can specify how strictly the system enforces Status policies by configuring the Status Policy Violations option in Options Manager (General Options). This option only applies to automated system processes, such as integrations and macros.

Work with Status Transitions and Dependent Attribute Controls

To work with status transitions and dependent attribute controls, do the following:

1. On the Administration tab, configure the appropriate tenants, contacts, and roles for your environment.

2. On the Service Desk node, specify a ticket type (Change Order, for example), and select Status. The Status List page displays active status codes.

3. Edit the appropriate status code (Acknowledged, for example) and use the controls available on the tabs at the bottom of the ticket's status detail page to do the following:

   - Configure Status Transitions (see page 2066)

   - Configure Dependent Attribute Controls (see page 2067)

Note: You can configure unique transitions and dependent attribute controls for each ticket type.

Configure Status Transitions

You can configure a subset of the full status list and specify the default next status of a ticket based on the current status. Transitions are enforced when the status is changed on the ticket detail form.

To configure status transitions

1. Click the Transitions tab at the bottom of the ticket's status detail page.
   The Transitions List page shows all valid transitions for the status.

Note: When configured, linked transition types appear on the Incident and Request Transition list.

2. Click the Update Transitions button.
   The Update Ticket Status Transitions page appears.

3. Configure the following check boxes as appropriate:

   - **Allowed**
     Specifies a valid transition for the status. Use this option to restrict status workflows.

   - **Default**
     (Optional) Specifies the default status transition. CA SDM applies the default transition when a user clicks the default transition button on the ticket detail form, or when a user (including a web services user) updates the status to a <d> value. There is only one default transition for each status (or one for each tenant in a multi-tenanted system).

- **Must Comment**
  (Optional) Specifies that an activity log comment for the transition is required when changing the status on a ticket.

  Note: This option applies to CA SDM tickets only. It does not apply to other areas, such as web services or the edit in list functionality.

4. (Optional) Select a status code in the Name column to update its details.

5. Click Save.
   The list of transitions configured for the new status appears on the Transition list. When the analyst selects the Status drop-down on the ticket form, the new status list appears.

Configure Dependent Attribute Controls

You can determine which fields are shown or required for the ticket status.

Note: Before you configure dependent attributes as "required" for the ticket status, be aware that the Edit in List option that appears on the ticket's list page may not display the attribute field values that are required. If the required attribute field value is not already part of the saved ticket, and if it is not presented in the Edit In List format, then the ticket is not saved. Consequently, the analyst must edit the required dependent attribute field values on the ticket's detail page instead of using the Edit in List option.

To configure a dependent attribute control

1. On the ticket's status detail page, select the Dependent Attribute Control tab at the bottom of the page.
   The Attribute Control List appears.

2. Click Create.
   The Update Status Dependent Attribute Control page appears.

3. Complete the following fields:

   - **Tenant**
     (Optional) In a system with multi-tenancy installed, specifies an optional tenant name. If a tenant is specified, the dependency applies only to that tenant and to its sub-tenants.

   - **Attribute**
     Specifies the name of the attribute you want to control, for example, Summary.

   - **Locked**
     Specifies the attribute as locked. A locked attribute associated with a status cannot be updated in a ticket with the same status. The attribute is unlocked when the status is changed.

- **Required**
  Specifies the attribute as required. A required attribute for the status cannot use a null value in a ticket with the same status.

4. Click Save.
   The new attribute control for the status appears in the Attribute Controls List when you redisplay the page. When a user updates the ticket status, the system retrieves the list of required attributes corresponding to the new status, and updates the ticket form as appropriate. An error message appears at the top of the ticket form when a user attempts to close the ticket without filling in a required field.

Web Services Methods

You can configure the following status transition and dependent attribute control SOAP web services methods:

- **getValidTransitions**
  Lists the transitions for a ticket. This method is modeled on the existing getValidTaskTransitions method, except that the argument can be a ticket or a status.

- **getDependentAttrControls**
  Lists the locked and required attributes for an attribute of an object that persistent id specified. The Status attribute is supported at this time.

Predefined Transition Flows

For each ticket type, you can use the predefined status transitions provided with the product and modify them to accommodate your desired transition flow.

To view the list of predefined transitions, do the following:

On the Administration tab, expand the Service Desk node, and select one of the following:

- Change Order Transitions
- Issue Transitions
- Request/Incident/Problem Transitions

The Transitions List displays the predefined transitions that let you control how a ticket (incident /request/problem, change order, and issue) continues through its lifecycle.

Incident Transition Flow

The following table shows the predefined Incident transition flow:

Current Status	Default Transition	Available Next Statuses
Acknowledged	In Progress <d>	Avoided, Awaiting Vendor, Cancelled, Closed, Closed Unresolved, In Progress, Open, Pending Change, Resolved
Avoided		

Current Status	Default Transition	Available Next Statuses
		Acknowledged, Avoided, Awaiting End User Response, Closed, Closed Unresolved, In Progress, Reject Solution, Researching, Resolved
Awaiting End User Response	Researching <d>	Closed, Closed Unresolved, In Progress, Open, Researching, Resolved
Awaiting Vendor	Researching <d>	Acknowledged, Closed, Closed Unresolved, In Progress, Open, Pending Change, Researching, Resolved
Cancelled		Closed
Closed		Open
Closed Unresolved		Acknowledged
Closed Unresolved		Closed
Closed Unresolved		Open
Hold		Acknowledged, Closed, In Progress, Open, Pending Change, Resolved
In Progress	Researching <d>	Acknowledged, Awaiting End User Response, Awaiting Vendor, Closed, Closed Unresolved, Open, Pending Change, Researching, Resolved
Pending Change	Researching <d>	Acknowledged, Closed, In Progress, Open, Resolved
Researching	Resolved <d>	Closed, Open, Resolved
Resolved	Closed <d>	Awaiting End User Response, Closed, Open

Problem Transition Flow

The following table shows the predefined Problem transition flow:

Current Status	Default Transition	Available Next Statuses
Acknowledged	In Progress <d>	Acknowledged, Approved, Cancelled, Closed, Fix in Progress, Open, Rejected, Researching
Analysis Complete	Approved <d>	Acknowledged, Cancelled, Closed, Fix in Progress
Approved	Fix in Progress <d>	Closed, Fixed, Pending Change
Awaiting Vendor	Researching <d>	Acknowledged, Closed, Closed Unresolved, Fixed, In Progress, Open, Pending Change, Researching
Cancelled	Closed <d>	Closed, Closed Unresolved, Open
Closed Unresolved		Acknowledged, Closed, Open
	Fixed <d>	Approved, Cancelled, Fixed, Fix in Progress, Researching, Rejected

Current Status	Default Transition	Available Next Statuses
Fix in Progress		
Fixed	Closed <d>	Closed
Hold	Researching <d>	Acknowledged, Closed, Fixed, In Progress, Open, Pending Change, Researching
In Progress	Researching <d>	Acknowledged, Approved, Cancelled, Closed, Fix in Progress, Pending Change, Rejected, Researching
Known Error	Fix in Progress <d>	Closed, Fix in Progress, Fixed
Open	Acknowledged <d>	Acknowledged, Approved, Cancelled, Closed, Fix in Progress, In Progress, Rejected, Researching
Pending Change	Fixed <d>	Closed, Fixed, Researching
Rejected	Closed <d>	Closed, Closed Unresolved, Open
Researching	Analysis Complete <d>	Acknowledged, Analysis Complete, Approved, Cancelled, Closed, fix in Progress, Fixed, Rejected

Issue Transition Flow

The following table shows the predefined Issue transition flow:

Current Status	Default Transition	Available Next Statuses
Acknowledged	In Progress <d>	Awaiting End User Response, Awaiting Vendor, Closed, Closed Unresolved, In Progress, Open, Pending Change, Resolved
Awaiting End User Response	Researching <d>	Acknowledged, Closed, Closed Unresolved, In Progress, Open, Researching, Resolved
Awaiting Vendor	Researching <d>	Acknowledged, Closed, In Progress, Open, Pending Change, Researching, Resolved
Cancelled	Closed <d>	Closed
Closed		Acknowledged, Open
Closed Unresolved		Acknowledged, Closed, Open
Hold		Acknowledged, Closed, In Progress, Open, Pending Change, Resolved
In Progress	Researching <d>	Acknowledged, Awaiting End User Response, Awaiting Vendor, Closed, Closed Unresolved, Open, Pending Change, Researching, Resolved
Open	Acknowledged <d>	Acknowledged, Avoided by Self Service, Awaiting End User Response, Awaiting Vendor, Closed, Closed Unresolved, In Progress, Pending Change, Resolved

Current Status	Default Transition	Available Next Statuses
Pending Change	Researching <d>	Acknowledged, Closed, In Progress, Open, Researching, Resolved
Researching	Resolved <d>	Closed, Open, Resolved, Awaiting End User Response, Closed, Open

Change Order Transition Flow

The following table shows the change order transition flow:

Current Status	Default Transition	Available Next Statuses
Approval in Progress	Approved <d>	Approved, Cancelled, Closed
Approved	Scheduled <d>	Cancelled, Closed, Implementation in Progress, Scheduled
Backed Out		Approval in Progress, Closed, Open, RFC
Cancelled		Closed
Customer Hold		Cancelled, Closed, Implementation in Progress, Rejected, Scheduled, Verification in Progress
Hold		Cancelled, Closed, Implementation in Progress, Scheduled
Implementation in Progress		Backed Out, Cancelled, Closed, Customer Hold, Rejected, Scheduled, Vendor Hold, Verification in Progress
Open	RFC <d>	Approval in Progress, Cancelled, Closed, Customer Hold, Implementation in Progress, Rejected, RFC, Scheduled, Vendor Hold
Rejected	Closed <d>	Approval in Progress, Cancelled, Closed
RFC	Approval in Progress <d>	Approval in Progress, Cancelled, Closed, Customer Hold, Implementation in Progress, Open, Rejected, Scheduled, Vendor Hold
Scheduled	Implementation in Progress <d>	Cancelled, Closed, Customer Hold, Implementation in Progress, Vendor Hold, Verification in Progress, Cancelled, Closed, Implementation in Progress, Scheduled, Backed Out, Closed

Best Practice Predefined Status Transitions

The predefined status transitions delivered with the product are Active in a new installation and Inactive after the upgrade. For every status listed on the Transitions List page, there is a default status transition (or next status). The path taken by the default status transition reflects the best practice. The additional status transitions listed on the Transitions List page are provided to fulfill

various ticket management workflows. However, only Active status transitions that use this best practice can ensure that the proper workflow for managing Requests, Incidents, Problems, and Change Orders occurs. This best practice helps promote the movement of tickets to resolution and closure within the IT environment.

For example, the following predefined incident transitions listed on the Incident Transition list page are set to Inactive to help promote the resolution and closure of incidents:

Status	New Status	Default	Status Description	Record Status
Acknowledged	Closed	No	Acknowledged to Closed Status Transition	Inactive
Acknowledged	Closed Unresolved	No	Acknowledged to Close Unresolved Status Transition	Inactive
Acknowledged	Open	Yes	Acknowledged to Open Status Transition	Inactive
Awaiting End User Response	Acknowledged	No	Awaiting End User Response to Acknowledged Status Transition	Inactive
Awaiting End User Response	Open	No	Awaiting End User Response to Open Status Transition	Inactive
Awaiting Vendor	Acknowledged	No	Awaiting Vendor to Acknowledged Status Transition	Inactive
Awaiting Vendor	Closed	No	Awaiting Vendor to Closed Status Transition	Inactive
Awaiting Vendor	Open	No	Awaiting Vendor to Open Status Transition	Inactive
Closed	Acknowledged	No	Closed to Acknowledged Status Transition	Inactive
Closed Unresolved	Acknowledged	No	Closed Unresolved to Acknowledged Status Transition	Inactive
Closed Unresolved	Closed	No	Closed Unresolved to Closed Status Transition	Inactive
Hold	Acknowledged	No	Hold to Acknowledged Status Transition	Inactive
Hold	Closed	No	Hold to Closed Status Transition	Inactive
Hold	Open	No	Hold to Open Status Transition	Inactive
In Progress	Acknowledged	No	In Progress to Acknowledged Status Transition	Inactive
In Progress	Closed	No	In Progress to Closed Status Transition	Inactive
In Progress	Open	No	In Progress to Open Status Transition	Inactive
Open	Closed	No	Open to Closed Status Transition	Inactive
Pending Change	Acknowledged	No	Pending Change to Acknowledged Status Transition	Inactive
Pending Change	Closed	No	Pending Change to Closed Status Transition	Inactive
Pending Change	Open	No	Pending Change to Open Status Transition	Inactive
Researching	Open	No	Researching to Open Status Transition	Inactive

Status Transitions for Self-Service

This article contains the following topics:

Status transitions let you control the movement of a ticket from one discrete state to another (for example, from Open to Closed). For employees using self-service, you can include buttons on the Incident and Request detail forms to represent any status transition (see page 2065).

Status transition buttons for incident and request process workflows appear in the employee interface when incident or request transitions are linked to active transition types. A transition type defines the button text and controls the behavior of the ticket detail form. When buttons are defined, the legacy Close Incident (or Request) and Reopen Incident (or Request) buttons are not displayed on the ticket detail forms. Instead, the employee can only change the status of the Incident or Request using the status transition buttons configured by the administrator.

By default, all predefined transition types delivered with the product are inactive, so status transition buttons are not in effect. As a system administrator, you can activate and modify predefined transition types or create transition types to accommodate your status transition workflows. After you create or modify a transition type, you can link them to any incident or request status transition.

How Transitions for Self-Service Work

Transition types and their corresponding statuses control when employees can close and reopen tickets as follows:

1. Active transition types are linked to incident (or request) status transitions by the administrator.
2. The employee creates an incident using self-service.
3. The analyst assigned to the incident finds a solution and moves the ticket to the Resolved status.
4. When the ticket is in a Resolved status, the employee detail form displays status transition buttons to Accept or Reject the resolution.
   - If the employee accepts the resolution, the Resolved to Closed transition occurs.
   - If the employee rejects the resolution, the Resolved to Open transition occurs.
5. After the employee clicks a button, they can add their remarks in the resolution form that appears.

How to Create or Update Transition Types for Transitions

As a system administrator, you can create new or update existing transition types for incident and request status transition workflows on the Transition Types List page.

To create a transition type for a status transition, do the following:

1. On the Administration tab, select Service Desk, Requests/Incidents/Problems, Transition Types.

2. Click Create on the list page.

3. Edit the fields as appropriate on the detail page.
   The transition type for the status transition is created.

4. Click Save.
   The new transition type appears in the Transitions Type List when you redisplay the page.

To update a transition type, do the following:

1. Open the desired transition type for editing on the Transition Types List page.

2. Edit the fields as appropriate.

3. Click Save.
   The updated transition type appears on the Transition Type list.

How to Link Transition Types to Transitions

When status transitions are linked to transition types, the employee ticket detail form displays status transition buttons to Accept or Reject the resolution. To link a transition type with a status transition, do the following:

1. On the Administration tab, select Service Desk, Requests/Incidents/Problems, Incident (or Request) Transitions.

2. Open the desired status transition for editing on the Request or Incident Transition List page.

3. Specify the desired transition type in the Transition Type field.

4. Click Save.
   The transition type is linked to the status transition.

Activate Predefined Transition Types

By default, all predefined transition types that are delivered with the product are Inactive, so status transition buttons are not in effect. You can activate and modify these transition types to accommodate your desired status transition flow.

To activate a predefined transition type

1. Select Show Filter on the Transition Type List page.
   The top portion of the page reveals additional search fields.

2. Select Inactive in the Record Status field and click Search.
   The Transition Type List displays all inactive transition types.

3. Right-click the desired transition type and select Edit from the menu.

4. Select Active in the Record Status field.

5. Click Save, Close window.

6. Click Search.
   The Transition Type List displays the active transition type.

Predefined Transition Types for Incident Status Transitions

The following table describes the predefined transition types for incident status transitions:

Symbol	Button Text	Form Header Text	Incident Status Transition
Accept incident resolution button	Accept	Accept Resolution	Resolved to Closed
Reject incident resolution button	Reject	Reject Resolution	Resolved to Open
Reject Closure incident button	Request Closure	Request Closure	To Closed Unresolved from Open Awaiting End User Response Awaiting Vendor In Progress Acknowledged

Predefined Transition Types for Request Status Transitions

The following table describes the predefined transition types for request status transitions:

Note: The Closed Requested status for Requests is the equivalent of the Resolved status for Incidents.

Symbol	Button Text	Form Header Text	Request Status Transition
Accept request resolution button	Accept	Accept Resolution	Close Requested to Closed
Reject request resolution button	Reject	Reject Resolution	Close Requested to Open
Request Closure request button	Request Closure	Request Closure	

Symbol	Button Text	Form Header Text	Request Status Transition
			To Canceled from Open Awaiting End User Response Awaiting Vendor Approval In Progress Acknowledged
Close request button	Close	Close Requested	From In Progress to Closed

Define Issue Transitions

Issue status transitions control the movement of a issue from one discrete state to another (for example, from Open to Closed). With transitions, you can define a subset of the full status list and determine the next status of the ticket as it continues through its lifecycle. You can use the predefined transitions (listed on the Issue Transitions List page), modify the transitions, or create transitions.

Note: You can specify how strictly the system enforces Status policies by configuring the Status Policy Violations option in Options Manager (General Options). This option only applies to automated system processes, such as integrations and macros.

You can define a subset of the full status list and determine the next status of the ticket as it continues through its lifecycle.

Note: Because status transitions can be shared between integrations such as Events and Macros, do not inactivate predefined status transitions unless explicitly requested.

Follow these steps:

1. On the Administration tab, select Service Desk, Issues.
   The Issue Transition List page appears.

2. Click Create.
   The Update Status Transitions page appears.

3. Complete the fields as appropriate. The following fields require explanation:

   - **From Status**
     Defines the current status of the ticket, for example, Open.

   - **To Status**
     Specifies a valid next status of the ticket, for example, Assigned.

- **Default Transition**
  Specifies the default status transition. CA SDM applies the default transition when a user clicks the default transition button on the ticket detail page, or when a user (including a web services user) updates the status to a <d> value. You can only configure one default transition for each status (or one for each tenant in a multi-tenanted system).

- **Must Comment**
  Indicates that a comment for the transition must be supplied. Specifying this option indicates that an analyst must supply an activity log comment when changing the status on a request.

- **Condition**
  Specifies the condition by which the transition is allowed. For example, when the condition "nonprty 1&2 assigned req" is associated with the Request Transition of Acknowledged to Hold, the condition verifies if the transition to move the status from Acknowledged to Hold is allowed.

- **Condition Error Message**
  Specifies the message returned to the user if the transition is rejected.

- **Description**
  Specifies the message returned to the user if the transition is rejected.

The transition is defined.

4. Click Save, Close Window.
   The new transition appears in the Issue Transition List when you refresh the page.

Define Transition Types

This article contains the following topics:

For employees using self-service, you can modify incident and request process flows by including buttons to represent any *status transition*. Status transition buttons for incident and request process workflows are configured through *transition types*. A transition type lets you define the button text, form header text, and control the behavior of the Incident and Request detail page. You can link a transition type to any incident or request status transition.

To define a transition type

1. On the Administration tab, select Service Desk, Requests/Incidents/Problems, Transition Types.
   The Transitions Type List page appears.

2. Click Create.
   The Update Transition Types page appears.

3. Complete the fields as appropriate.
   The transition type for the status transition is created.

4. Click Save, Close Window.
   The new transition type appears in the Transitions Type List when you refresh the page.

Link Transition Types to Incident/Request Status Transitions

You can link a transition type to any incident or request status transition.

To link a transition type to an incident or request status transition

1. On the Administration tab, select Service Desk, Requests/Incidents/Problems, Request (or Incident) Transitions.
   The Transition List page appears.

2. Open the desired status transition.
   The Transition Details page appears.

3. Click Edit.
   The Update Transition page appears.

4. Specify the transition type that you want to link to in the Transition Type field. You can enter a value directly or click the magnifying glass to search for a service type.
   The transition type is associated with the status transition.

5. Click Save, Close Window.
   The transition type appears on the Status Transition list when you redisplay the list.

Activate Predefined Transition Types

By default, all predefined transition types delivered with the product are inactive, so status transition buttons are not in effect. You can activate and modify these transition types to accommodate your desired status transition flow.

To activate a predefined transition type

1. Select Show Filter on the Transition Type List page.
   The top portion of the page reveals additional search fields.

2. Select Inactive in the Record Status field and click Search.
   The Transition Type List displays all inactive transition types.

3. Right-click the title of the transition type and select Edit from the menu.

4. Select Active in the Record Status drop-down list.

5. Click Save, Close Window.

6. Click Search.
   The Transition Type List displays the active transition type.

Issue Workflows

Contents

A *workflow* is an automated or partially automated business process that specifies the sequence of tasks that must be performed to resolve a ticket.

Two workflow solutions are supported for issues:

- **CA SDM "classic" workflow** -- internal workflow automation features provided as a standard CA SDM component.
- **CA Process Automation** -- workflow with task-based steps that run remotely on the CA Process Automation web service.

Your administrator can configure issue categories to use either type of workflow. When an issue ticket is assigned to a category with an associated workflow, a series of tasks appear on the ticket's Workflow Tasks tab.

Some workflow tasks may be optional, which allows you to delete them from the task list.

You must complete all mandatory workflow tasks before you can close the ticket. The only exception is that if the ticket status is set to Cancelled, the workflow process terminates automatically.

If a ticket is removed from a category with an attached workflow, or assigned to a different category, the workflow process terminates automatically. If the new category has an attached workflow, its process starts automatically.

Process CA Process Automation Workflow Items

You can use CA Process Automation to manage required tasks for requests, incidents, problems, issues, and change orders. From CA SDM, you can view the status for a workflow. You can log in to the CA Process Automation server to view, update, or approve tasks, When you log in, CA Process Automation shows more details about each workflow task.

Note: For information about using CA Process Automation, see the CA Process Automation documentation.

Follow these steps:

1. On the CA SDM tab, select one of the following item:
   - Incidents, Assigned, or Unassigned, and the Priority
   - Problems, Assigned, or Unassigned, and the Priority
   - Requests, Assigned, or Unassigned, and the Priority
   - Change Orders, Assigned, or Unassigned, and the Priority

- Issues, Assigned, or Unassigned, and the Priority

The ticket List appears.

2. Select the ticket.
   The ticket Detail page appears.

3. Select the Workflow Tasks tab.
   When a CA Process Automation workflow is attached, a list of workflow tasks appears on the tab.

4. Click View Process or select a Process Instance Name.
   The CA IT Process Automation Manager log in page appears.

5. Enter your CA Process Automation user login and password.
   CA Process Automation launches a graphical snapshot of the workflow or a Task List for the process instance. After you close CA Process Automation, the CA SDM Workflow Tasks tab updates. During the same browser session, you do not have to re-enter your credentials to access CA Process Automation.

Incident Management

This article contains the following topics:

Incidents are events outside of normal operations. When an incident occurs, it disrupts the normal operational processes of an organization.

Important! Unless otherwise noted, all the CA SDM Request features are also available for Incidents and Problems.

Note: Depending on your role, you may not have access to all the functionality described in this section. For example, some predefined roles can edit records but cannot create records.

Create an Incident

You can either create an incident from scratch or use an existing template.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Service Desk tab, click the File menu and select the ticket type that you want to create. For example: To create a request from scratch, click File, New Request. To create a request from a template, click File, New Request from Template.

2. Fill in the incident fields (see page) as appropriate. Use the controls available on the issue tabs (see page 2080) to process the ticket as appropriate.

3. Click one of the following buttons:

   Auto Assign -- Triggers an auto assignment task, and updates the activity log. This button appears only when the ticket specifies a category or area that has auto-assignment enabled.

   Create Change Order -- Opens the Create New Change Order page. You can create a change order ticket that is associated with this incident. This button appears only when you create incidents, problems, and requests.

   Create Problem -- Opens the Create New Problem page so you can create a problem ticket associated with this incident. This button appears only when you create incidents and requests.

   Find Similar -- Opens the Find Similar page to search for similar problems.**Quick Profile --** Displays the contact information for the specified user in the **Affected End User** field. You can also view their environment details and their entire ticket history.

   Use Template -- Displays a list of available templates for the selected ticket type. You can select the template that you want to use for creating this ticket.

Note: You can use Quick Profile to identify a contact to be the affected end user of your new ticket. Quick Profile allows you to search for a contact, and view the history of the issues, requests, change orders, incidents, and problems that are assigned to that contact. When you have identified a contact, you can create the incident ticket directly from Quick Profile.

Incident Fields

The following fields are required to create or update an incident:

- **Incident Reference Number**
  This is a unique reference number assigned by CA Service Desk Manager for all incident tickets. This is used by analysts and customers to refer to a particular incident ticket.

- **Requester**
  Specifies the name of the person who initiated the ticket. This person must be a defined contact. You can enter a value directly or click the magnifier to search for the name.

- **Affected End User**
  Specifies the contact name of the person who is affected by the record. If the contact is assigned to a special handling type, special handling indicators are displayed. You can enter a value directly or click on the magnifier icon to search for a contact name.

- **Incident Area**
  Indicates the general area of your IT environment that is affected by the incident. For example, Applications, E-mail, Hardware, and Software. An incident area provides default values that are automatically entered on all the incident tickets pertaining to that area. In addition to the predefined incident areas, your system administrator can define custom incident areas. You can enter a value directly, or you can expand the node to display the defined incident areas and select one.

  Note: Your system administrator has the option of adding custom properties to incident areas. The custom properties are available on the Properties tab when you create, edit, or view an incident ticket. Some custom properties require that you enter a value.

- **Status**
  Specifies the status code of the record. For example, you can list only the tickets with a status code of Fix in Progress, or Close Requested. You can enter a value directly or click on the magnifier icon to search for a status. The blue button (on the left side of the Status field) lets you change the current status to the next default status.

- **Priority**
  Specifies the priority ranking of the record. The ranking determines the amount of attention the ticket receives. The predefined priority levels are 1 (highest) through 5 (lowest). Your system administrator or an active priority calculation can generate the appropriate priority values for various installations and tenants. When priority calculation is enabled, this field is updated based on Impact, Urgency, Affected Service, and Affected User settings. When your administrator disables priority calculation and uninstalls the urgency_on_employee option, Self Service Users see the Priority field on the Request Detail page.

- **Active**
  Indicates whether the record is Active or Inactive. This value applies to the current record only and not the associated template.

Detail Fields

- **Reported By**
  Specifies the name of the person reporting the record.

- **Assignee**
  Specifies the name of the person who is assigned to handle the record. You can enter a value directly or click on the magnifier icon to search for a name. Selecting an assignee populates the groups that the assignee belongs to in the **Group** field.

- **Group**
  Specifies the group that is responsible for this record. Your system administrator defines groups of contacts that are responsible for different types of issues, requests, incidents, or problems. Any contact who is part of the group can handle the record after it is assigned to the group. You can enter a value directly or click on the magnifier icon to search for a group. Selecting a group populates the **Assignee** field with the corresponding assignee name that belongs to the group.

- **Affected Service**
  Specifies the primary service that affects the problem or incident. The CIs of type Service have a class that is defined in the Enterprise Service Family field. The ticket stores the currently affected service information for reporting. You can enter a value directly or click on the magnifier icon to search for a CI.

- **Urgency**
  Specifies the urgency of the record. The urgency is determined by the importance of the user tasks that are affected by the record. Urgency codes indicate the importance of a ticket based on the degree to which it affects user tasks. For example, a network outage is more urgent than a printer failure. Your system administrator can modify the default urgency codes, so they can vary from one installation to another. Urgency values can update automatically based on an active priority calculation.

- **Impact**
  Specifies an impact code, such as 1 -- Entire Organization, that indicates how a ticket affects the work being performed. For example, a ticket that requires a network outage for several hours would have a higher impact than a ticket that takes a printer off-line. Your system administrator can modify the default impact codes, so they can vary from one installation to another.

- **Major Incident**
  Specifies that the incident is major or significant. Because of its importance, changes to this value on a ticket generate an activity log entry.

  Note: When you copy an incident, the value of this field is cleared. In addition, related tickets (child incidents) do not include the Major Incident value.

- **Configuration Item**
  Specifies the hardware, software, or service that is affected by the record. Your system administrator creates a record that uniquely identifies each configuration item for your organization and indicates its precise location. You can enter a value directly or click on the magnifier icon to search for an item.

- **Problem**
  Provides the number and name of the problem that is associated with this record. Enter the number or name of the problem directly into this field or click the search icon to search for the problem.

- **Symptom**
  Specifies a code that describes a primary symptom of the incident. For example, Slow Response.

- **Resolution Code**
  Indicates the action that the analyst had taken to resolve an incident or request. Resolution codes specify the general resolution of the ticket. For example, an Applied Patch resolution code indicates that the analyst used a software patch to address an incident.

- **Resolution Method**
  Indicates *how* an analyst implemented the resolution. For example, a Chat Session resolution method indicates that an analyst used a chat session to address an incident.

- **Call Back Date/Time**
  Specifies the date and time to follow up on this record. You can enter the date and time, in the format *mm/dd/yyyy hh:mm am | pm*, or click the calendar icon to open a calendar window where you can select the date and time for follow-up.

- **Change**
  Specifies the number and name of the change order that is associated with this record. You can enter the number or name of the change order directly in this field. Or, click the search icon to search for the change order.

- **Caused by Change Order**
  Specifies the change order number when the Incident ticket is the result of changes that are implemented from a change order.

- **External System Ticket**
  Specifies an identification for a ticket that belongs to an external system that integrates with CA SDM. This field stores hyperlinks and displays functional links in read-only mode.

Summary Information Fields

- **Summary**
  Provides a brief description of the record.

- **Spelling**
  Checks the spelling of the text that you enter in the Summary field.

- **Search Knowledge**
  Searches the CA SDM knowledge base to help resolve tickets. If you do not find any relevant knowledge base articles, you can submit your own knowledge base article after the ticket is resolved.

- **Total Activity Time**
  Displays a running total of the overall amount of time that is spent on the ticket. This value is updated each time a change is made to the ticket record. You cannot edit this field.

- **Timer**
  Tracks the incremental amount of the time spent working on various phases of ticket processing. The timer is reset to 00:00:00 each time you open the ticket record for updates. You cannot edit this field.

Note: The amount of time that is spent on each activity is shown on the Activities tab of the ticket record.

- **Description**
  Describes the record in detail.
- **Created via**
  Specifies the component reporting the record (Form Name: detail_in.htmpl)
- **Ticket Open Date/Time**
  Displays the date and time the ticket was opened.
- **Last Modified Date/Time**
  Displays the date that this ticket was last modified.
- **Ticket Resolved Date/Time**
  Displays the date and time the ticket was resolved.
- **Ticket Closed Date/Time**
  Displays the date and time the ticket was closed.
- **Last Modified By**
  Displays the name of the last person who edited the ticket.

Incident Tabs

The following tabs are available on the Create New Incident, Incident Detail, and Update Incident pages:

- **Activities:** Displays a log of the activities performed to resolve the incident. For more information, see Ticket Management (see page 2308).
- **Event Log:** Displays a record of significant actions that occur regarding the incident.
- **Verification Log:** Displays the change verification activity history for this Incident. The log shows details about the policy and actions taken during the change verification operations involved in this Incident. For example, this log identifies the policy, CI, and managed attribute values that caused a change specification to create the Incident.

Note: This tab only appears if a CACF policy created the Incident.

- **Attachments:** Attaches a document or a link to a URL to the incident.
- **Service Type:** Attaches a service type event (see page 2313) to indicate the level of support for the ticket.

- **Workflow Tasks:** Lists the process instance and related audit trail messages for CA Process Automation or Classic Workflow that is associated with the ticket. The Workflow Tasks tab shows fields that apply to an attached workflow. The workflow may require some of the work items to complete before the ticket can close. The Workflow Tasks tab appears only if your administrator configured workflows for the ticket area or category. For more information, see Define a Category or Area (see page 1054) topic.

- **Efficiency Tracking:** You can specify criteria to track incidents. The information that you specify provides your organization with metrics about incidents for reports. For example, you can indicate that an incident was assigned incorrectly. When a large percentage of incorrectly assigned incidents appears in a report, your organization is aware that assignments must be adjusted. Efficiency tracking options appear only when the efficiency_tracking Options Manager option is installed. For more information about installing efficiency_tracking, see Install Incident Tracking (see page 1072). Complete the following fields as appropriate:

  - **Resolvable at a Lower Level**
    Flags incidents that are resolvable at a lower level.

  - **Incorrectly Assigned**
    Flags incidents that are assigned incorrectly.

  - **Remote Control was Used**
    Flags incidents in which remote control was used.

  - **Action**
    Sets or resets the Actual Date/Time to the current date and time.

  - **Target**
    Specifies the current Service Target. Service Targets measure whether the required service or repair is completed within the required time frame.

  - **Target Date/Time**
    Specifies date and time when this Service Target is due. If the ticket is in Hold status, this value is blank.

  - **Actual Date/Time**
    Specifies the time when the target condition was met. If no value appears, the target condition has not been met.

  - **Time Left**
    Specifies the amount of remaining time for the service target when the ticket is on hold. If the Service Target has been met, Time Left shows the unused time. A negative value indicates the amount of time that elapsed since the missed target date.

  - **Violation Cost**
    Specifies the incurred cost when the service type time limit is violated.

- **Parent / Child:** Create a parent/child relationship between the incident and another CA SDM record.

- **Knowledge:** Searches for or submits information to the knowledge base to help resolve incidents. The Federated Search capability helps you to get the knowledge search results from multiple sources. For example, Google, SharePoint, CA Open Space, and so on.

- **Solutions:** Stores information about the incident solution with the incident record for future reference.

- **Properties:** Adds custom properties to incident areas.

- **Outage:** Specifies information about service outages for an incident. Complete the Service Outage fields as appropriate:

  - **Start Time**
    Specifies the start date and time for an outage period related to the subject of the incident ticket. This value, together with the End Time, lets you track incident outages with the tickets that are opened relative to the outage. You can click the calendar icon to open the Date Helper window to select a date.

  - **End Time**
    Specifies the end date and time for an outage period related to the subject of the incident ticket. This value, together with the Start Time, lets you track incident outages with the tickets that are opened relative to the outage. You can click the calendar icon to open the Date Helper window so you can select a date.

  - **Type**
    Specifies the type of outage, such as a network outage. You can use the predefined outage types or create outage types.

  - **Return to Service**
    Indicates that service was restored.

  - **Percent of Service Restored**
    Specifies the percentage of service that was restored.

- **Template:** Allows you to create a Problem template (see page 2315) using the current ticket as a model.

- **Support Automation:** Displays the assistance session log and lets you invite the end user to an assistance session.

Request Management

Request Management Using CA IT Asset Manager

You can automate the request of IT assets through a repeatable service offering that is accessible through a service catalog. This function can increase customer satisfaction and can standardize your asset base to improve response times and service levels.

To automate request fulfillment, use the CA APM integration with CA Service Catalog.

Request Fulfillment

When CA APM and CA Service Catalog are integrated, you can perform request fulfillment using the two products. Use request fulfillment to associate requested items from a CA Service Catalog service request with CA APM assets. During the fulfillment process, you can perform the following tasks:

- View the assets that are assigned to a request.
- Assign the assets to a request.
- Remove the assets from a request.
- Deny the fulfillment of a request for assets.

For information about creating and managing requests in CA Service Catalog, see Integrate with CA Service Catalog Manually (see page 3470).

How to Fulfill Requests from Inventory

When you integrate CA Service Catalog with CA APM, you can associate assets with items requested from the catalog during request fulfillment. To fulfill requests from inventory, complete the following steps:

1. In CA APM, verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled.

   Note: For more information about creating user roles, see User Roles (see page 1574).

2. In CA Service Catalog, create a request for an asset.
   The request contains information about the requester and the type of hardware or software asset being requested.

3. In CA Service Catalog, open the request and click the gold brick action icon that is associated with the request.
   CA APM opens and the CA APM Fulfillment page appears.

Note: For information about creating and managing requests, see Integrate with CA Service Catalog Manually (see page 3470).

4. In CA APM, complete the following steps:
   a. Search for the assets from the inventory request that you want to fulfill.
   b. Complete any of the following steps:
      - Fulfill the inventory request for a hardware asset (see page 2090).
      - Fulfill the inventory request for a software asset (see page 2090).
      - (Optional) Deny an inventory request (see page 2089).
      - Display the list of assigned assets (see page 2089) to verify that they match the request.
      - (Optional) Remove an assigned hardware asset from an inventory request (see page 2091).
      - (Optional) Remove an assigned software asset from an inventory request (see page 2092).
5. In CA Service Catalog, verify the status of the fulfilled inventory request.

Deny an Inventory Request

You can deny an inventory request to indicate that none of the assets that are requested are fulfilled. When you open CA APM from a CA Service Catalog request, the CA APM Fulfillment page appears with a list of all assets available in CA APM.

Note: Verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled. For more information about creating user roles, see User Roles (see page 1574).

On the CA APM Fulfillment page, click Not Fulfilled from Inventory. The inventory request is denied, and the status of the request is updated in CA Service Catalog.

Display Assets Assigned to a Request

CA APM lets you display all assets that are currently assigned to a CA Service Catalog request. The enables you to manage the request fulfillment. When you open CA APM from a CA Service Catalog request, the CA APM Fulfillment page appears with a list of all assets available in CA APM.

Note: Verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled. For more information about creating user roles, see User Roles (see page 1574).

To display assets that are assigned to an inventory request, click Assigned Asset in the menu on the left of the CA APM Fulfillment page. A list of all assets that are assigned to the request appears in the search results.

Fulfill an Inventory Request for a Hardware Asset

You can fulfill a CA Service Catalog inventory request so that hardware assets are correctly assigned and fulfilled. When you open CA APM from a CA Service Catalog request, the CA APM Fulfillment page appears with a list of all hardware assets available in CA APM.

Note: Verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled. For more information about creating user roles, see User Roles (see page 1574).

Follow these steps:

1. On the CA APM Fulfillment page, complete one of the following steps to search for an asset:
   a. Scroll through the list of all available hardware assets that appear in the search results.
   b. Specify the search criteria and click Go.
      A list of matching hardware assets appears in the search results.
2. In the search results, select the assets that you want to fulfill.
3. (Optional) In the Fulfillment Changes area of the page, make field-level changes to all selected assets. For example, you can change the department, cost center, general ledger (GL) code, contact, and location for all selected assets.
4. Click Fulfill.
   The request is fulfilled, the request status is updated in CA Service Catalog. The asset information is updated in CA APM.

Fulfill an Inventory Request for a Software Asset

You can fulfill a CA Service Catalog inventory request so that a software asset is correctly assigned and fulfilled. When you open CA APM from a CA Service Catalog request, the CA APM Fulfillment page appears with a list of all software assets available in CA APM.

Important! If you have a CA SAM implementation, we do not recommend that you fulfill software asset requests in CA APM. We recommend that you use CA SAM to manage your software assets and licenses.

Note: Verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled. For more information about creating user roles, see User Roles (see page 1574).

Follow these steps:

1. On the CA APM Fulfillment page, complete one of the following steps to search for a software asset:

    a. Scroll through the list of all available assets that appear in the search results.

    b. Specify the search criteria and click Go.
    A list of matching software assets appears in the search results.

2. In the search results, click the software asset that you want to fulfill.
The Asset Details page for the selected software asset appears.

3. Define or update software internal allocations for the software asset by clicking Asset Allocation in the Relationships menu.

4. Click New and select the hardware asset that you want to associate with the software asset.

5. Click Fulfill and Save.
The software request is fulfilled, the internal allocations are saved, the request status is updated in CA Service Catalog. The asset information is updated in CA APM.

Remove an Assigned Hardware Asset from an Inventory Request

CA APM lets you remove an assigned hardware asset from an inventory request. For example, you have a laptop that was mistakenly added to a request and you want to remove it. When you open CA APM from a CA Service Catalog request, the CA APM Fulfillment page appears with a list of all hardware assets available in CA APM.

Note: Verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled. For more information about creating user roles, see User Roles (see page 1574)

Follow these steps:

1. On the left of the CA APM Fulfillment page, click Assigned Asset.
   A list of all hardware assets that are assigned to the request appears in the search results.

2. In the search results, select the hardware assets that you want to remove from the request.

3. (Optional) In the Fulfillment Changes area of the page, make field-level changes to all selected assets. For example, you can change the general ledger (GL) code, cost center, department, contact, location.

4. Click Remove Assignment.
   The hardware asset is removed from the request, the status of the request is updated in CA Service Catalog. The asset information is updated in CA APM.

Remove an Assigned Software Asset from an Inventory Request

CA APM lets you remove an assigned software asset from an inventory request. For example, a graphics software package was mistakenly added to a request and you remove the software from the request. When you open CA APM from a CA Service Catalog request, the CA APM Fulfillment page appears with a list of all software assets available in CA APM.

Note: Verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled. For more information about creating user roles, see User Roles (see page 1574).

Follow these steps:

1. On the left of the CA APM Fulfillment page, click Assigned Asset.
   A list of all software assets that are assigned to the request appears in the search results.

2. In the search results, click the software asset that you want to remove from the request.
   The Asset Details page for the selected software asset appears.

3. Remove or update software internal allocations for the software asset by clicking Asset Allocation in the Relationships menu.

4. Click the Delete icon next to your selected asset.

5. Click Remove Fulfillment and Save.
   The asset is removed from the request, the internal allocations are saved. The status of the request is updated in CA Service Catalog and the asset information is updated in CA APM.

Request Management Using CA SDM

This article contains the following topics:

- Request Tabs (see page 2097)

Requests are records of reports made to the help desk and the activities performed to resolve the requests. If you create a ticket as a copy of another ticket, the Status field displays all Status values.

Important! Depending on your role, you do not have access to all the functionality described in this section. For example, some predefined roles can edit records but cannot create new ones.

Create a Request

You can either create a request from scratch or use an existing template.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Service Desk tab, click the File menu and select the ticket type that you want to create. For example, to create a request from scratch, click File, New Request. To create a request from a template, Click File, New Request from Template.

2. Fill in the request fields (see page) as appropriate.
   Use the controls available on the tabs (see page) to process the ticket as appropriate.

3. Click one of the following buttons:

   Auto Assign -- Triggers an auto assignment task, and updates the activity log. This button appears only when the ticket specifies a category or area that has auto-assignment enabled.

   Create Change Order -- Opens the Create New Change Order page. You can create a change order ticket that is associated with this incident. This button appears only when you create incidents, problems, and requests.

   Create Problem -- Opens the Create New Problem page so you can create a problem ticket associated with this incident. This button appears only when you create incidents and requests.

   Create Incident – Opens the Create New Incident page so you can create an associated incident ticket. This button appears only when you create change orders and requests.

   Find Similar -- Opens the Find Similar page to search for similar problems.**Quick Profile --** Displays the contact information for the specified user in the **Affected End User** field. You can also view their environment details and their entire ticket history.

Use Template -- Displays a list of available templates for the selected ticket type. You can select the template that you want to use for creating this ticket.

Note: You can use the Quick Profile to identify a contact to be the affected end user of your new ticket. Quick Profile allows you to search for a contact, and view the history of the issues, requests, change orders, incidents, and problems that are assigned to that contact. When you have identified a contact, you can create the incident ticket directly from the Quick Profile.

Request Fields

The following fields are required to create or update a request:

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

- **Request Reference Number**
  This is a unique reference number assigned by CA Service Desk Manager for all request tickets. This is used by analysts and customers to refer to a particular request ticket.

- **Requester**
  Specifies the name of the person who initiated the ticket. This person must be a defined contact. You can enter a value directly or click the magnifier to search for the name.

- **Affected End User**
  Specifies the contact name of the person who is affected by the record. If the contact is assigned to a special handling type, special handling indicators are displayed. You can enter a value directly or click the magnifier to search for a contact name.

- **Request Area**
  Indicates the general area of your IT environment affected by the request (for example, Applications, E-mail, Hardware, and Software). Request areas provide default values that are entered automatically on all requests assigned to the area. In addition to the predefined request areas provided, your system administrator can define custom request areas.
  You can enter the request area directly into the field, or click the Lookup icon to select from the defined request areas.

  Your system administrator has the option of adding custom properties to request areas. If custom properties have been added, they are displayed on the Properties tab when you create, edit, or view a request. Some custom properties require that you enter a value. For details, see Request Properties.

- **Status**
  Specifies the status code of the record. For example, you can list only the tickets with a status code of Fix in Progress, or can Close Requested. You can enter a value directly or click the magnifier to search for a status. The blue button (on the left side of the Status field) lets you change the current status to the next default status.

- **Priority**
  Specifies the priority ranking of the record. The ranking determines the amount of attention the ticket receives. The predefined priority levels are 1 (highest) through 5 (lowest). Your system administrator or an active priority calculation can generate the appropriate priority values for various installations and tenants. When priority calculation is enabled, this field is updated based on Impact, Urgency, Affected Service, and Affected User settings. When your administrator disables priority calculation and uninstalls the urgency_on_employee option, Self Service Users see the Priority field on the Request Detail page.

Detail Fields

- **Reported By**
  Specifies the name of the person reporting the record.

- **Assignee**
  Specifies the name of the person who is assigned to handle the record. You can enter a value directly or click the magnifier to search for a name. Selecting an assignee populates the groups that the assignee belongs to in the **Group** field.

- **Group**
  Specifies the group that is responsible for this record. Your system administrator defines groups of contacts that are responsible for different types of issues, requests, incidents, or problems. Any contact who is part of the group can handle the record after it is assigned to the group. You can enter a value directly or click the magnifier to search for a group. Selecting a group populates the **Assignee** field with the corresponding assignee name, which belong to the group.

- **Configuration Item**
  Specifies the hardware, software, or service that is affected by the record. Your system administrator creates a record that uniquely identifies each configuration item for your organization and indicates its precise location. You can enter a value directly or click the magnifier to search for an item.

- **Severity**
  Specifies the severity of the record, determined by the effect on people. Your system administrator can modify the default severity codes, so they can vary from one installation to another.

- **Urgency**
  Specifies the urgency of the record. The urgency is determined by the importance of the user tasks that are affected by the record. Urgency codes indicate the importance of a ticket based on the degree to which it affects user tasks. For example, a network outage is more urgent than a printer failure. Your system administrator can modify the default urgency codes, so they can vary from one installation to another. Urgency values can update automatically based on an active priority calculation.

- **Impact**
  Specifies an impact code, such as 1 -- Entire Organization, that indicates how a ticket affects work being performed. For example, a ticket that requires a network outage for several hours would have a higher impact than a ticket that takes a printer off-line. Your system administrator can modify the default impact codes, so they can vary from one installation to another

- **Active**
  Indicates whether the record is Active or Inactive. This value applies to the current record only, not the associated template.

- **Charge Back ID**
  Identifies the ID that is charged for service.

- **Call Back Date/Time**
  Identifies the date and time to follow up on this record. Enter the date and time in the format mm/dd/yyyy hh:mm am | pm, or click the calendar icon to select the date and time for follow-up.

- **Resolution Code**
  Indicates the action that the analyst had taken to resolve an incident or request. Resolution codes specify the general resolution of the ticket. For example, an Applied Patch resolution code indicates that the analyst used a software patch to address an incident.

- **Resolution Method**
  Indicates *how* an analyst implemented the resolution. For example, a Chat Session resolution method indicates that an analyst used a chat session to address an incident.

- **Change**
  Specifies the number and name of the change order associated with this record. You can enter a value directly or click the magnifier to search for a change order.

- **Caused by Change Order**
  Specifies only tickets that were opened as a result of a specific change order ticket. You can enter a value directly or click the magnifier to search for a change order ticket.

- **External System Ticket**
  Specifies an identification for a ticket that belongs to an external system that integrates with CA SDM. This field stores hyperlinks and displays functional links in read-only mode.

Summary Information Fields

- **Summary**
  Provides a brief description of the record.

- **Spelling**
  Checks the spelling of the text you enter in the Summary field.

- **Total Activity Time**
  Displays a running total of the overall amount of time spent working on the ticket. This value is updated each time a change is made to the ticket record. You cannot edit this field.

- **Timer**
  Tracks the incremental amount of the time spent working on various phases of ticket processing. The timer is reset to 00:00:00 each time you open the ticket record for updates. You cannot edit this field.

  Note: The amount of time spent on each activity is shown on the Activities tab of the ticket record.

- **Search Knowledge**
  Searches for or submits information to the CA SDM Knowledge Base to help resolve tickets.

- **Description**
  Describes the record in detail.

- **Ticket Open Date/Time**
  Displays the date and time the ticket was opened.

- **Last Modified Date/Time**
  Displays the date that this ticket was last modified.

- **Ticket Resolved Date/Time**
  Displays the date and time the ticket was resolved.

- **Ticket Closed Date/Time**
  Displays the date and time the ticket was closed.

Request Tabs

The following tabs are available on the Create Request, Request Detail, and Update Request pages:

- **Activities:** Displays a log of the activities performed to resolve the request. For more information, see Add an Activity from the Ticket Management (see page 2308) topic.
- **Event Log:** Displays a record of significant actions that take place regarding the request.
- **Attachments:** Attaches a document or a link to a URL to the request.
- **Workflow Tasks:** Lists the process instance and related audit trail messages for CA Process Automation or Classic Workflow that is associated with the ticket. The Workflow Tasks tab shows fields that apply to an attached workflow. The workflow may require some of the work items to complete before the ticket can close. The Workflow Tasks tab appears only if your administrator configured workflows for the ticket area or category. For more information, see Define a Category or Area (see page 1054) topic.
- **Service Type:** Allows you to attach a service type event (see page 2313) to indicate the level of support for the ticket.
- **Parent / Child:** Allows you to create a parent/child relationship between the request and another CA SDM record.

- **Knowledge:** Searches for or submit information to the CA SDM Knowledge base to help resolve requests. The Federated Search capability helps you to get the knowledge search results from multiple sources. For example, Google, SharePoint, CA Open Space, and so on.
- **Solutions:** Stores information about the request solution with the request record for future reference.
- **Properties:** Adds custom properties to request areas.
- **Templates:** Allows you to create a template (see page 2315) using the current ticket as a model.
- **Support Automation:** Displays the assistance session log and lets you invite the end user to an assistance session.

Edit Service Targets for a Request

This article contains the following topics:

Service targets determine whether Service Level Agreements (SLA) have been met within the required time frame. If a service type has a set of service targets, you can view the status and deadlines for completing each target on the ticket. If necessary, you can update or override service target values such as Workshift.

Follow these steps:

1. On the Service Desk tab, select Incidents, Problems, Requests, Change Orders, or Issues.
   The ticket detail page appears.
2. Click the Service Type tab.
   Additional Service Type information appears at the bottom of the ticket.

   Note: Service targets appear on tickets that meet the conditions that the Administrator sets up. Priority calculation can be a factor in how target information calculates and displays.
3. In the Target column, click the target.
   The Service Target Detail page appears.
4. Click Edit.
   The Update Service Target page appears.
5. Complete the following fields as appropriate:
   - **Name**
     Identifies the service target.

- **Target Duration**
  Specifies the amount of allotted time to perform the service target. You can only override this value by editing the ticket.

- **Workshift**
  Displays the schedule to use for service target time calculations.

- **Condition**
  Specifies the name of the condition or site-defined condition. The condition evaluates the ticket data to determine whether the service target is met.

- **Required Outcome**
  Displays the required result of the condition or site-defined condition Macro.

- **Cost**
  Specifies the penalty that incurs for missing the target. This information also displays on the ticket.

- **Target Date/Time**
  Specifies the deadline for completing the target. If the ticket is in a Hold status or the target has been met, this field is blank.

- **Actual Date/Time**
  Specifies the date and time that the condition was satisfied or the user clicked Set Actual.

- **Time Left**
  Specifies the amount of remaining time for the service target. A negative value indicates the amount of time that exceeded the target time frame.

- **Allow Set Actual**
  Lets the users set the date and time of a service target.

- **Allow Reset Actual**
  Lets the users reset the service target.

- **Last Modified Date/Time**
  Displays the date that this ticket was last modified.

- **Service Type**
  Displays the Service Type that is attached to this service target.

- **Service Target Template**
  Specifies the name of the service target template to link to the service type.

- **Last Modified By**
  Displays the name of the last person who edited the ticket.

- **Lock Target Date/Time From Hold Recalculations**
  Prevents automatic target date and time updates when the ticket goes on hold or when the ticket is delayed.

6. Click Save.
   The system saves and updates the service target.

View Ticket Counters and Timers for Service Targets

If an analyst assigned a set of service targets to a ticket, you can view the status and deadlines for completing each target.

Follow these steps:

1. On the Service Desk tab, display a list of Incidents, Problems, Requests, Change Orders, or Issues.
   The ticket detail page appears.

2. Click the Service Type tab.
   Additional Service Type information appears at the bottom of the ticket.

3. In the Target column, click the Service Target for additional information.
   The Ticket Counters and Timers section appears near the bottom of the Assigned Service Target Detail page. The Assigned Service Target Detail page displays the following fields:

   - **Name**
     Displays the name of the service target.

   - **Target Duration**
     Displays the amount of allotted time to perform the service target. You can only override this value by editing the ticket.

   - **Workshift**
     Displays the schedule used for time calculations for the service target.

   - **Condition**
     Displays the condition or site-defined condition macro that evaluates the ticket data to determine whether the work can complete within the target time frame.

   - **Required Outcome**
     Displays the required result of the condition or site-defined condition Macro.

   - **Cost**
     Displays the penalty that incurs for missing the target. This information also displays on the ticket.

   - **Target Date/Time**
     Displays the deadline for completing the target. If the ticket is in a Hold status or the service target has been met, this field is blank.

   - **Actual Date/Time**
     Specifies the date and time that the condition was satisfied or the user clicked Set Actual.

   - **Time Left**
     Displays the amount of remaining time for the service target. A negative value indicates the amount of time that exceeded the target time frame.

- **Allow Set Actual**
  Displays whether you can set the actual time. Yes indicates that you can set the Actual Date/Time of a Service Target. No indicates that you cannot override the Actual Date /Time.

- **Allow Reset Actual**
  Displays whether you can restart the time. Yes indicates that you can reset the Actual Date /Time of a Service Target. No indicates that you cannot reset the Actual Date/Time.

- **Last Modified Date/Time**
  Displays the date that this ticket was last modified.

- **Last Modified By**
  Displays the name of the last person who edited the ticket.

- **Service Type**
  Displays the name of the service type that attached this service target.

- **Service Target Template**
  Displays the name of the service target template that was linked to the service type that was used to create this Service Target.

- **Lock Target Date/Time From Hold Recalculations**
  Locks the Target Date/Time from being automatically updated when the ticket goes on hold or is delayed.

- **Last Start Date/Time**
  Displays the last time the service target timer was started.

- **Ticket Status**
  Displays the value of the Status field of the ticket.

- **Hold Status**
  Displays whether the ticket status has placed the ticket on hold.

- **Last Hold Date/Time**
  Displays the last time that the ticket was placed on hold.

- **Hold Count**
  Displays the number of times the ticket was placed on hold.

- **Last Resolved Date/Time**
  Displays the last time that the ticket transitioned to a resolved status.

- **Resolved Count**
  Displays the number of times that the ticket changed to resolved status.

- **Last Closed Date/Time**
  Displays the last time the ticket was changed to a closed status.

- **Closed Count**
  Displays the number of times the ticket was changed to a closed status.

- **Ticket Open Date/Time**
  Displays the date and time the ticket was opened.

- **Ticket Resolved Date/Time**
  Displays the date and time the ticket was resolved.

- **Ticket Closed Date/Time**
  Displays the date and time the ticket was closed.

View Service Target Status

On an open ticket, you can view the status for each service target. Status information such as Time Left and Violation Cost help you prioritize your work.

Follow these steps:

1. On the Service Desk tab, display a list of Incidents, Problems, Requests, Change Orders, or Issues.
   The respective ticket list displays with the following Service Target information:

   - **Service Target**
     Displays the time that the next service target is due.

   - **Projected Violation**
     Displays the incurred cost when the service type time limit is violated.

2. Select the ticket that you want from the list page.
   The ticket detail page appears.

3. Select the Service Type tab.

   Note: Service targets appear on tickets that meet the conditions that the administrator sets up. Priority calculation can be a factor in how target information calculates and displays.

   If the ticket meets predefined target conditions, the Service Targets List the following information about service targets:

   - **Action**
     Sets or resets the Actual Date/Time to the current date and time.

   - **Target**
     Specifies the current service target for the ticket.

   - **Target Date/Time**
     Specifies date and time when this service target is due. If the ticket is in a Hold status, this value is blank.

- **Actual Date/Time**
  Specifies the time when the target condition was met. If no value appears, the target condition has not been met.

- **Time Left**
  Specifies the amount of remaining time for the service target when the ticket is on hold. If the service target has been met, the Time Left field shows the unused time. A negative value indicates the amount of time that elapsed since the missed target date.

- **Violation Cost**
  Displays the penalty that incurs for missing the target. This information also displays on the ticket.

Create a Parent/Child Relationship for Requests

This article contains the following topics:

Records that are entered in the CA SDM system can be related to other records that are entered into the system. For example, a problem could result in two more problems when you attempt to resolve the original problem. The original record is referred to as the *parent*, and the additional records are referred to as *children*.

You can record such relationships in the CA SDM system for future references. The Parent/Child tab on the ticket detail page lists the parent and children tickets of a ticket.

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.

2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.

3. Open the desired ticket from the list that appears.

4. Select the Parent/Child tab and click Update Children.
   The search page opens.

5. Complete one or more of the search fields for related ticket records, and click Search.
   A list of tickets matching the search criteria are displayed.

6. Select the related tickets from the list on the left, and click  .
   The selected tickets are added to the list on the right.

7. When all related tickets are in the list on the right, click OK.
   The detail page displays with the selected tickets listed on the Parent/Child tab.

Close All Children

You can close all the children tickets before closing the parent ticket.

Follow these steps:

1. Select the appropriate ticket type from the Scoreboard. For example, select Requests.
2. Open the parent ticket.
3. Click the Action menu and select Close All Children.

Use Knowledge to Resolve a Request

This article contains the following topics:

You can search the CA SDM Knowledge Base to help resolve a ticket, such as an incident, problem, request, issue, or change order.

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.
3. Open the desired ticket from the list that appears.
4. Select the **Knowledge Management** tab.
5. Enter text in the search field to describe the problem, or copy text from the **Summary** or **Description** fields of the ticket.
6. From the drop-down list, select where you want to search.
7. Click **Search**.
   A list of documents matching the search criteria displays.
8. Look for the document that provides the solution to your ticket.
9. Right-click the document and select **Accept as Solution**.
   The knowledge document information is copied into the **Summary** and **Description** fields.

Submit a Knowledge Document

When you log a solution activity for a ticket, you can submit the solution to the knowledge base administrator as a candidate for publication.

Follow these steps:

1. Open a ticket, such as an Incident.
   The ticket detail page appears.
2. On the Knowledge tab, click Submit Knowledge.
   The Create New Document page displays.

For more information on creating knowledge documents, refer to Create Knowledge Documents (see page 2732).

After you submit a solution to the knowledge base, it becomes a candidate for publication in the knowledge base. A Knowledge Management administrator reviews the information and publishes it if it is deemed appropriate and accurate. After it is published, the information becomes available to other users.

Request Management Using CA Service Catalog

This section contains the following articles:

Approval Processes and Fulfillment Processes

Approval Processes

When a user submits a request, approvers must approve or reject each service in the request. For each service, the administrator specifies one of the following approval processes on the Service Details tab:

- **No Approval**
  Requires no approval. When a request containing the service is submitted, the status is changed to Approval Done.

- **System Approval Process**
  Determines the approver and the number of approval levels by using a combination of the following parameters:

  - The management hierarchy.
  - The authorization level of each user in the hierarchy.
  - The approval level that is specified for the service.

  When a request containing the service is submitted and the Requested For value is a user, not an account, the Catalog system:

  1. Finds the Requested For authorization level of the user in the user profile.
  2. Compares it with the approval level of the service.

If the authorization level of the user matches or exceeds the approval level that the service specifies, then no further approval is required. The system moves the request to the next status, typically Pending Fulfillment, or Completed.
Otherwise, then the system determines an approver, as follows:

- The Requested For value is a user. In this case, the system determines the manager of the user and assigns the request to that manager for approval.
- The user does not have a manager or the Requested For value is an account. The system assigns the approval task to the user-specified in the configuration option that is named Default User For Request Actions.

After the manager or other approver approves the service, the system uses similar logic to determine whether another level of approval is required. If yes, then the system routes the request to a request manager whose authorization level matches or exceeds the approval level of the service.

- **Workflow Driven Approval Process**
  Uses a CA Process Automation process to determine the approval process.
  The process includes the business logic to determine the approver and the number of approval levels. CA Service Catalog provides sample processes and process definitions, including default ones for a single level of manager approval.
  For any service, if you use this approval process with a CA Process Automation process, you can optionally use policies. In that case, the approval process proceeds the same as with Policy driven approval process, except as follows:
  - The Workflow driven approval process uses the CA Process Automation workflow engine to evaluate and implement policies.
  - Policy driven approval process uses the Catalog Policy Engine to evaluate and implement policies. This option is typically more efficient for an approval process because this engine is internal. Verify that the rules and actions are enabled (see page) for the option that you specify.
- **Policy driven approval**
  Uses a policy to determine the approval process for requests. You specify conditions in policies, which are based on the attributes of service options, services, requested items, and users. If a policy is active and a submitted request meets the condition in the policy, then the assignees in the policy receive a request pending action to approve, reject, or fulfill a service option, service, or request.

Policy driven approval and system approval use a few common terms. For example, in both methods, the *level of approval* refers to the authority of an approver in numeric terms: the higher the number, the greater the authority of the approver. However, in policy driven approval, the administrator assigns each approver and authority level uniquely, with no relation to system approval.

If a policy does not apply to a request, the Catalog system uses the approval flow as defined in the workflow driven approval process. For example, you are using the predefined workflow approval process. Also, no predefined sample policy applies to a request pending action. In that case, the Catalog system assigns request pending action to the manager of the Requested For user. If the user has no manager, then the system assigns the request pending action to the Default User for Request Actions. This user is specified in the Catalog Configuration.

Fulfillment Processes

Fulfillment is required for each service option included in the services in a request. When the status of a service option is set to Pending Fulfillment, it enters the fulfillment phase. When the status is set to Fulfilled or Fulfillment Cancelled, the service option leaves the fulfillment phase. For each service Approval Process setting, the fulfillment phase of the requested service options can be managed separately.

- No Approval and System Approval Process: After approval, the status of the service options for the service is set to either Fulfilled or Pending Fulfillment.
- Workflow Driven Approval Process: After approval, the status of the service options for the service is set to Pending Fulfillment.

When you set the requested service options status to Pending Fulfillment, a Workflow process definition manages the fulfillment process. Several process definitions manage the fulfillment process. These process definitions and associated event rules support three different approaches to fulfillment.

Generally, fulfillment options do not fit your business processes. More commonly, alter the distributed components to more accurately fit your business processes. Before altering the existing components or adding to them, it is important to understand what they do.

Note: Enabling all the rules that are related to all the options is not recommended, because the fulfillment options overlap.

- **Complex Fulfillment**
  This process considers the current status value of the service option and new status being assigned to determine the next step in the fulfillment process. The Complex Fulfillment process supports major fulfillment phases that are related to:
  - Checking availability of the requested service option when initially requested or when the service option status is Received.
  - (Optional) Opening a CA Service Desk Manager Change Order (for Hardware or Software) or notifying appropriate fulfillment personnel when the service option is found in the available inventory.
  - Notifying Procurement of the requested service option when it is not found in available inventory. In this case, the service option is ordered and marked as Received when it arrives.
- **Simple Fulfillment**
  This process notifies the appropriate fulfillment personnel that the item must be fulfilled with no special regard for fulfillment phases.
- **CA Service Desk Manager Request Fulfillment**
  This process:
  - Opens a CA Service Desk Manager request.

- Notifies the appropriate fulfillment personnel that the service option must be fulfilled.
- Lays responsibility of the fulfillment process on the CA Service Desk Manager request logic.

Status Values

On a viewed request, the name of the current status displays in the Status column or Status drop-down list. To display other available statuses, click the list. Optionally, change the request to a new status, such as Approved, Cancelled, or Fulfilled. To change the request, click its status.

The following table shows the number, name, and meaning of the default statuses of Service Accounting Component and CA Service Catalog. The number of a status does not appear in the drop-down list. However, the number is used in the requeststatus.xml file. This file contains specifications for all default statuses and any customized statuses. Optionally, create new statuses and customize the statuses in the drop-down list by editing the requeststatus.xml file.

Some text in this table refers to the two request fulfillment models: simple and complex. In certain situations, the request flow differs for each model. These differences, when applicable, are noted in the following table.

Number	Name	Meaning
2	Completed	Catalog system-assigned status. When a request finishes with approval and fulfillment cycles, it reaches a Completed status. Once completed, the underlying request subscription reaches an active subscription status.
3	Pending Cancellation	This status applies when: ▪ CA Service Catalog is installed. ▪ Service is not subscribed. ▪ The default Cancellation status under Accounting, Configuration is set to Pending Cancellation. On cancellation, a request first attains the Pending Cancellation status. Then, after an invoice is run, it attains Cancelled status. If a request attains the complete state and is cancelled, then the request stays in pending cancellation state until the invoice is run.
4	Cancelled	A request attains this status on cancellation. A request does not attain Cancelled status when the Service Accounting Component is installed and the default Cancellation status is Pending Cancellation. The default Cancellation status is set under Accounting, Configuration.
6	Pending Resource Assignment	This status applies only when: ▪ CA Business Service Insight is integrated. ▪ A request that includes a service option of type application or agreement reaches Fulfilled status. Such a service option requires provisioning; therefore, the request is moved to Pending Resource Assignment status.
7	Resource Assigned	This status applies only when a request is at Pending Resource Assignment status. Once the service option in such a request is provisioned, the request moves to Resource Assigned status.

Number	Name	Meaning
100	Not Submitted	This status is user-initiated. When creating a request, optionally, click Save as Request to save the request in Not Submitted status. This option is an alternative to submitting the request.
101	Not Submitted - Cart	This status is Catalog system-assigned. This status is attained when a request item is added to the cart. **Note:** This status appears only in reports, not on the GUI.
103	Not Submitted - Rejected	This status is system-assigned. After a service in a request is rejected, the request eventually reaches a Not Submitted - Rejected status. The request is returned to the open queue of the requestor for review, modification, and resubmission.
104	Not Submitted - Approved	This status is catalog system-assigned. When the same request contains both approved and rejected services, the approved services eventually reach a Not Submitted - Approved status. This status helps the user to differentiate between a previously rejected request items and approved request items. In this case, the entire request is in Not Submitted - Rejected status.
200	Submitted	This status is user-initiated. A request reaches this status when a requestor submits the request. For each service in the request, the configured approval process type drives three scenarios: ▪ For the Workflow driven approval process, a rule action is triggered to activate the approval process. This process determines the approver for the service and changes the status to Pending Approval. ▪ For the System Approval process, the Catalog system determines the next action and status. This determination is based on: ▪ The approval level that is assigned to the service. ▪ The management hierarchy of the user for whom the service is requested. ▪ For the No approval process, if the service is configured for fulfillment, then the status eventually changes to Pending Fulfillment. If the service is not configured for fulfillment, then the status eventually changes to Fulfilled. When all services in the request reach the Fulfilled status, the request reaches the Completed status.
201	Re-submitted	This status is User-initiated. When a rejected request is submitted, it reaches a Re-submitted status. The eventual flow is similar to Submitted status.
400	Pending Approval	This status is Catalog system-assigned. A request reaches this status when one or more services in a request require approval. For each service in the request, the configured approval process type drives two scenarios: ▪ For the Workflow driven approval process, a rule action is triggered to activate the approval process. This process determines the approver for the service and changes the status to Pending Approval. By default, all Catalog Content services use the Workflow driven approval process. ▪ For the System Approval process, the Catalog system determines the next action and status. This determination is based on: ▪ The approval level that is assigned to the service. ▪ The management hierarchy of the user for whom the service is requested.
600		

Number	Name	Meaning
	Rejected	This status is User-assigned. If a service in the request is configured for approval, a pending action is assigned to the approver. The approver can optionally either approve or reject each service in the request. The entire request is rejected when a service is rejected. Then, the request is returned to the queue of the requestor for review, modification, and resubmission.
800	Approved	This status is User-assigned. If a service in the request is configured for approval, a pending action is assigned to the approver. The approver can either approve or reject each service in the request. When you approve a service, the status can either: ▪ Attain Approval Done status ▪ The status can get reassigned to Pending Approval status, when further approval is required. When all services in the request have received all required approvals, the request reaches the Approval Done status.
801	Approval Not Needed	This status is Catalog system-assigned. If a service in the request is configured for no approval, then the service reaches this status after the request is submitted. The service eventually reaches Approval Done status.
999	Approval Done	This status is Catalog system-assigned or workflow-assigned. When all required approvers approve a service in a request, that service attains Approval Done status. When all services in a request attain Approval Done status, the entire request is approved. The request eventually reaches Approval Done status. The next status after Approval Done is either Pending Fulfillment or Fulfilled. ▪ Using Pending Fulfillment allows for more fulfillment business processes to be followed by using CA Process Automation processes. ▪ If the request does not require fulfillment, then it reaches a state of Fulfilled.
1000	Pending Fulfillment	This status is Catalog system-assigned or workflow-assigned. In a request containing multiple services, the services can belong to any or all of the following categories: ▪ If a service in the request is configured for fulfillment, then a fulfillment process is triggered. This process determines the fulfiller for the service option and changes its status to Pending Fulfillment. Using Pending Fulfillment allows for more fulfillment business processes to be followed. If the request does not require fulfillment, then it reaches a state of Fulfilled. Once the service is configured for Pending Fulfillment, one of the following actions occurs: ▪ If a service option in the request is configured for simple fulfillment, then a fulfillment process is triggered. The status is set to Pending Fulfillment. ▪ If a service in the request is configured for complex fulfillment, then a fulfillment process is triggered. The status is set to Check Availability.
1001	Check Availability	This status is Workflow-assigned. This status applies when the Catalog system is configured for complex fulfillment. If a service option in the request is configured for fulfillment and it belongs to a hardware or software category, then an associated rule action triggers a fulfillment process definition. The process definition typically assigns a pending action to an IT Services User (that is, a fulfiller). The fulfiller can:

Number	Name	Meaning
		▪ Choose between Filled from Inventory and Not Filled from Inventory. ▪ Bypass fulfillment completely by selecting Fulfillment Cancelled or Fulfilled.
1002	Filled From Inventory	This status is User-assigned. This status applies when the Catalog system is configured for complex fulfillment. If an IT Services user is assigned a service option that is in Check Availability status, then the fulfiller can choose between Filled from Inventory and Not Filled from Inventory. This status is set in one of the following ways: ▪ If CA APM is integrated with CA Service Management, then this status is set when a CA APM user assigns an asset. ▪ If CA APM is not integrated with CA Service Catalog, then the IT Services user: ▪ Verifies that the requested items are available. ▪ Sets manually the status to Filled from Inventory.
1003	Not Filled From Inventory	This status is User-assigned. This status applies when the Catalog system is configured for complex fulfillment. If an IT Services user is assigned a service option that is in Check Availability status, then the fulfiller can choose between Filled from Inventory and Not Filled from Inventory. This status is set in one of the following ways: ▪ If CA APM is integrated with CA Service Catalog, then this status is set when an asset is not available in CA APM. ▪ If CA APM is not integrated with CA Service Catalog, then the IT Services user sets manually the status to Not Filled from Inventory when one or more requested items are not available. When the status of the service option is set to Not Filled From Inventory, then the status eventually reaches Pending Procurement. The requested hardware or software must then be ordered.
1004	Ordered	This status is User-assigned. This service option status applies when the Catalog system is configured for complex fulfillment. Once the status is set to Pending Procurement, then the IT Services user sets its status to the actual status of the ordered item, such as Ordered.
1005	Backordered	This status is User-assigned. This service option status applies when the Catalog system is configured for complex fulfillment. Once the status is set to Pending Procurement, then the IT Services user sets its status to the actual status of the ordered item, such as Backordered.
1006	Shipped	This status is User-assigned. This service option status applies when the Catalog system is configured for complex fulfillment. Once the status is set to Pending Procurement, then the IT Services user sets its status to the actual status of the ordered item, such as Shipped.
1007	Received	This status is User-assigned. This service option status applies when the Catalog system is configured for complex fulfillment. Once the status is set to Pending Procurement, then the IT Services user sets its status to the actual status of the ordered item, such as Received. If the status of the service option is set to Received, then it eventually reaches a status of Check Availability for re-assignment. This re-assignment is performed by an IT Services user or by a CA APM user (if CA APM is integrated with CA Service Catalog).

Number	Name	Meaning
1008	Order Cancelled	This status is User-assigned. This service option status applies when the Catalog system is configured for complex fulfillment. Once the status is set to Pending Procurement, then the IT Services user sets its status to the actual status of the ordered item, such as Order Cancelled. If the status of the service option is set to Order Cancelled, then it eventually reaches a status of Check Availability for re-assignment. This re-assignment is performed by an IT Services or user or by a CA APM user (if CA APM is integrated with CA Service Catalog).
1012	Pending Procurement	This status is User-assigned. This status applies when the Catalog system is configured for complex fulfillment. If the status of the service option is set to Not Filled From Inventory, then it eventually reaches a status of Pending Procurement. The requested hardware or software must then be ordered.
1013	CA SDM Change Order Opened	This status is Workflow-assigned. This status applies when the Catalog system is configured for complex fulfillment and a rule action for creating a CA Service Desk Manager change order is enabled. A status change occurs when the following actions occur: ▪ An IT Services user is assigned a service option in Check Availability status. ▪ The IT Services user then sets the status of the service option to Filled from Inventory. ▪ The CA Service Desk Manager is integrated with CA Service Catalog The status is then set to CA SDM Change Order Opened and a Change Order is created in the CA Service Desk Manager.
1015	Notified IT Services	This status is Workflow-assigned. This status applies when the Catalog system is configured for complex fulfillment. A status change occurs when the following conditions apply: ▪ An IT Services user is assigned a service option in Check Availability status. ▪ The IT Services user sets the status of the service option to Filled from Inventory. ▪ The CA Service Desk Manager is not integrated with CA Service Catalog. A process definition is triggered which assigns a pending action to an IT Services User and sets the status to Notified IT Services.
1016	Being Staged	This status is User-assigned. This service option status applies when the Catalog system is configured for complex fulfillment. Once the status is set to Notified IT Services, then the IT Services user sets its status to the actual status of the requested service option, such as Being Staged.
1017	Staged	This status is User-assigned. This service option status applies when the Catalog system is configured for complex fulfillment. Once the status is set to Notified IT Services, then the IT Services user sets its status to the actual status of the requested service option, such as Staged.
1018	Being Configured	This status is User-assigned. This service option status applies when the Catalog system is configured for complex fulfillment. Once the status is set to Notified IT Services, then the IT Services user sets its status to the actual status of the requested service option, such as Being Configured.
1019		

Number	Name	Meaning
	Configured	This status is User-assigned. This service option status applies when the Catalog system is configured for complex fulfillment. Once the status is set to Notified IT Services, then the IT Services user sets its status to the actual status of the requested service option, such as Configured.
1020	CA SDM Request Opened	This status is Workflow-assigned. This service option status applies when the Catalog system is configured for simple fulfillment and a rule action for creating a CA Service Desk Manager change order is enabled. A status change occurs when the following conditions apply: ▪ An IT Services user is assigned a service option in Pending Fulfillment status. ▪ The CA Service Desk Manager is integrated with CA Service Management. The status is then set to CA SDM Request Opened and a request is created in CA Service Desk Manager.
1999	Fulfillment Cancelled	This status is User-assigned or Catalog system-assigned. This status applies when one of the following actions is true: ▪ The IT Services user sets the status to Fulfillment Cancelled when the service option does not require fulfillment. ▪ The Catalog system sets the status to Fulfillment Cancelled when a user cancels a request that has been approved but has not been fulfilled. If all services are set to Fulfillment Cancelled, then the request eventually reaches Cancelled status. If the request contains services with both Fulfilled and Fulfillment Cancelled status, then the request eventually reaches Completed status.
2000	Fulfilled	This status is User-assigned. This status applies when one of the following actions is true: ▪ The IT Services user sets the status of the service option to Fulfilled. ▪ The CA Service Desk Manager is integrated and the process definition in CA Service Desk Manager sets the status to Fulfilled. This occurs when an associated change order is closed in the CA Service Desk Manager. When all services are set to Fulfilled, the request eventually reaches Completed status. If the request contains services with both Fulfilled and Fulfillment Cancelled status, then the request eventually reaches Completed status.
3000	Hold	This status is User-assigned. This status applies when either an administrator or the Catalog system sets the status of the service option to Held. When an item is held, no status changes can occur to it until you change its status to Resume. If a service option is held, then the monitoring of time is stopped for any request SLAs attached to the service option. This stoppage prevents related SLA warnings and SLA violations from being issued inordinately.
4000	Resume	This status is User-assigned. This status applies when an administrator sets the status of a previously held service option to Resume. When resumed, service options that were formerly held move to a temporary Resume status before automatically moving back to their previous status before being put on Hold. When you resume a previously held service or service option, the monitoring of time is resumed for any request SLAs attached to the service or service option.

Subscriptions and Requests

You use the same service catalog for both subscriptions and requests. CA Service Catalog enables catalog users to request services. Service Accounting Component enables accounts in the catalog to have subscriptions.

Requests have a Requested For value. When you add services to your cart, the Requested For value is set to your user ID by default. As an administrator, you can change the Requested For value to be a user or account within your business unit scope. When you set the Requested For value to a user, you are also setting the value to the *user account* associated with the user.

Subscriptions apply to an account. You can optionally associate an account with a user. However, an account is not required to be associated with a user. As an administrator, you can manage subscriptions for an account within your business unit scope. Users who are not administrators can view subscriptions for their user account but cannot manage these subscriptions.

Request Service Levels and Reports

Three phases of the request life cycle are monitored: Approval, Fulfillment, and Completion. Each phase represents the time that is taken for a requested service option to move from one status to another.

- Approval - The duration of moving from **Submitted** to **Approval Done**.
- Fulfillment - The duration of moving from **Approval Done** to **Completed**.
- Completion - The duration of moving from **Submitted** to **Completed**.

For each service option, service providers can establish SLA warning and violation thresholds for each phase.

Example

This example uses the Standard Desktop service option. The fulfillment phase warning time is five days and the violation time is seven days. Therefore, the service provider expects that a standard desktop be fulfilled (configured, delivered, and set up) within five days. A violation occurs if the time frame exceeds seven days.

The violation setting for a service option displays in the catalog as the *estimated time to fulfill*. In this example, the estimated time to fulfill the Standard Desktop service is seven days.

Note: (optional) Set up reports to monitor other request life cycles phases by altering the STATUS_RANGES value that is used in a report data object.

Several report data views and underlying data objects enable you to monitor request service levels.

- **Request Fulfillment Data View**

This report accepts a date range and business unit. Each row represents one request. The columns represent the duration in days, hours and minutes to approve, fulfill, and complete the requests. The date range filters for requests whose initial creation is within the range specified. The business unit value filters for requests for a user or account from a business unit.

Display the Request Item Fulfillment subreport for the service options that are contained in the request by clicking the Request ID field.

- Yellow = Time durations that exceed the warning duration for the service option.
- Red = Time durations that exceed the violation duration for the service option.

- **Request Item Fulfillment Averages Data View**

  This report accepts a date range and business unit. Each row represents one service option. The columns represent the average duration in days, hours, and minutes to approve, fulfill, and complete the requests. The date range filters for requests whose initial creation date is within the range. The business unit value filters for requests for a user or account from a business unit.

  - Yellow = Average time duration exceeds the warning duration for the service option.
  - Red = Average time duration exceeds the violation duration for the service option.

Click the Service Option field to display the Request Item Fulfillment report. This sub-report displays requests containing the service option.

- Yellow = Time durations that exceed the warning duration for the service option.
- Red = Time durations that exceed the violation duration for the service option.

Request Management from an Administrator Perspective

Requests have a life cycle reflected in their status. The status of a request falls into one of the following several phases:

- Not Submitted
- Submitted
- Approval
- Fulfillment
- Completed

For the request and its services and service options to move through the request life cycle, its status must change.

The requesting user controls the **Not Submitted** phase. A request is in the Not Submitted phase when one of the following conditions is true:

- The request is in the user's cart.

- The user has saved the cart as an unsubmitted request.
- The submitted request has been rejected.

> **Note:** The user must submit the request or cart before the request can exit the **Not Submitted** phase.

The **Submitted** phase is brief and controlled by the system. Each service option in the request has a specified approval process. The submitted phase is used only until the approval process begins.

An approving user or the system controls the **Approval** phase. This control depends on the approval process for each service in the request. All services in the request must be approved (or not require approval) before the request enters the Fulfillment phase. If any services are rejected, the entire request is returned to the Not Submitted phase for the requesting user to manage.

A fulfilling user or the system controls the **Fulfillment** phase. This control depends on the fulfillment process for each service option in the request. Set the status of all service options in the request to either Fulfilled or Fulfillment Cancelled before the request enters the Completed phase.

An administrator or the system controls the **Completed** phase. This control depends on the type of service option elements requested.

- If CA Business Service Insight is integrated and the request includes an Agreement service option element that depends on resource metering, then:
  - The status of the service option is changed to Pending Resource Assignment.
  - When a resource is assigned, the status changes to Completed.
- For other types of service options elements, the status is set to Completed. After the status is set to Completed and if Service Accounting Component is installed, invoices then include the service option.

Enable Approval and Rejection of Multiple Items Simultaneously

Administrators enable *multi-item approval* so that request managers can simultaneously approve and reject multiple items in a request. Examples include all services in a request or all service options in a service. Multi-item approval lets request managers process requests quickly and efficiently, especially when they are already familiar with the requests:

- Request managers access their requests pending action, select the services that they want to act on. Then, they click Approve or Reject. Multi-item approval provides this ability *regardless* of whether discrete approval (see page 2120) is implemented.
  Without multi-item approval, request managers must approve or reject every service *individually* by updating its status in the Status drop-down list.
- If discrete approval is implemented, request managers approve or reject multiple *service options* in a service simultaneously, as follows: Request managers access their requests pending action and open the services. In each service, they select the service options that they want to act on, and click Approve or Reject.

- If discrete approval is implemented *without* multi-item approval, request managers can approve or reject each service option *individually* by updating its status in the Status drop-down list.

The benefits of multi-item approval are more pronounced as the number of services or service options in a request increases. Multi-item approval is especially helpful for mobile users, who have limited space and typically have limited time.

Follow these steps:

1. Click Catalog, Configuration, Request Management, and verify that the following option is enabled: Allow Multi Service/Service Option Approval.
2. Verify whether you have implemented discrete approval.
3. Inform request managers of the new approval option for your implementation:
   - Multi-item approval only
   - Multi-item approval and discrete approval
4. Verify that multi-item approval functions as you intended.

Requests with Multiple Approval or Rejection Statuses

The default statuses of the request life cycle (see page 2108) include these statuses: Approved and Rejected. When request managers approve or reject a service option or service, the status of the item changes accordingly. The changed status is displayed to request managers before they confirm their approval or rejection of services or service options. If an approval or rejection changes change the default status, the Catalog system highlights the service or option in green.

Catalog administrators can optionally create custom approval and rejection statuses, such as Approved - Manager, Approved - Finance, Rejected - No Budget. To define custom statuses, edit the requeststatus.xml file. For more information, see the Modify the Request Status List (see page 2006) section.

If one or more custom statuses exist for this service or service option, the Catalog system performs the following actions:

- Displays an informational message that multiple statuses exist.
- Selects the first custom status that is defined in requeststatus.xml file.
- Highlights the service or option in orange.

For all status changes (custom or default), before confirming the approval or rejection, request managers can choose one of these options:

- Accept the status changes
- Update one or more statuses, for example, from a custom status to a default status

Services or options that are not selected are not highlighted and do not change status. They remain as pending items in the request until they are either approved or rejected.

Implement Discrete Request Life Cycle

This article contains the following topics:

The predefined CA Process Automation processes supplied for use with CA Service Catalog require *no* additional configuration to support the discrete request life cycle. However, verify that they work efficiently with the discrete request life cycle after you implement it.

Minimize impact on requests in progress by following the best option for introducing the use of discrete life cycle.

- Instruct the users to stop creating requests in your organization temporarily. When most or all of the requests in progress are completed, begin using a discrete life cycle by setting the related configuration parameters.

- In-progress requests may become stuck as a result of the configuration changes. If the requests become stuck, retry or override (push-through) the alerts (see page 2218) to complete the requests.
  Retries and overrides may be required when you use the configuration setting Allow Discrete Handling of Service Options After.

- Give special attention to canceled items, rejected items, and items pending fulfillment while others are still in pending approval, when one or both of the following are true:

  - You expect some requests to reach pending fulfillment after all the items are approved.

  - You expect to reject the entire request if one item is rejected.

  In these cases, take special care before changing the configuration to support the discrete request life cycle. Verify that such requests have completed before you make the configuration changes.

- Review the following important considerations:

  - Overall status of the request
    The service option with the lowest status value (see page 2108) determines the overall status of the request. To see the status of a request, click Home, Requests, and, if applicable, use the My Requests drop-down list to display requests. Open the request, and view the status.
    When the request contains services and service options having different status values, the lowest status value appears with asterisk (*) next to it, indicating that at least one service or service option in the same request has a higher status. When determining the overall status of the request, the Catalog system ignores services and service options that are rejected, completed, deleted, cancelled, pending cancellation, or on hold.

  - Billing
    If you are using Service Accounting Component, the invoices you generate (see page 3114) *do* include completed services and service options, even if other services and service options in the same request are not completed. The uncompleted services and service options are *not* included in the same billing run as the completed ones.

- Request SLAs
  This point is relevant only if you use request SLAs. The monitoring and recording of request SLA data is not affected when you use a discrete request life cycle. The Catalog system monitors and records the status changes of service options that have request SLAs the same way, regardless of your discrete request life cycle configuration settings.

- CA Business Service Insight-related metrics
  This point is relevant only if you are integrating CA Service Catalog with CA Business Service Insight. Your discrete request life cycle configuration settings do not affect the monitoring and recording of any CA Business Service Insight contract-related metrics that are associated with service options in the Catalog system.

Understand the Discrete Settings

The following table shows whether the request manager acts on a service, service option, or either one, based on the settings for Allow Discrete Handling of Service Options After (ADHSOA).

The table applies to all settings of Allow Discrete Request Life Cycle After.

Request Manager Action	ADHSOA=Submitted	ADHSOA=Pending Fulfillment	ADHSOA=Completed
Approve or Reject	service option	service	service
Hold or Resume	either	either	either
Transfer or Delegate	service option	**A**-service **B**-service option	service
Override	service option	**A**-service **B**-service option	service
Take or Return	service option	**A**-service **B**-service option	service
Pus-Through	service option	**A**-service **B**-service option	service
Cancel	service	service	service
Fulfillment Cancelled	service option	service option	service
Fulfill	service option	service option	service
CA Service Desk Manager Change Order	service option	service option	service

A-service, from Submitted status through Approval Done -service option, from Pending Fulfillment status through Fulfilled status.status.**B**

Set the Configuration Parameters

To enable the discrete handling of requests pending action, set the related configuration parameters. You can use these configuration parameters individually. However, they are most effective when you use them together to achieve the desired request processing.

Follow these steps:

1. Click Catalog, Configuration, Options, Request Management Configuration.

2. Set the following parameters:

- **Allow Discrete Handling of Service Options After**
  Specifies the status at which request managers can discretely (individually) approve, reject, or fulfill each service option in every service in the request. Use this parameter to specify that pending actions are assigned at the service option level, rather than the service level.
  The setting that you specify applies to the request *from* the starting status that you specify *through* the remainder of the request life cycle.
  Valid values: Submitted, Pending Fulfillment, or Completed
  Default: Pending Fulfillment

- **Allow Discrete Request Life Cycle After**
  Specifies the status at which individual service options in a service and individual services in a request advance to further statuses in the request life cycle independently. When the request reaches the specified status, the service options that you approve or fulfill can complete the remainder of the request life cycle. These service options complete the remainder of the request life cycle even if other service options in the same service are not acted on.
  When the request reaches the status that you specify, the services that you approve or fulfill can complete the remainder request life cycle, even if other services in the same request are rejected or not acted on.
  Valid values: Submitted, Pending Fulfillment, or Completed
  Default: Completed

- **Allow Discrete Handling for Reject**
  This parameter specifies the effect of the rejection of a single service or service option upon other services and service options in the same request:

  - **Yes**: When rejecting a service or service option, the remaining services or service options can advance if they are approved. Other services in the same request can advance in the request life cycle if they are approved. Similarly, other service options in the same service can advance in the request life cycle if they are approved.

  - **No**: When you reject a service or service option, the entire request is rejected. All services in the same request are rejected and cannot advance in the request life cycle, even if they were previously approved. All service options in the same service are rejected and cannot advance in the request life cycle, even if they were previously approved.
    Default: No

Discrete Request Life Cycle Parameters

This article contains the following topics:

Administrators can implement a discrete request life cycle to enable services and service options to advance to higher request statuses *without waiting* for all other services and service options to reach the same statuses. Consequently, services and service options can reach Fulfilled and Completed statuses, and can be invoiced earlier than without a discrete life cycle, even if a request manager rejects one or more services or service options in the same request.

An administrator can optionally specify discrete settings for the request life cycle for individual business units, as follows:

- Depending on the configuration you choose, you can specify when the request managers (approvers and fulfillers) can discretely (individually) approve, reject, or fulfill each service option in every service in the request. The setting applies to the request *from* the starting status that you specify *through* the remainder of the request life cycle.
- The status of individual service options in a service and individual services in a request advance to further statuses in the request life cycle independently. Here, *independently* means *without* requiring or waiting for any other service options in the same service or any other services in the same request to advance to any further statuses. The setting applies to the request *from* the starting status that you specify *through* the remainder of the request life cycle.
- The effect of the rejection of a single service or service option upon other services and service options in the same request:
  - If this setting is Yes, when you reject a service or service option, the remaining services or service options can advance if they are approved.
  - If this setting is No, when you reject a service or service option, the entire request is rejected. Even other services or service options that were previously approved change to Rejected status and can not advance in the request life cycle.

Sample Settings and Their Meanings

For all examples, if the request manager rejects one or more services or services options in a request that includes other services and service options, the setting of Allow Discreet Handling for Reject configuration (see page 2119) determines effect of the rejection on the other service options and services in the request.

Examples for Allow Discrete Handling of Service Options After

The *Allow Discrete Handling of Service Options After* parameter specifies the status at which request managers (approvers and fulfillers) can handle requests pending action (approval, rejection, or fulfillment) discretely. When the request reaches the status you specify, request managers can discretely (individually) approve, reject, or fulfill each service option in every service in the request.

Example 1--Submitted

In this example, you want *both* discrete approval and discrete fulfillment. Thus, you want to approve or reject service options individually, rather than approve or reject *all* service options in the service in one action. Similarly, you want to fulfill service options individually, rather than fulfill *all* service options in the service in one action.

To achieve this goal, specify Submitted as the value for this parameter. When the user submits the request, approvers can approve or reject each service option in a service individually. Moreover, fulfillers can fulfill each approved service option individually.

To ensure that the request managers receive notification emails when they address pending actions:

- Set the *Allow Discrete Handling of Service Options After* parameter to Submitted.
- Keep the setting of Yes (predefined) for the parameter named *Notify users when they complete their own pending actions*.

For example, if a service has five service options and the request manager approves each option, the request manager receives five confirmation emails.

Example 2-- Pending Fulfillment

In this example, you do *not* want discrete approval but want discrete fulfillment. Thus, you do *not* want to approve or reject service options individually but rather want to approve or reject all service options in the service in one action. However, once the entire request is approved, you want to *fulfill* service options individually.

To achieve this goal, specify Pending Fulfillment as the value for this parameter. So, as soon as the entire request is approved, fulfillers can fulfill each approved service option in every service individually.

Example 3--Completed

In this example, you do *not* want discrete approval or discrete fulfillment. You do *not* want to approve, reject, or fulfill service options individually at any point during the request life cycle. Instead, you always want to approve, reject, or fulfill all services in the request as a single unit. To achieve this goal, specify Completed as the value for this parameter.

Essentially, this setting "turns off" discrete handling of approval and fulfillment activities. So, request managers must approve, reject, and fulfill all services in the request at once.

Examples for Allow Discrete Request Life Cycle After

The *Allow Request Life Cycle to Continue After* parameter specifies the status at which individual service options in a service and individual services in a request advance to further statuses in the request life cycle independently. Here, *independently* means *without* requiring or waiting for any other service options in the same service or any other services in the same request to advance to any further statuses.

Example 1--Submitted

For example, suppose that you want each service option in a service to advance to the remaining statuses in the request life cycle independently after being approved rather than requiring or waiting for any other service options in the same service to be approved. To achieve this goal, you specify Submitted as the value for this parameter.

As soon as the user submits a request, each service option in all services can advance independently to the remaining statuses in the request life cycle as soon as it (the service option) is approved, *without* waiting for any others to be approved or rejected.

Similarly, as soon as the user submits a request, each service in all requests can advance independently to the remaining statuses in the request life cycle as soon as it (each service) is approved *without* waiting for any others to be approved.

If an approver does not act on one or more service options, the approved service options in the same service can advance to the remaining statuses in the request life cycle. If an approver does not act on one or more services, the approved services in the same request can advance to the remaining statuses in the request life cycle.

Thus, with Submitted as the value for this parameter, the following results occur in a service that has two options: one approved and one no action, as follows:

Service Option	Approver's Action	Resulting Status
Option-1	Approve	Pending Fulfillment
Options-2	No action	Pending Approval

After all service options in the same service are approved, the service reaches Pending Fulfillment status.

After all services in the same request are approved, the request reaches Pending Fulfillment status.

Example 2--Pending Fulfillment

For example, suppose you want each service option in a service to be able to advance to the remaining statuses in the request life cycle independently after all services in the request are approved. To achieve this goal, you specify Pending Fulfillment as the value for this parameter.

So, as soon as the service is approved, it reaches Pending Fulfillment. Each service option in the service can advance independently to the remaining statuses in the request life cycle independently. Similarly, as soon as the request is approved, it reaches Pending Fulfillment, and each service in the request can advance independently to the remaining statuses in the request life cycle independently.

A setting of Pending Fulfillment as the value for this parameter differs from a setting of Submitted in these ways:

- Approved service options *cannot* advance to the remaining statuses in the request life cycle *until* all other service options in the same service are approved.
- Approved services *cannot* advance to the remaining statuses in the request life cycle *until* all other services in the same request are approved.

Thus, with Pending Fulfillment as the value for this parameter, the following results occur in a service having two options. The two are approved sequentially, as follows:

Service Option	Approver's Action	Resulting Status
Option-1	Approve	Approval Done
Option-2	Approve	Pending Fulfillment
Option-1	Fulfilled	Completed
Option-2	Fulfilled	Completed

After all service options in the same service are approved, the service reaches Pending Fulfillment status.

After all services in the same request are approved, the request reaches Pending Fulfillment status.

Example 3--Completed

In this example, you do *not* want individual service options in a service or individual services in a request to be able to change statuses independently of each other at any point in the request life cycle.

Instead, you always want complete services and complete requests to change statuses *only* as a single unit, not independently. To achieve this goal, specify Completed the value for this parameter.

Essentially, this setting "turns off" any possibility of service options in a service or services in a request changing statuses independently of each other at any point in the request life cycle.

Common Settings

The following points apply to all combinations of the *Allow Discrete Handling of Service Options After* and *Allow Discrete Request Life Cycle After:*

- If *Allow Discrete Handling for Reject* is No and you reject any service or service option, the entire request is rejected. The request life cycle stops immediately. After the rejection, the following status changes occur:
  - The status for the entire request changes to Not Submitted - Rejected.
  - Previously approved service options change to Not Submitted - Approved status.
  - All other service options move to Not Submitted - Rejected status.

  The requestor can optionally modify and resubmit the request.
  However, if this setting is Yes and you reject any service or service option, the remaining services or service options continue their request life cycle according to settings for the *Allow Discrete Handling of Service Options After* and *Allow Discrete Request Life Cycle After* parameters, as specified in the tables.
- If the request manager rejects one or more services or services options in a request that includes other services and service options, the setting of *Allow Discreet Handling for Reject* determines effect on the other service options and services in the request, regardless of whether the other services and service options were previously approved.
- The Perform Action icon or button appears on the GUI in all cases, except when *Allow Discrete Handling of Service Options After* is set to Pending Fulfillment and *Allow Discrete Request Life Cycle After* is set to Completed.
  When you click the Perform Action, a new page opens, enabling you to perform all applicable actions for each service or service option in the request, such as approve, reject, fulfill, transfer, delegate, take, return.

Use Policies to Manage Requests

This article contains the following topics:

CA Service Catalog administrators can create policies. Policies define conditions for automatically designating specific users as the assignees for a task during the request life cycle. The most common use is to define conditions for automatically assigning specific approvers for services and service options in a request pending action.

Policies provide the flexibility to assign tasks (such as approval or rejection of requests pending action) to users *other than* the managers of the requestor. However, you can optionally include these managers in your list of assignees.

The policy that you create consists of the following main components:

- The condition under which the policy applies
- The assignment to occur if the condition is met.
  If the condition is met, the user or users you specify are assigned to perform a pending action. You can specify the list of assignees according to any of several attributes, including but not limited to:
  - User name (first name and last name)
  - Membership in a user group
  - Management hierarchy, meaning the manager of the user, the manager of that manager
- An active-or-inactive setting
- Description and priority fields

You create *global* policies and global actions for general use with any service. In contrast, you create *attached* policies and actions for use with a specific service option only. You can create an attached policy or action *only* from the Policies & Actions tab (see page 3018) of that service option.

Comparison to Events, Rules, and Actions

The conditions and actions that you specify in policies are similar to the rules and actions (see page 3040) that CA Service Catalog supplies in events. You can view and edit these events, rules, and actions by selecting Administration, Tools.

In both the cases, you specify conditions that become part of the request life cycle workflow in CA Service Catalog. In both cases, when a request meets the specified conditions, CA Service Catalog assigns the users that are specified in the policy. For example, suppose you create a policy that applies only to requests with cost greater than $100. When a user submits a request that meets this condition, the assignees that are specified in the policy are assigned a pending action to approve, reject, or fulfill the request.

The major difference is that events, rules, and actions are system wide. But, you can optionally specify policies to be either system wide or specific to a business unit.

Step 1 - Review the Criteria to Apply Policies to Individual Requests

CA Service Catalog matches policies to individual requests according to priority and business unit (tenant) level in the following order.

1. High-priority policies at the lowest level business unit (farthest from the root)
2. High-priority policies at the next lowest level business unit
3. High-priority policies at the remaining business unit levels, from the lowest though the highest (the root)
4. Low-priority policies at the lowest level business unit
5. Low-priority policies at the next lowest level business unit
6. Low-priority policies at the remaining business unit levels, from the lowest though the highest
7. When CA Service Catalog matches a policy to a request, it considers other policies *only* if they are at the same priority and business unit level.
8. If CA Service Catalog finds two or more policies at the same priority and business unit level, it assigns requests pending action to *all* applicable assignees from *all* applicable policies.

The Catalog system requires *all* approvals from these assignees to advance the request pending action to the next status in the request life cycle. To help avoid situations in which multiple policies and approvers apply to a single request pending action, create and maintain conditions to use specific criteria.

Step 2 - Create Folders for Policies

You can create and maintain folders (as needed) to store your policies. Organize policies in folders according to the business units and child business units to which they apply, using intuitive names. Similarly, suppose that the policies apply to all business units. In that case, you can organize them according to categories under a folder that is named For All Business Units.

Follow these steps:

1. Click Catalog, Policies.
2. Add a folder, as follows:
   a. Select the folder to which you want to add the new folder and click Add, Folder.
   For example, to add a folder to the root folder (the Policies folder), select it and click Add Folder.
   b. Enter the name of the new folder and click OK.
   The folder is created and appears under the parent folder.

You can create, rename, move, copy, and delete folders.

Note: The names of folders are case-aware, but not case-sensitive. Thus, when you rename a folder, change more than the case. For example, you cannot rename an existing folder from spg policies to Spg Policies or SPG POLICIES.

Step 3 - Enable Rules and Actions for Policies

Policies require an engine. The rules and actions that you enable depend on the engine you use. On the Details Tab (see page 2997) for any service that wants to associate with a policy, you specify the approval process as *one* of the following options:

- Enable policy rules and actions for CA Process Automation (see page 2127).
  Perform this task if any services in the catalog specify the Workflow driven approval process to apply policies. If your implementation uses CA Process Automation for approving and fulfilling requests, you can use CA Process Automation as the engine for policies.
- Enable policy rules and actions for the Catalog Policy Engine (see page 2128).
  Perform this task if any services in the catalog specify the Policy driven approval process to apply policies. The Catalog Policy Engine is part of the Policy Builder, and is available to all CA Service Catalog implementations. The Catalog Policy Engine does not require CA Process Automation. This approach is typically more efficient and therefore is typically preferred.

If necessary, copy and modify a predefined rule or action to specify a custom rule or action. If both options apply, then you can use either option as the policy engine for any service.

Enable Policy Rules and Actions for CA Process Automation

If any services in your catalog specify the Workflow driven approval process, enable the required rules and actions. If necessary, also enable the policy rules and actions for the Catalog Policy Engine.

Follow these steps:

1. Click Administration, Events-Rules-Actions.
2. Click the Event Type named *Request/Subscription Item Change*.

3. Select the rule *When Status is Submitted and Approval Process is driven by Workflow*.
   The Rule Details page for this rule appears. This rule is enabled by default. If it has been disabled, click the Enable button. This button appears on the Rules bar.

4. Select the action that is named Launch Policy Driven Approval SRF and click the Enable button.
   The Enable button appears on the Actions bar.

5. Click Done.
   The Event Details page appears.

6. To configure CA Service Catalog so that you can use policies to fulfill requests, using *simple* fulfillment, perform the following actions:

   a. Open the *When Status is Pending Fulfillment* rule. Do not exit the Event Type named Request/Subscription Item Change.

   b. Create a CA Process Automation action and select the Policy_Approval Start Request Form.

   c. Complete the parameters that appear.

   d. Specify the following parameters as indicated:

   e. **RequestStatusUponAssignment =1000**
      Specifies that the requested item is set to this status (Pending Fulfillment) when the request pending action is assigned.

   f. **RequestStatusUponSuccess =2000**
      Specifies that the requested item is set to this status (Fulfilled) when the request pending action is completed.

   The Policy_Approval Start Request Form supports *simple* fulfillment but does *not* support multilevel fulfillment and complex fulfillment. However, you can optionally create a CA Process Automation process that *does* support multilevel fulfillment and complex fulfillment. To do so, use the assignPolicyBasedPendingActions method in the web service named RequestService.

The rules and actions are enabled.

Enable Policy Rules and Actions for Catalog Policy Engine

If any services in your catalog specify the Policy driven approval process, enable the required rules and actions.

Follow these steps:

1. Click Administration, Events-Rules-Actions.

2. Click the Event Type named Request/Subscription Item Change.

3. Locate the rule *When Status is Submitted and Approval Process is driven by Policy*.
   This rule is enabled by default. If the rule is disabled, select its check box. Click Enable, and click OK.

4. Click the rule name.

5. Click the Edit icon for the action *Evaluates Policy Driven Approval Process*.
   The Edit Action page appears. This action is disabled by default.

6. Select Enabled in the Status drop-down list, and click OK.
   This action checks the policy setting on the Policies and Actions tab of each service option that triggers the action. According to that setting, the action evaluates global policies, attached policies, or both for the service option.

The rules and actions are enabled.

Step 4 - (Optional) Export and Import Policies

The IXUTIL command-line utility is an importing and exporting command-line utility that allows the preservation and migration of CA Service Catalog data between computers. You can use IXUTIL to export and import new and updated objects, including policies, from one computer to another. You can export and import policies in the following cases:

- When you upgrade or migrate CA Service Catalog.
- When you upgrade your computer.
- When the server fails.

Note: You can also use the Import Export Utility on the product UI to import and export policies.

Follow these steps:

1. Open the CA Service Catalog command prompt on any Catalog Component computer.

2. Enter one or more of the following commands:

   - To export all policies in all business units, enter the following command:

     ```
     ixutil export policy -f file
     ```

   - To export all policies in a business unit, enter the following command:

     ```
     ixutil export policy -f file - businessunit businessunit id
     ```

   - To export a single policy, use the following command:

     ```
     ixutil export policy -f file -policy name -businessunit id
     ```

     If the name contains spaces, enclose the name in double quotation marks.

```
ixutil export policy -policy "Mobile Device Policy--Tier 1" ...
```

- To export multiple policies, enclose the names in double quotation marks, and separate the names with commas.

```
ixutil export policy -policy "Mobile Device Policy--Tier 1,Mobile Device Policy--Tier 2,Mobile Device
Policy--Tier 3" ...
```

- To export a folder containing one or more policies, enter the following command:

```
ixutil export policy -f file -folder name -businessunit id
```

  To export multiple folders, enclose the names in double quotation marks, and separate the names with commas. Use the previous command for multiple polices as a model.

- To import a previously exported file containing one or more policies, enter the following command:

```
ixutil import policy -f file -businessunit id
```

  The -businessunit *businessunit id* option is optional when you import the policy file. However, consider the important factors explained in the description of this option later in this topic.

- To import a previously exported file containing one or more policies in disabled status, enter the following command:

```
ixutil import policy -f file -businessunit businessunit id -disable
```

3. Log in to CA Service Catalog on the computer where you imported the policies. If you had imported policies into a specific business unit, log in to the respective business unit.
4. Click Catalog, Policies.
5. Expand the policy folders. Verify that the Catalog system imported the policy or policies as you want.
6. Close the CA Service Catalog command prompt.

Step 5 - Create a Policy

Administrators create policies to assign approvers automatically for services and service options in a request pending action. In this way, you use policies to manage requests.

Follow these steps:

1. Click Catalog, Policies.
2. Select the folder to which you want to add the new policy and click Add, Policy.
3. Enter an intuitive name for the policy and click OK.

4. Enter meaningful descriptions in the policy fields for the policy that is created under the parent folder.

5. Select either High or Low in the Priority drop-down list.

> **Note:** When a user submits a request, CA Service Catalog checks for and the system applies any matching *high-priority* policies. Only if no high-priority policy applies to the request, the system checks for and applies any matching *low-priority* policies.

6. Select either Active (ready to use the policy) or Inactive in the Status drop-down list.

7. Save the policy.

Step 6 - Create Conditions for a Policy

Administrators create the condition as the major decision point of the policy. If the condition is met, the Catalog system automatically assigns the pending action to the assignees. You specify the condition using the attributes of CA Service Catalog elements such as users, requests, services, business units. In addition, you can use match functions for creating conditions that are based on service options and service option elements.

Create simple conditions that are based on known attributes, such as category, external_id, code, item type, cost, status. Specify the criteria that the value of the specified attribute must meet to assign the pending action.

The condition builder is the tool in the Condition field that helps you specify valid conditions, one segment at a time. When you initially move the cursor to the field, the condition builder prompts you with valid options for the first part of the condition. These options appear in a drop-down list under the Condition field. Select the option that you want from the list. As you complete each part of the condition, the condition builder continues to prompt you with valid options for the next part. This process continues until the condition is finished, typically with a closing parenthesis.

The condition must be a valid JavaScript expression. Typically specify one condition per policy, using the following format:

$(_.*group.attribute operator 'value'*)

- ***group***
  Specifies service, request, business unit, or any other group that is illustrated in the types of conditions (see page 2137).

- ***attribute***
  Specifies any attribute of that group

- ***operator***
  Specifies one of the following options:
  == (equal to)
  != (not equal to)

> (greater than)
< (less than)
>= (greater than or equal to)
<= (greater than or equal to)

- ***value***
  Specifies a literal value, typically the name of a business unit, request, service, service option group, or user.
  Enter numeric values without quotation marks, for example: $(_.request.bu.status==0).
  Enclose string values in single quotation mark; for example: $(_.request.bu.taxRegion =='South').
  If a string value includes a single or double quotation mark, precede that mark with a backslash (\) as the "escape" character. For example, if the service name is Demandes d'IP Statique, then specify the condition as follows:

  ```
  $(_.service.name=='Demandes d\'IP statique')
  ```

  As you construct an expression in the Condition Builder, the data type (string or numeric) of the attribute appears on the right, letting you know whether to use quotation marks around the value.

  ```
  $(_.service.name=='Procure Server')
  ```

  This condition means that when the name of the service is Procure Server, the users you specify are assigned as actors, typically approvers, or fulfillers.
  For example: $(_.request.estimatedCost >==1000)
  This condition assigns the pending action to the specified approvers or fulfillers when the estimated cost of the total request is greater than or equal to $1,000.

Step 7 - Specify Assignees for a Policy

Administrators specify assignees for a policy to configure the Catalog system to assign automatically the request pending action that triggered the policy. If the condition of the policy is met, the Catalog system automatically assigns the request to the specified assignees. The assignees typically process the request by approving, rejecting, or fulfilling it.

To specify assignees for a policy, follow this process:

1. Review Information about Assignees for Policies (see page 2132)
2. Decide how to Specify Assignees (see page 2133)

The Catalog system searches for and assigns approvers and fulfillers in the following order:

1. A relevant policy
2. The management hierarchy of the requestor
3. The Service Provider administrator (spadmin)

Review Information about Assignees for Policies

Assignees are typically request managers or other administrators who act on the requests pending action. The Catalog system assigns these requests, either to the assignees personally or to an administrative group to which they belong.

For example, suppose that the condition specifies that the pending action is triggered when both of the following conditions are true:

- The name of the requested service is Procure Laptop.
- The status is Submitted (by default, 200).

In this example, the assignee can be any of the following conditions, depending on the size and scope of the organization:

- The person or group that approves hardware requests.
- The manager of the requestor or another manager.
- The IT Finance Group.
- The Purchasing department.

You can assign only one approver or several approvers. Thus, you can assign either of the following levels:

- Only one *level* of approval, such as the manager only.
- Several levels of approval, such as the manager first, followed in succession by an IT approver and a financial officer.

When you are creating a policy or editing one, you *decide* how many approvers and how many levels of approval to specify. Examples follow:

- For requests to purchase third-party software, the following conditions apply:
  - First, both the immediate manager and the next-level manager must approve the request, in succession.
  - Next, a member of the Software Purchasing department must approve the request.
- If the Requested For user or the Requested By user is a delegate, include the manager of that user in the list of assignees.
- If the Requested For user belongs to a specific business unit, specify the approvers or fulfillers for that business unit in the list of assignees.

Decide How to Specify Assignees

Use the following use cases as guidelines:

- One known user is the assignee. Use either the Action Builder or an API plug-in.
- Multiple known users at specific levels comprise the list of assignees. Use either the Action Builder or an API plug-in.
- You query an external system for data to specify the assignees. Use the API plug-in.

- The identities and number of assignees vary, depending on the data in the request. Use the API plug-in.

Use the Action Builder to Specify Assignees

The Action Builder lets you manually find and select one or more assignees for one or more levels of approval.

Follow these steps:

1. Click Catalog, Policies, and open the policy.
2. Add the first assignee by clicking the plus sign (+) in the Action Builder (the box under the Condition field).
3. Complete the first Requirement field (the one next to the Level 1 column), as follows:
   In the drop-down list, select ANY or ALL.
   - **ANY**
     - The first approval or fulfillment for a requested item changes the status of the item and closes any remaining pending actions for the item. (*Item* means a service or service option.)
     - If all users reject or cancel an item, then the item is rejected or canceled.
   - **ALL**
     - Every assignee must approve or fulfill the requested item.
     - If any assignees are groups, then one member of each assigned group must act on the item.
     - If any assignee cancels or rejects the item, then all pending actions for the item are rejected or canceled.
4. Complete the first Assignees field (the one next to the first Requirement field) by clicking the magnifying lens:

   Note: In the Find Approvers dialog, if you select User or Group, the name of the next field remains Name Filter. If you select Manager, the name of the next field changes to Manager Level.

   The assignees you selected are recorded. The Find Approvers dialog closes. You return to the Action Builder page.
5. Click OK under the first row of approvers, and click Save (above the Policy tree).

6. Specify one or more assignees, as follows:
   If you specify multiple assignees, specify whether the pending actions are to be sequential or parallel.
   Parallel actions occur at the same time and at the same level of approval.
   Sequential actions occur in order, one after the other, and at different levels of approval.

7. To specify a complex (OR) or compound (AND) expression for the first-level approval, click the first row.
   The Operation field and the second Requirement and Assignees fields open for input.

   a. Complete the second Assignees field and second Requirement fields.

   b. Specify AND to require that *both* the first and second assignees you specify must approve (or fulfill) the pending action. Otherwise, the pending action is rejected (or is not fulfilled). Specify OR to require that *only one* of the first and second assignees you specify must approve (or fulfill) the pending action. Otherwise, the pending action is rejected (or is not fulfilled).

   c. Click OK under the first row of approvers, and click Save (above the Policy tree).

   If you are finished specifying approval levels and approvers, navigate away from this window.

8. To specify a second level of approval, go to the next step.
   Optionally complete the steps for the previous bullet (if applicable) before going to the next step.

9. If you are finished specifying approval levels and approvers, navigate away from this window.

10. (Optional) Click the plus sign (+) in the Action Builder to add a second level of approval.
    A second approval row appears, with the fields open for input.

    a. Complete the first Assignees and Requirement fields in this row.

    b. If applicable, specify a complex (either-or) or compound (both-and) expression for this row.

11. (Optional) Specify a third or more level of approval, until you are finished specifying approvers for this policy.

You have specified the assignees for this policy.

Use an API Plug-in to Specify Assignees

An API plug-in is most useful when you query an external system for data to specify the assignees. An API plug-in is also useful when the identities and number of assignees vary, depending on the data that is supplied in the request. Based on this data, the plug-in dynamically creates the assignee list and specifies the assignee levels.

Follow these steps:

1. Click Catalog, Policies, and open the policy.

2. Select Use Plug-in for Assignees. This check box appears under the Condition field.

3. Complete the fields:

   - **Plug-in Id**
     Specifies the ID of your custom plug-in for dynamically populating the list of assignees. You or another administrator must have previously written, tested, and loaded this plug-in. To view the list of plug-ins, select Administration, Tools, Plug-ins.

   - **(Optional) Variables**
     Specify the list of variables for the plug-in, if necessary.
     If applicable, open the plug-in that you selected to display its details, including variables. On the details page, the Inputs section lists the ID values and descriptions of the input variables for the plug-in. Copy the ID values of the variables that you want from that page and paste them into the value of the Variables attribute. Enter the variables as a JSON expression.

You have specified assignees for this policy.

Example: Use of Variables

$({'form_field_value':_.sog['sog1'].serviceoption[2].form['form1'].txt1, 'est_service_cost':_.service.estimatedCost, 'est_sog_cost':_.sog['sog1'].estimatedCost, 'req_status':_.request.status})

These variables return data to the plug-in, as follows:

- form_field_value hold the value of the field named txt1. This field is in the form whose ID is form1. This form is in the service option in row 2 of the service option group whose ID is sog1.
- If necessary, use the product UI to find the row number of a service option. (The linked topic references policy *conditions* but the row number has the same value in this context. The row number is an object property that remains constant, whether you reference it in a policy condition, a JSON expression, or another type of code.)
- est_service_cost holds the estimatedCost property for the service.
- est_sog_cost holds the estimatedCost property for the service option group.
- req_status holds the request status.

The data from the variables populates the list of assignees and the levels of approval, according to the code specified in the plug-in. For example, you can write a plug-in to specify that if the following *conditions* are true, then trigger the following *action*:

Conditions:

- If The txt field in form_field_value equals Deluxe.
- If est_service_cost is greater than 5,000.
- If est_sog_cost is greater than 500.
- If req_status equals 200 (Submitted).

Action: Create the following assignment table:

- Level 1 Assignee is the manager of the IT department.
- Level 2 Assignee is the manager of the Purchasing department.
- Level 3 Assignee is the Vice President of the business unit of the requested-for user.

Types of Conditions

When a condition you specify is met, CA Service Catalog assigns the related pending actions. The pending action is typically to approve, reject, or fulfill a requested item.

Specify one of the following types of conditions:

- Conditions based on the attributes of requests (see page 2137)
- Conditions based on the attributes of users (see page 2139)
- Conditions based on the attributes of the business unit (see page 2145)
- Conditions based on the attributes of services (see page 2148)
- Conditions based on the attributes of service option groups (see page 2150)
- Conditions based on the attributes of service options (see page 2151)
- Conditions based on the attributes of service option elements (see page 2156)
- Match functions for service options and service option elements (see page 2162)
- Conditions based on the fields of Form Designer forms (see page 2163)
- Conditions based on the attributes of the location (see page 2165)

Conditions Based on the Attributes of Requests

You can specify conditions that are based on the following attributes of the request that the policy affects:

- **completionDate**
- **dateCreated**
- **dateRequired**
- **description**
- **estimatedCost**
  Specifies the total estimated cost of all services (including all service options) in the request. The Catalog system calculates this cost when the request is submitted.

> **Note:** To find the cost of the request, click Home, Requests. If applicable, use the My Requests drop-down list to display requests. Find the request and view the details.

- **id**
- **lastModified**
- **name**
- **priority**
  Specifies the priority of the request as a number, using one of the following values:
  1 = high
  2 = medium_high
  3 = medium
  4 = medium_low
  5 = low
- **requestedBy**
- **requestedByAccountId**
- **requestedFor**
- **requestedForAccountId**
- **status**
  Specifies the numeric value of the status of the request.
  To use request status as a condition for *approval*, specify this attribute in your condition, using the *approval range*, by default, less than 800. For example, the following condition is met when the service is named "Procure Laptop" and the request status is approved:

  ```
  $(_.service.name=='Procure Laptop' && _.request.status < 800)
  ```

  To use request status as a condition for *fulfillment*, specify this attribute in your condition, using the *fulfillment range*, by default, greater than or equal to 999. For example, the following condition is met when the service is named "Procure Laptop" and the request status is fulfilled:

  ```
  $(_.service.name=='Procure Laptop' && _.request.status >= 999)
  ```

  If your organization is *not* using custom statuses, you can specify the default status values (see page 2108).
  If your organization *is* using custom statuses, find all *actual* status values (both default and custom). Open the requestshared.xml file. Record the values that you want to use in your conditions.
- **other attributes**
  You can view most of the other attributes when you view the request list pages. Otherwise, open a request to view its additional details.

Examples

- To assign a pending action when the estimatedCost of the request equals 100 monetary units (by default, dollars):

```
$(_.request.estimatedCost == 100)
```

- To assign a pending action when the priority of the request equals 1, meaning high priority, use this condition:

  ```
  $(_.request.priority==1)
  ```

- To assign a pending action when a request item has not been approved (status 800) and the Requested For user has a manager:

  ```
  $(anySoWith('status', lt, 800) &&_.request.requestedForUser.manager != '')
  ```

- To assign a pending action when a request item has been approved or when the Requested For user does not have a manager:

  ```
  $(anySoWith('status', gteq, 800) || _.request.requestedForUser.manager == '')
  ```

  The assignee list for this example can specify the default user (spadmin) or another suitable user.

- To assign a pending action when the request status is greater than 200 (submitted) and the business unit of the assignee is ca.com:

  ```
  $(_.request.status>200 && _.request.bu.id=='ca.com')
  ```

Conditions Based on the Attributes of Users

You can specify conditions that are based on the attributes of users, as follows:

- Conditions that are based on the attributes of the Requested For user (see page 2143)
  The Requested For user is the user who receives the requested services.

- Conditions that are based on the attributes of the Requested By user (see page 2144)
  The Requested By user is the user who created and submitted the request.
  The Requested For user and Requested By user can be the same user or different users. If you submit a request for yourself, you are both the Requested For user and the Requested By user. If you submit a request for another user, you are the Requested By user, and the other user is the Requested For user.

- Conditions that are based on the attributes of the assigner (see page 2144)
  Typically, the assigner is a workflow process utilizing an automated user like CERT-Service Delivery. Relatively few conditions are likely to use these attributes.

You can use the following attributes in conditions based on the attributes of users:

- **alias**

- **commonName**

- **defaultDomain**
  Each user has a default domain (business unit) in the user profile. Administrators set this default business unit when they add or edit the user.
  Specifies different values for different parameters, as follows:

  - For the Requested For user parameter, specifies the default business unit of the Requested For user.

- For the Requested By user parameter, specifies the business unit of the request.

Enter the ID of the business unit you want from the usm_tenant_ext table.
For example, to list the values of all business unit IDs in that table, run the following query on the MDB from your database client:

```
select tenant_id from usm_tenant_ext
```

To list the default business unit of a user, run the following query on the MDB from your database client:

```
select domain from usm_contact_domain_role where user_id=userid and default_domain=1
```

- ***userid***
  Specifies the user ID whose default business unit you want to find.

- **default_domain=1**
  Specifies the default business unit of the user.

- **defaultRole**
  Specifies the default role of a user in a domain.
  Enter the ID of the role ID you want from the usm_role table.
  For example, to list the IDs of all roles in that table, run the following query on the MDB from your database client:

```
select role_id from usm_role
```

To list the default role of a user in a domain, run the following query on the MDB from your database client:

```
select role_id from usm_contact_domain_role where user_id=userid and default_domain=1
```

- ***userid***
  Specifies the user ID whose default domain you want to find. For example:

```
select role...where user_id='john smith'...
```

  If the user ID includes one or more spaces, enclose it with single quotation marks, as shown in the example on the previous line.

- **default_domain=1**
  Specifies that the role is for the default domain of the user.

- **delegate**
  Specifies the user ID of a delegate for auto-delegation of the requests pending action of the user. Such delegates appear in the user profile in the Request Auto Delegation section. Users and their administrators can specify such delegates in the profile.
  If any delegate specified in the condition matches any delegate of the Requested For user, the

Catalog system assigns the pending action.
Enter the user ID of the delegate you want from the MDB.
For example, to list the delegates for a user ID, run the following query on the MDB from your database client:

```
select delegate_id from usm_request_Auto_delegation where delegator_id=userid and
delegation_type=0
```

- ***userid***
  Specifies the user ID of the delegator.

- **delegation_type=0**
  Specifies that the type of delegation is auto-delegation.

Contains all the CA EEM groups to which the user belongs. You can, for example, create a policy condition to assign a request pending action that is based on whether a user belongs to a specific CA EEM user group.
To find the names of CA EEM user groups, query CA EEM. Log in to CA EEM and review the group names.
Use the groups property to check if the requested by user is a member of a CA EEM group. For example, you can create a policy that requires all requests that are created by developers to be assigned to architects. To do so, use the following permission to check the requested by user group membership in the developers group:

```
_.request.requestedByUser.groups.indexOf('developers') >= 0
```

In contrast, you can also create a policy for users who are not members of a CA EEM group. To do so, specify the following expression:

```
_.request.requestedForUser.groups.indexOf('developers') < 0
```

- **description**
- **email**
- **fax**
- **firstName**
- **groups (user groups)**
- **id**
- **lastName**
- **localeCountry**

Specifies the ISO 3166 two-letter country code of the logged in user.
Commonly used ISO 3166 two-letter country codes include the following country codes:

- - Brazil - BR
  - China - CN

- France - FR
- Germany - DE
- Italy - IT
- Japan - JP
- Spain - ES
- United Kingdom - GB
- United States - US

Note: The *localeCountry* attribute uses different values than the *country* attribute (from the ca_country table) used in several other conditions.

- **localeLanguage**
- **manager**

Enter the value of the manager user ID you want from the ca_contact table.
For example, to list the values of all manager user IDs in that table, run the following query on the MDB from your database client:

```
select supervisor_contact_uuid from ca_contact
```

- **middleName**
- **mobile**
- **pager**
- **phone**
- **roles**
- **status**

Specifies the status of the Requested For user.
Values:

- 0 - Active
- 1 - inactive (deleted)

- **timezone**

Specifies the code for the time zone for the business unit.

Examples:

- Eastern USA
- Greenwich Mean Time
- Amazon Time

Enter the time_zone_code from the ca_time_zone table.
For example, run the following query on the MDB from your database client:

```
select contact_uuid from ca_contact
```

- **title**
- **uuid**
  Enter the value of the contact_uuid you want from the ca_contact table.For example, run the following query on the MDB from your database client:

  ```
  select contact_uuid from ca_contact
  ```

- **Title**
  Enter the value of the job title for the user. The ca_contact table stores the job title of each user. For example, list the job title of a specific user (here, Omar PE Patel) in that table. To do so, run the following query on the MDB from your database client:

  ```
  Select job_title from ca_contact where userid='Omar PE Patel'
  ```

  To list the values of all job titles available in CA Service Catalog, run the following query:

  ```
  select id from ca_job_title
  ```

Conditions Based on the Attributes of the Requested For User

To specify conditions that are based on the attributes of the Requested For user that is affected by the policy, use the following format:

`$(_.request.requestedForUser.`*`attribute operator 'value'`*`'')`

Enclose string values in single quotation marks. Enter numeric values without quotation marks. Do not enter spaces.

Examples

Sample conditions follow:

- To assign a pending action when the country of the business unit of the Requested For User is Brazil, use this condition:

  ```
  $(_.request.requestedForUser.localeCountry==BR)
  ```

  Note: BR is the ISO 3166 two-letter country code (see page 2139) for Brazil.

- To assign a pending action when the role of the Requested For user is request manager, use this condition:

  ```
  $(_.request.requestedForUser.role=='request manager')
  ```

- To assign a pending action when the title of the Requested For user is Procurement Officer, use this condition:

  ```
  $(_.request.requestedForUser.title=='Procurement Officer')
  ```

Conditions Based on the Attributes of the Requested By User

To specify conditions that are based on the attributes of the requested by user the policy affects, use the following format:

```
$(_.request.requestedByUser.attribute operator 'value'')
```

Enclose string values in single quotation marks. Enter numeric values without quotation marks. Do not enter spaces.

Examples

Sample conditions follow:

- To assign a pending action when the local language of the requested by user is Arabic, use this condition:

  ```
  $(_.request.requestedByUser.localeLanguage='Arabic')
  ```

- To assign a pending action when the time zone of the requested by user is GMT-11:00 MIT, use this condition:

  ```
  $(_.request.requestedByUser.timezone=='GMT-11:00 MIT')
  ```

  The time zone code for each user is specified in the user profile. To retrieve the time zone code that is associated with a specific user (Isabella Lauderos), run the following query:

  ```
  select time_zone_code from usm_contact_extension where user_id='Isabella Lauderos'
  ```

Conditions Based on the Attributes of the Assigner

To specify conditions that are based on the attributes of the assigner, using the following format:

```
$(_.user.attribute operator 'value')
```

Enclose string values in single quotation marks. Enter numeric values without quotation marks. Do not enter spaces.

Examples

Sample conditions follow:

- To assign the pending action when the title of the assignee is Purchasing Officer, use this condition:

  ```
  $(_.user.title=='Purchasing Officer')
  ```

- To assign the pending action when the default role of the user in the business unit is either Service Delivery Administrator (spadmin) or the Super Business Unit Administrator (stadmin), use this condition:

  ```
  $(_.user.defaultRole=='spadmin' || _.user.defaultRole=='stadmin')
  ```

Conditions Based on the Attributes of the Business Unit

You can specify conditions that are based on the attributes of the business unit, as follows:

- Conditions that are based on the attributes of the business unit of the request (see page 2147); that is, on the business unit of the Requested For user
- Conditions that are based on the attributes of the business unit of the assignee (see page 2148) The assignee is the logged in user attempting to complete the pending action triggered by the policy condition being met. Typically, the assignee performs an approval or fulfillment task.

In both of these types of conditions, you can use the following attributes:

- **Business unit type**
  Specifies the code for the type of the business unit.
  V**alues:**
  - TE - Tenant
  - ST - Super Tenant
  - SP -Service Provider
- **country**
  Specifies the country code for the business unit.
  Enter the code for the country you want from the ca_country table.
  An example follows: To list the code of a specific country (here, India) in that table, run the following query on the MDB from your database client:

  ```
  Select id from ca_country where country='India'
  ```

  The results show that the country code for India is 114.
  To list all country codes for CA Service Catalog, run the following query on the MDB from your database client:

  ```
  select id from ca_country
  ```

- **currency**
  Specifies the code for the currency unit for the business unit.

  Enter the value of the currency_type_code you want from the ca_currency_type table.
  For example, run the following query on the MDB from your database client:

  ```
  select currency_type_code from ca_currency_type
  ```

- **dateFormat**
  Specifies the date format for the business unit.
  Values:
  - M/d/yyyy
  - M-d-yyyy
  - d/M/yyyy
  - d-M-yyyy
  - yyyy/M/d
  - yyyy-M-d
  - dd.MM.yyyy
- **decimalFormat**

Specifies the decimal symbol for the business unit.

Values:

- 1 implies that the decimal symbol is a comma (,)
- 0 implies that the decimal symbol is a dot (.)

- **description**
- **email**
- **federalTaxId**
- **id**
- **name**
- **loginId**
- **openedDate**
- **parent**

Specifies the tenant_id of the parent business unit.
Enter the parent_tenant_id of the usm_tenant_ext table.
For example, run the following query on the MDB from your database client:

```
select parent_tenant_id from usm_tenant_ext
```

- **primaryContact**

- **Single account mode**
  Specifies whether the business unit contains a single account only.
  Values:
  - 0 - The business unit users can have multiple accounts.
  - 1- The business unit can have only a single account.
- stateTaxId
- **status**
  Specifies the status of the business unit (not the request).
  Values:
  - 0 = Inactive (Deleted)
  - 1= Active (Open)
- taxRegion
- **timeformat**
  Specifies the time format for the business unit.
  Values:
  - HH:mm:ss
  - HH.mm.ss
- **Timezone**
  Specifies the code for the time zone for the business unit.
  Enter the time_zone_code from the ca_time_zone table.

For example, run the following query on the MDB from your database client:

```
select time_zone_code from ca_time_zone
```

- **type**
- **website**
- **data1, data2, data3...**
  Specify custom data fields, if applicable, that you have created and use.

Conditions Based on the Attributes of the Business Unit of the Request

To specify conditions that are based on the attributes of the business unit of the request, using the following format:

```
$(_.request.bu.attribute operator 'value')
```

Enclose string values in single quotation marks. Enter numeric values without quotation marks. Do not enter spaces.

Examples

Sample conditions follow:

- To assign the pending action that is based on the status of the business unit, use this condition:

  ```
  $(_.request.bu.status==0)
  ```

  Note: The value of 0 specifies that the business unit is inactive. You can, for example, use a policy to assign all requests from an inactive business unit to a specific user.

- To assign the pending action when the tax region of the business unit of the request is named South, use this condition:

  ```
  $(_.request.bu.taxRegion =='South')
  ```

- To assign the pending action when the currency of the business unit of the request is named Euro, use this condition:

  ```
  $(_.request.bu.currency =='Euro')
  ```

Conditions Based on the Attributes of the Business Unit of the Assignee

To specify conditions that are based on the attributes of the business unit of the assignee, use the following format:

```
$(_.user.bu.attribute operator 'value')
```

Enclose string values in single quotation marks. Enter numeric values without quotation marks. Do not enter spaces.

Examples

Sample conditions follow:

- To assign the request pending action when the name of the business unit of the assignee is Western Regional Sales, use this condition:

  ```
  $(_.user.bu.name==‘Western Regional Sales’)
  ```

- You can assign the request pending action when the value of the singleAccountMode attribute of the assignee's business unit is 1 (meaning Yes). To do so, use this condition:

  ```
  $(_.user.bu.singleAccountMode==1)
  ```

- To assign the pending action when the business unit of the assignee is located in India, use this condition:

  ```
  $(_.user.bu.location.country==114)
  ```

  This condition uses 114, because 114 is the ID number for India in the ca_country table.

Conditions Based on the Attributes of Services

You can specify conditions that are based on the following attributes of the service that the policy affects:

- **bu**

- **code**
- **dateAvailable**
- **dateUnavailable**
- **dateCreated**
- **dateCancelled**
- **description**
- **estimatedCost**

Specifies the total estimated cost of a service in a request. The Catalog system calculates this cost when the request is submitted.

Note: To find the cost of the service, click Home, Requests. If applicable, use the My Requests drop-down list to display requests. Find the request that contains the service and view the details.

- **id**
- **name**
- **status**

Specifies the numeric value of the status of the service (*not* the request), as follows:

- 0 - Deleted
- 1 - Available
- 2 - Unavailable
- 3 - Created
- 4 - Canceled

- **website**
- **version**

You can view most of the attributes when you add or edit a service (see page 2996).

Use the following format:

```
$(_.service.attrbute operator 'value')
```

Enclose string values in single quotation marks. Enter numeric values without quotation marks. Do not enter spaces.

Examples

Sample conditions follow:

- You can assign a pending action that is based on the service name. For example, if the service name is Knowledge Management Tools, use this condition:

  ```
  $(_.service.name=='Knowledge Management Tools')
  ```

- You can assign a pending action that is based on the estimated cost of the service being greater than or equal to 100 monetary units. (The default unit is dollars). To do so, use this condition:

  ```
  $(_.service.estimatedCost<=100.0)
  ```

- You can assign a pending action for any service option (requested item) whose status is greater than 1000 when the service ID is 9999. To do so, use this condition:

  ```
  anySoWith('status', gt, 1000) || _.service.id==9999
  ```

  By default, 1000 is the value for a status of Pending Fulfillment.

Conditions Based on the Attributes of Service Option Groups

You can specify conditions that are based on the following attributes of the service option group that is affected by the policy. Use the following format:

```
$(_.sog['sogname'].serviceoption[rownumber].attribute operator 'value')
```

Enclose string values in single quotation marks. Enter numeric values without quotation marks. Do not use spaces.

The service option group has the following attributes:

- **bu**
- **code**
- **dateAvailable**
- **dateUnavailable**
- **dateCreated**
- **dateCancelled**
- **description**
- **estimatedCost**
  Specifies the total estimated cost of a service option group in a service in a request. The Catalog system calculates this cost when the request is submitted.

> **Note:** To find the cost of the service option group, click Home, Requests. If applicable, use the My Requests drop-down list to display requests. Find the request that contains the service option group and view the details. Add the costs of all service options that belong to the service option group.

You can verify the service options that belong to a specific service option group by clicking Catalog, Service Offerings, Option Groups. Review the details for the service option group.

- **id**
- **name**
- **status**

Specifies the numeric value of the status of the service option group. The status of the service option group is the same as the status of the service (*not* the request).

Values:

- 0 - Deleted
- 1 - Available
- 2 - Unavailable
- 3 - Created
- 4 - Canceled

Examples

Sample conditions follow:

- You can assign a pending action that is based on a service option group being named Procure Server and having an estimated cost greater than 1,000 monetary units. (The default unit is dollars). To do so, use this condition:

  ```
  sog['Procure Server'].estimatedCost>1000
  ```

- You can assign a pending action that is based on a service option group being named Create email Account and having an estimated cost greater than or equal to 200 monetary units. To do so, use this condition:

  ```
  $(_.sog['Create email Account'].estimatedCost >=200)
  ```

- You can assign a pending action that is based on a service option group being named New Hire Onboarding and being contained in a business unit named Eastern District. To do so, use this condition:

  ```
  sog['New Hire Onboarding'].bu=='Eastern District'
  ```

Conditions Based on the Attributes of Service Options

Conditions that are based on service options can apply to either global or attached policies (see page 3018).

Formats

Use the following format for conditions *with* a match function (see page 2162):

```
$(anySoWith('attribute',operator,'value'))
```

Use the following format (without spaces) for conditions *without* a match function:

- For global policies, you specify conditions that begin with the service option group to which the service option belongs. Use the following format:

  ```
  $(_.sog['sogname'].serviceoption[rownumber] operator 'value' )
  ```

  To find the row number of a service option (see page 2155), use the product UI. Row numbers apply to global policies *only*.

- For attached policies, you specify conditions *without* the service option group name and row number. Use the following format:

  ```
  $(_.serviceoption operator 'value' )
  ```

  Note: Attached policies let you specify a policy that you can share among multiple service options efficiently, using a simple condition. When you specify a global policy for a service option, you must find its row number and must use that number in the condition.

For all formats, enclose string values in single quotation marks, and enter numeric values without quotation marks.

To specify conditions that are based on service options, use the following attributes:

category	external_id
category_class	keywords
category_subclass	status
estimatedCost	track_as_asset

1. For service options and service option elements, you can specify conditions that use match functions (see page 2162).

- **category, category class, and category subclass**
  Specifies the values for category, category class, and category subclass from the category.xml file. View this file and record the values that you want to use in your conditions. This file is located in a different folder for each localized version of CA Service Catalog. For example, for English (icusen), the category.xml file is located in the USM_HOME\view\webapps\usm\locale\icusen\billing folder.

- **estimatedCost**
  Specifies the estimated cost of a service option in a service in a request. The Catalog system calculates this cost when the request is submitted.

Note: To find the cost of the service option, click Home, Requests. If applicable, use the My Requests drop-down list to display requests. Find the request that contains the service option and view the details.

- **external_id and keywords**
  Specifies the values for the attributes that are named external_id and keywords.
  Service builders specify these values when defining the service options of a service option group.
  Service builders typically use these attributes to add meta information about services, especially for categorizing services.
  You can find the values of these attributes and can record them for use in this condition.

- **status**
  Specifies the request status of the service option.

- **track_as_asset**
  Specifies a numeric value indicating whether to track this service option as an asset in CA APM, as follows:
  0 - No
  1 - Yes

  Note: This attribute is relevant *only* when CA Service Catalog is integrated with CA APM.

  You can verify whether a service option uses this attribute (see page 2156), as follows: View the value of the Track as an Asset field on the Service Option Element Options window--Options tab (see page 3019).
  You identify service options in conditions by their row number in the service option group. On the CA Service Catalog GUI, you can find this row number by selecting Catalog, Service Offerings, Option Groups. Click the service option group on left pane, and click the Definition tab on right pane.
  When you do so, each service option in the group appears in a table; each row contains one service option. In the condition, specify the row number of the service option of interest. For example, suppose row 2 contains a service option named Windows server. In that case, specify the following conditions to include this service option.
  For a global policy:

  ```
  $(_.sog['sogname'].serviceoption[2]
  ```

  For an attached policy:

  ```
  $(_.serviceoption
  ```

Examples

Consider the following examples.

- You can specify the assignee when the name of the service option group is Procure Laptop and the category of the first service option is 1. To do so, use this condition:
  For a global policy:

  ```
  $(_.sog[‘Procure Laptop’].serviceoption[1].category==1)
  ```

This policy applies to the service option in row 1 of the service option group.
For an attached policy:

```
$(_.serviceoption.category==1)
```

This condition specifies that the pending action is assigned to the approver or fulfiller when the service option group is named Procure Laptop and the first service option in it belongs to Category 1. By default, Category 1 signifies hardware.

- You can specify the assignee when both of the following conditions are true:
  - The name of the service option group is New Hire Onboarding.
  - The estimated cost of the third service option is 30 monetary units. A sample unit is Euros.

  To do so, use this condition:
  For a global policy:

  ```
  $(_.sog['New Hire Onboarding'].serviceoption[3].estimatedCost==30.0)
  ```

  This policy applies to the service option in row 3 of the service option group.
  For an attached policy:

  ```
  $(_.serviceoption.estimatedCost==30.0)
  ```

- You can specify the assignee when both of the following conditions are true:
  - The name of the service option group is Handheld Devices.
  - The estimated cost of the service option in the third row of the group is 300 monetary units.

  To do so, use this condition:
  For a global policy:

  ```
  $(_.sog[‘Handheld Devices’].serviceoption[3].estimatedCost==300)
  ```

  This policy applies to the service option in row 3 of the service option group.
  For an attached policy:

  ```
  $(_.serviceoption.estimatedCost==300)
  ```

Examples with the Match Function

Consider the following examples:

- You can specify the assignee when the service option group includes a service option (in any row) with a category class greater than 10. To do so, use this condition:

  ```
  $(anySoWith('category_subclass',gt,10))
  ```

  This condition specifies that the pending action is assigned to the approver or fulfiller when any service option belongs to a category class greater than 10. By default, a category class greater than 10 signifies that the request is not related to any IT category, such as hardware or software.

- To specify the assignee when any service option in the request includes a category subclass greater than 10, use this condition:

  ```
  anySoWith('category_subclass',gt,10)
  ```

- To specify the assignee when the external_id (a string) of any service option ends with the string "MB," use this condition:

  ```
  $(anySoWith('external_id',endsWith,'MB'))
  ```

- You can specify the assignee when the category of any service option in the request is greater than 10 but less than 30. To do so, use this condition:

  ```
  $(anySoWith('category',gt,10) && anySoWith('category',lt,30))
  ```

- You can specify the assignee when *both* of the following are true:

  - The value of the external_id attribute of any service option in the request begins with the case-sensitive word "Memory"
  - The request contains a service option group that is named Procure Server. The category attribute of its first service option (row 1) has a value of 1, signifying hardware

  To do so, use this condition:

  ```
  $(anySoWith('external_id',startsWith,'Memory') && _.sog['Procure Server'].
  serviceoption[1].category==1)
  ```

- To specify the assignee when any service option in the request is tracked as an asset in CA APM, use this condition:

  ```
  $(anySoWith('track_as_asset',eq,1))
  ```

  Note: This attribute is relevant only when CA Service Catalog is integrated with CA APM.

Find the Row Number of a Service Option

When you specify a condition that is based on the attributes of a service option (see page 2151), specify the row number of the service option. This row number is the position of the service option in its service option group. Row numbers apply to global policies (see page 3018) *only*.

Follow these steps:

1. Click Catalog, Service Offerings.
2. Click the Option Groups tab.
3. Click the service option group of interest.
4. Click the Definition tab.
5. Find the service option of interest and click its Edit icon.
   The Service Option Details page opens. The row number appears under the image, near the Description field.
6. Record the row number.

> **Note:** Row numbers start at 1 and increase sequentially by 1 as you add service options to a service option group.

You have found and recorded the row number of the service option. You can now use the row number in a condition that is based on the attributes of this service option.

Examples

For example, a service option group contains these service options: Small, Medium, and Large. The Small service option is in row 1. The Medium service option is in row 2, and the Large service option is in row 3.

To specify a condition for the Small service option in a global policy, use the following format:

```
$(_.sog['sogname'].serviceoption[1] operator 'value' )
```

Similarly, to specify a condition for the Medium service option in a global policy, use the following format:

```
$(_.sog['sogname'].serviceoption[2] operator 'value' )
```

Find the Values of the Attributes of a Service Option

You can find the values of the attributes of a service option when required. For example, you can create conditions that are based on the attributes of service options (see page 2151). In that case, you can specify the values of the external_id, code, and keyword attributes as part of the condition.

Follow these steps:

1. Click Catalog, Service Offerings, Option Groups.
2. Click the service option group that you want to open.
3. To display the service options, click the Definition tab.
4. Open the service option of interest and view its details, including its service option elements.
5. Find and optionally record the values of the attributes you want, for example, the external_id, code, and keywords.

You have found and optionally recorded the values of the attributes of a service option.

Conditions Based on the Attributes of Service Option Elements

Conditions that are based on service option elements can apply to either global or attached policies (see page 3018).

For service options and service option elements, you can specify conditions that use match functions (see page 2162).

You can specify conditions that are based on the following attributes of service option elements:

- code item_type
- estimatedCost status
- item_text

The following attributes require explanation:

- **Code**
  Is a user-specified text value to represent the product code, subscription code, SKU # or any other applicable code.
  To find the value of this attribute for a service option element, click Catalog, Services Offerings, Option Groups. View the service option and service option element of interest. On the Service Option Element Definition dialog, click the Options tab and find the value of the Code field.

- **estimatedCost**
  Specifies the estimated cost of a service option element in a service option in a service in a request. The Catalog system includes the cost of all service option elements in the cost of the service option to which they belong. The Catalog system calculates this cost when the request is submitted.

  Note: To find the cost of the service option, click Home, Requests. If applicable, use the My Requests drop-down list to display requests. Find the request that contains the service option and view the details.

- **item_type**
  Specifies a valid value (see page 2161) for the item type, as specified in the Type label of the service option element. For example, if the type of the service option element is CA BSI contract (for CA Business Service Insight contract), the value of item_type is 5. Similarly, if the type is Form, the value of item_type is 14.

- **item_text**
  Specifies the value of the Display Text field on the service option element definition page. You can specify the condition to require either an exact match or an approximate match, as follows:

  - To require an exact match, specify the condition as follows:
    For global policies:

    ```
    $(_.sog['ab'].serviceoption[1].soe[2].item_text=='abc')
    ```

    For attached policies:

    ```
    $(_.serviceoption.soe[2].item_text=='abc')
    ```

    In this format, the text must match exactly, including case and spaces. For example, suppose "Premium Laptop" is the value of the Display Text field. In that case, the value of item_text must also be 'Premium Laptop': The value *cannot* be 'premium laptop' or 'Premium laptop'; the value *cannot* be any value except an exact match.

  - To require an approximate match, specify the condition as follows:

    ```
    $(anySoeWith('item_text',contains,'abc'))
    ```

In this format, the string that is specified must be either the same as the Display Text or a substring of Display Text. The string is not required to match exactly and is case-sensitive. For example, if "Premium Laptop" is the value of the Display Text field, then the string that is specified can be any of the following options:

- 'Premium Laptop'
- 'Laptop'
- 'Premium'

- **status**
  Specifies the request status of the service option that contains this service option element.

Formats

For all formats, enclose string values in single quotation marks, and enter numeric values without quotation marks.

Use the following format for conditions *with* a match function (see page 2162):

```
$(anySoeWith('attribute',operator,'value'))
```

Use the following formats (without spaces) for conditions *without* a match function.

- For global policies, conditions for service option elements use this format:

  ```
  $(_.sog[sogname].serviceoption[rownum].soe[colnum].attribute operator 'value')
  ```

  - ***sogname***
    Specifies the name of the service option group.
  - ***rownum***
    Specifies the row number of the service option.
    To find the row number of the service option (see page 2155) in the service option group, use the product UI.
    Row numbers apply to global policies *only*.
  - ***colnum***

  Specifies the column number of the service option element in its service option.
  To find the column number of the service option element (see page 2160) in the service option, use the product UI.

- For attached policies, conditions for service option elements use this format:

  ```
  $(_.serviceoption.soe[colnum].attribute operator 'value')
  ```

  The same *colnum* attribute as for global policies also applies to attached policies.

Examples

Consider the following examples:

- You can specify the assignee for the request pending action when all of the following conditions are true:
  - The service option group is named Reserve Virtual Machine. This condition applies to global policies only.
  - The service option is in row 2. This condition applies to global policies only.
  - The service option element is in column 3. This condition applies to both global and attached policies.
  - The item type of the service option element is 15 (for reservation). This condition applies to both global and attached policies.

  To do so, use this condition:
  For global policies:

  ```
  $(_.sog['Reserve Virtual Machine'].serviceoption[2].soe[3].item_type==15)
  ```

  For attached policies:

  ```
  $(_.serviceoption.soe[3].item_type==15)
  ```

  Thus, this condition is met when a service option for creating or extending a reservation meets the specified criteria.

- You can specify the assignee for the request pending action when all of the following conditions are true:
  - The service option group is named Increase Mailbox Size. This condition applies to global policies only.
  - The service option is in row 3 of the service option group. This condition applies to global policies only.
  - The estimated cost for the service option element is greater than 200 monetary units. The default unit is dollars. This condition applies to both global and attached policies.
  - The service option element is in column 2 of the service option. This condition applies to both global and attached policies.

  To do so, use this condition:
  For global policies:

  ```
  $(_.sog['Increase Mailbox Size'].serviceoption[3].soe[2].estimatedCost >200)
  ```

  For attached policies:

  ```
  $(_.serviceoption.soe[2].estimatedCost >200)
  ```

  Thus, this condition is especially useful to specify approvers or fulfillers for service option elements costing more than a specified amount.

- You can specify the assignee for the request pending action when all of the following conditions are true:

- The service option group is named Application Hosting.
- The estimated cost is greater than or equal to 2500 monetary units for the sixth service option element in the fifth service option.

To do so, use this condition:
For global policies:

```
$(_.sog['Application Hosting'].serviceoption[5].soe[6].estimatedCost>=2500)
```

For attached policies:

```
$(_.serviceoption.soe[6].estimatedCost>=2500)
```

Examples with the Match Function

Consider the following examples:

- You can specify the assignee for the request pending action when the following condition is true: Any service option element in the request has an estimated cost greater than 30.0 monetary units (for example, pounds). To do so, use this condition:

  ```
  $(anySoeWith('estimatedCost',gt,30.0))
  ```

- You can specify the assignee for the request pending action when the following is true: The value of the item_text attribute of any service option element in the request contains the 'share' text string. To do so, use this condition:

  ```
  $(anySoeWith('item_text',contains,'share'))
  ```

Find the Column Number of a Service Option Element

When you specify conditions that are based on the attributes of service option elements (see page 2156), you include the column number. This column number is the position of the service option element in its service option. This requirement applies to both global and attached policies (see page 3018). For global policies *only*, you also specify the row number of the service option in its service option group (see page 2155).

Follow these steps:

1. Click Catalog, Service Offerings.
2. Click the Option Groups tab.
3. Click the service option group of interest.
4. Click the Definition tab.
5. Edit the service option of interest.
6. Edit or add the service option element of interest, for example, a rate or text element.
   The Service Option Element Definition dialog appears.
7. Click the Options tab and view the Column field near the top of the dialog. Record the number for use in conditions.

Note: Column numbers start at 1 and increase sequentially by 1 as you add service option elements to a service option.

You have found the column number of the service option element. You can use the column number in a condition that is based on the attributes of a service option element.

Examples

For example, a service option group lists these service options, in sequential order: Gold, Silver, and Bronze. The Gold service option is in row 1. The Silver service option is in row 2, and the Bronze service option is in row 3. Each service option has a rate service option element in column 5.

The following examples apply to global policies *only*:

To specify a condition for the Gold service option, use the following format:

```
$(_.sog['sogname'].serviceoption[1].soe[5].attribute operator 'value')
```

Similarly, to specify a condition for the Silver service option, use the following format:

```
$(_.sog['sogname'].serviceoption[2].soe[5].attribute operator 'value')
```

The following example applies to attached policies *only*:

To specify a condition for any of the three options, use the following format:

```
$(_.serviceoption.soe[5].attribute operator 'value')
```

Valid values for item_type

The valid values for item_type and their meanings follow:

item_type	Meaning
0	Text
1	Header
2	Numeric range
3	Rate
4	Usage based price
5	CA Business Service Insight contract
6	Numeric
7	Boolean
8	Adjustment
9	Date
10	Date range
11	Day of billing

item_type	Meaning
12	Allocation
14	Form Designer form
15	Reservation

Service designers specify the item type when they complete the Service Option Element Definition window--Definition tab (see page 3021). They do so as part of the process of creating or editing a service option.

Match Functions for Service Options and Service Option Elements

Use match functions when defining conditions for service options and service option elements. To specify an attribute, value, and relationship in a condition *without* specifying any other elements that are required in other conditions, use a match function.

Elements that are required in other conditions but *not* in match functions include the following elements:

- The name of the request, service, or service option group
- The row number of a service option or service option element

Match functions thus provide flexibility by enabling you to specify the attribute condition across multiple components of a request.

To specify a match function for a service option, use the following format:

```
$(anySoWith('attribute',operator,'value'))
```

To specify a match function for a service option element, use the following format:

```
$(anySoeWith('attribute',operator,'value'))
```

For both formats, enclose string values in single quotation marks, and enter numeric values without quotation marks.

- ***attribute***
  For service options, you can use all the same attributes that are used (see page 2151) in conditions for service options without a match function.
  For service option elements, you can use all the same attributes that are used (see page 2156) in conditions for other service option elements without a match function.

- ***operator***
  For both service options and service option elements, *operator* can be any of the following values:

Operator	Meaning
eq	equal to
neq	not equal to
lt	less than

Operator	Meaning
gt	greater than
lteq	less than or equal to
gteq	greater than or equal to
startsWith	starts with
contains	contains
endsWith	ends with

- ***value***
  Specifies a string or numeric value for the attribute.
  For more information, see the examples of conditions that use the match function for service options (see page 2151) and service option elements (see page 2156).

Conditions Based on the Fields of Form Designer Forms

You can specify conditions that are based on the values of fields of Form Designer forms. Use the following format to specify such conditions:

```
$(_.sog[sogname].serviceoption[rownum].form[form-name].value of _id attribute string-operator'value of value attribute')
```

- ***rownum***
  Specifies the row number of the service option that includes the Form Designer form.

- ***form-name***
  Specifies the name of the Form Designer forms, from the Form Designer tree. Do *not* use the value of name attribute for the form.

- ***value of _id attribute string-operator 'value of value attribute'***
  Specifies the attribute operator value portion of the conditions, using the same format as other conditions (see page). For forms, the following requirements apply:

  - The *attribute* specification must be the value of the _id attribute of the field you want.

  - The *value* specification must be based on the value of the value attribute of the same field.

  Typically, the *value* specification is an option that is based on user input or user selection.

  Important! The Form Designer stores the values for all fields in string format. Even the fields that contain numeric input that users or the Catalog system specify are stored in string format. Therefore, conditions that are based on Form Designer fields can use *only* the comparison operators suitable for strings: equal (==) and not equal (!=). Moreover, always enclose these values in quotation marks, because they are always strings.

  If necessary, you can combine two or more expressions that use these comparison operators. Use operators for specifying complex or compound conditions (see page).
  See the following examples for details about specifying conditions that are based on Form Designer fields.

Examples Using a Predefined Form for Product Information

This example is based on a fictitious service option group that is named Insider Products. The service option group contains an actual predefined form named Product Info. To see this form, select Form Designer, expand the Forms tree, and select Product Info.

Users complete this form while requesting services to obtain services from Insider Products. This form includes a Discount Program Code field with an _id attribute whose value is discount_code and a value attribute whose default value is null. However, users can change this value by entering their discount code, if applicable.

You can specify the assignee for the request pending action, which is based on which of the following actions the user performs:

- User leaves the Discount Program Code field empty.
- User enters a discount code.

To meet each specification, use the following conditions, respectively:

- For an empty field:

```
$(_.sog['Insider Products'].serviceoption[1].form['Product Info'].discount_code==’
null’)
```

- For a field with user input:

```
$(_.sog['Insider Products'].serviceoption[1].form['Product Info'].discount_code!=’
null’)
```

Examples Using a Predefined Form with Radio Buttons

This example is based on a fictitious service option group that is named File Shares. The service option group contains an actual predefined form named File Share Access. To see this form, select Form Designer, expand the Forms tree, and select File Share Access. This form is useful for services that users use to request access to a network file share.

The sample conditions are based on the following options for access levels to the share and the values of their _id attributes:

- None: Permits no access.
- Read: Allows viewing of contained files and directories, loading of files, and executing software.
- Change: Provides all read permissions plus creating, deleting, and changing the directories and files.
- Full Control: Provides all change permissions, including file system changes and ownership.

For all these examples, both of the following conditions apply: The service option group is named File Shares, and the third service option includes a form that is named File Share Access.

The field is a select box that forces the user to select an option (using a radio button) on the form. Therefore, the form fieldportion of the condition uses the following format:

`id_attribute of parent field=='value attribute of child field'`

- **id_*attribute of parent field***
  Specifies the value of the id_attribute of parent field; here, the field that defines the select box. In this example, on the File Share Access form, the value is access_level. The select box appears as a radio button box on the form. Users must select one of the options by clicking its adjacent radio button.

- **'*value attribute of child field*'**
  Specifies the value of the value attribute (*not* the _id attribute) for the child attribute (the radio button option) that the user selected.
  In this example, on the File Share Access form, the valid values of these fields are none, read, change, and full. These values represent the options for each level of access to the file share.

View these form attributes on the Form Designer together with the following conditions to help gain a complete understanding of the relationship between them.

The following sample conditions are based on the radio button that the user selects on the File Share Access form:

- To specify the assignee for the pending action when the user selects No Access, use this condition:

  ```
  $(_.sog['File Shares'].serviceoption[3].form['File Share Access'].access_level
  =='none')
  ```

- To specify the assignee for the pending action when the user selects Read (for read-only access rights), use this condition:

```
$(_.sog['File Shares'].serviceoption[3].form['File Share Access'].access_level
=='read')
```

- To specify the assignee for the pending action when the user selects Change (for read and update access rights), use this condition:

```
$(_.sog['File Shares'].serviceoption[3].form['File Share Access'].access_level
=='change')
```

- To specify the assignee for the pending action when the user selects Full Control. Full Control provides access rights for read, update, create, delete, and so forth, use this condition.

  ```
  $(_.sog['File Shares'].serviceoption[3].form['File Share Access'].access_level
  =='full')
  ```

Conditions Based on the Attributes of the Location

You can specify conditions that are based on the attributes of the location, as follows:

- Conditions that are based on the attributes of the location of the assignee. (see page 2167)
  The assignee is the logged in user attempting to complete the pending action. When the policy condition is met, it triggers the pending action. Typically, the assignee performs an approval or fulfillment task.

- Conditions that are based on the attributes of the location of the business unit of the assignee. (see page 2168)

In both of these types of conditions, you can use the following attributes:

- **address**
- **city**
  Specifies the code for the city for the business unit of the assignee. Users enter their own values, rather than run a database query. This data is user-defined, and the MDB does not store this data.
- **country**
  Specifies the country code for the business unit.
  Enter the code for the country you want from the ca_country table.
  For example, to list the code of India in that table, run the following query on the MDB from your database client:

  ```
  Select id from ca_country where name="India"
  ```

  The results show that the country code for India is 114.
  To list all country codes for CA Service Catalog, run the following query on the MDB from your database client:

  ```
  select id from ca_country
  ```

- **county**
  Specifies the *user-specified* value, such as a name or code, for a county. Examples include a county in a state of the United States or in another country that has counties.
  Values for this attribute are user-specified. The CA Service Catalog and the MDB do not validate or maintain them.
- **description**
- **fax**
- **name**
- **state**
  Specifies the 50 states in the United States, and some but not all of the United States territories, such as American Samoa. Also applies to all provinces in Canada. This attribute is null for other countries and territories.
  This attribute specifies the ID for the applicable state, territory, or province for the business unit of the assigner. Examples include 7404 for California and 7434 for New York.
  Enter the ID you want from the ca_state_province table.
  To list the IDs for all states, territories, and provinces, run this query on the MDB from your database client:

  ```
  select id from ca_state_province
  ```

  Verify the two-letter symbol for the state, territory, or province from the United States Postal Service (www.usps.com (http://www.usps.com)). You can use that symbol to find the ID. For example, the symbol for the state of New York is NY. Therefore, to list the ID for New York, run the following query on the MDB from your database client:

```
select id from ca_state_province where symbol='NY'
```

This query returns a value of 7434, which you use in your condition to assign the pending action based on the user's location being the state of New York. For details, see the sample state attributes in the conditions that are based on the attributes of the location of the business unit of the assignee (see page 2168).
To list the IDs, symbols, and names for all applicable states, territories, and provinces, run the following query:

```
Select id,symbol,description from ca_state_province
```

The results appear similar to the following output:

```
7400 AK  Alaska

7401 AL  Alabama

...
```

- **phone**
- **postalCode**
- **uuid**

Conditions Based on the Attributes of the Location of the Assignee

To specify conditions that are based on the attributes of the location of the assignee, use the following format:

`$(_.user.location.`*`attribute operator 'value'`*`)`

Enclose string values in single quotation marks. Enter numeric values without quotation marks. Do not use spaces.

Examples

Sample conditions follow:

- To assign the pending action when the name of the location of the user is Home, use this condition:

  `$(_.user.location.name==‘Home’)`

- To assign the pending action when the country of the user's location is India, use this condition:

  `$(_.user.location.country==114)`

  Note: The code for India in the ca_country table is 114.

- To assign the pending action when the city of the location of the user is Hamburg, use this condition:

  `$(_.user.location.city==‘Hamburg’)`

Conditions Based on the Attributes of the Location of the Business Unit of the Assignee

To specify conditions that are based on the attributes of the location of the business unit of the assignee, use the following format:

```
$(_.bu.location.attribute operator 'value')
```

Enclose string values in single quotation marks. Enter numeric values without quotation marks. Do not use spaces.

Examples

Sample conditions follow:

- To assign the request pending action when the business unit is in the state of New York in the United States, use this condition:

  ```
  $(_. bu.location.state==7434)
  ```

  7434 is the code for New York in the ca_state_province table.

- To assign the request pending action when the business unit is in the country of Mozambique, use this condition:

  ```
  $(_. bu.location.country==169)
  ```

  169 is the code for the country of Mozambique in the ca_country table.

Manage Request SLAs

CA Service Catalog administrators can create request SLAs to monitor whether service options in a request are processed within the time period that you specify for each monitored state. Your SLAs specify time to warning and time to violation for the selected service option. A single request SLA specifies the amount of time that is permitted between specified statuses. For example, the time that is taken to move from Submitted to Approved or from Approved to Completed.

For each request SLA, you specify the starting and ending statuses to monitor. You also specify the length of time to reach warning and violation thresholds, the expected level of compliance, and related settings.

Setting SLA warning and violation thresholds helps service providers to track the progress of a request. The request SLA data is stored in the CA Service Catalog database so that it can be included in reports.

The monitoring of time for an SLA warning or violation (SLA time) is started and stopped according to the service hours that both the outage calendars and the business hours specifications that are associated to the service determine. Administrators optionally associate one outage calendar and one business hours specification to each service. Only during service hours, the SLA time is monitored.

You can optionally specify automated actions to be initiated when a request SLA reaches warning status or violation status. These actions include a predefined action for sending email alert messages. For more information, see Configure Automated Email Alerts for SLA Warnings and Violations (see page 2172) section.

Note: Request Service Level Agreements (SLAs) are a feature of CA Service Catalog. Quality of Service (QoS) SLAs are available only if CA Service Catalog is integrated with CA Business Service Insight.

Create Request SLAs

Request SLAs are processed according to both the fixed rules specified by CA Service Catalog and the Maximum Delay for Request SLA Alerts setting that you specify.

Fixed Rules

Request SLAs are processed according to the following fixed rules specified by CA Service Catalog:

- After a request containing one or more SLAs is submitted, the SLA clock for each SLA instance starts tracking time when the request reaches the starting status that is specified for the SLA. For example, if an SLA monitors the period from Pending Approval to Approved, the SLA clock for this SLA instance starts tracking time when the request status changes to Pending Approval.
- An SLA instance completes when either of the following situations occur:
  - The request reaches the ending status of the SLA before the SLA violation time expires. In this case, the SLA instance completes successfully. The SLA violation time is the maximum length of time that is permitted for the request reach the ending status of the SLA.
  - The SLA violation time expires before the request reaches the ending status of the SLA. In this case, the SLA instance completes unsuccessfully, causing an SLA violation to occur.
- The SLA clock tracks time for each active SLA instance and alerts the Catalog system if the SLA warning or violation time expires. The SLA clock is paused and resumed *only* when a CA Service Catalog user holds or resumes the request containing the SLA instance. If a user changes a request with an active SLA instance to Hold status, then the SLA clock is paused. When a user changes such a request to Resume status, the SLA clock is resumed.

  Note: If the user of another product that is integrated with CA Service Catalog puts a request on hold in that product, the CA Service Catalog request, the SLA instance remains active. To pause the SLA clock, hold the request in CA Service Catalog.

- The SLA clock is stopped immediately when a request is canceled.
- The SLA clock is never restarted (reset to zero) under any circumstances, even if the request is rejected and resubmitted.
  For example, consider an SLA named “Approved within 1 Day SLA.” This SLA monitors from “Submitted” status to “Approved” status with a one day SLA violation time. In this example, the approval process also follows this request status cycle, in the following order:
  1. Submitted
  2. Pending Approval

3. Approved
4. Approval Done or Submitted
5. Pending Approval
6. Rejected

In this example, if an end user requests a service, a day passes, and an approver rejects the request, then the SLA "Approved within 1 Day SLA" is violated. After the rejection, if the affected end user updates the request detail and submits it again, the request approval process is repeated, but the SLA instance is not monitored again because it has already been monitored once and completed with a violation.

- If an SLA instance completes, successfully or with a violation, that same instance is never monitored again under any circumstances.
- Once a monitored request SLA instance is violated, the violation is included in SLA-related BusinessObjects Enterprise reports, even if the related request is canceled or rejected after the violation occurs. To exclude such records from a report, customize the report.

Request SLA Processor

The request SLA processor is part of Catalog Component and:

- Listens for status changes for requests that have active SLA instances.
- Sends alert messages when SLA warnings or SLA violations occur.
- Tracks time for the SLA clock.

Maximum Delay for Request SLA Alerts

The request SLA processor checks for SLA instances to be processed at these times:

- When the SLA clock for an active SLA instance alerts the Catalog system that the SLA warning or violation time has expired.
- When it receives a message of a change in the status of a request with an active SLA instance.
- When the time period specified in the Maximum Delay for Request SLA Alerts setting expires. To access this setting, select Administration, Configuration, Request SLA. This setting specifies how frequently the request SLA processor checks for SLA warnings or violations. This setting applies to all SLA instances managed by a Catalog Component computer.

In a Catalog Component-clustered environment, if a clustered computer fails, then event notifications, including SLA alert messages, can be delayed until the failed computer is restored or until other computers in the cluster begin doing the work of the failed computer. So, SLA warning and violation messages may not be issued on time.

To minimize this possible delay in SLA processing time when a Catalog Component- clustered computer fails, you can configure the Maximum Delay for Request SLA Alerts to meet your needs. The smaller the value you set, the greater the frequency with which the request SLA processor checks

the SLA clock for warning and violation times. Therefore, set a less frequent time period, such as one hour, to be informed of SLA warnings and violations quickly. Otherwise, set a larger time period, such as one day, to be notified about SLA warnings and violations later, when the failed clustered computer is restored.

Setting the Maximum Delay for Request SLA Alerts helps reduce any delay of SLA processing in case the clustered computer that started the SLA clock becomes unavailable for a length of time longer than a warning or violation period. In such cases, other active clustered computers take over SLA processing from the failed computer, when one of the following events occurs:

- The Maximum Delay for Request SLA Alerts time period expires.
- An SLA warning or violation is issued.
- A status change occurs in a request with an active SLA instance.

The following criteria can help CA Service Catalog administrators determine which service options to monitor with SLAs:

- Check whether any *critical* business rules, business needs, or contractual obligations with service consumers affect any service options. Indicate that such service options require SLAs.
- Check whether it is expected that *all* service options in your implementation are monitored with SLAs.

Request SLAs monitor whether service options in a service option group are processed within the specified time period. Your SLAs specify time to warning and time to violation for the selected service option.

Follow these steps:

1. Select Catalog, Service Offerings.
2. Expand the tree and select the service to which you want to add the SLA.
3. Click the Definition tab of the service.
4. Click the expand sign on the header next to the service option group name.
5. Locate the service option to which you want to add the SLA.
6. Click the SLA icon and click Add to create the SLA.
7. Specify the values for each SLA.
8. If you create multiple SLAs, select one of them as the primary SLA. To do so, click the option button in the Primary column. If a service option contains only one SLA, then that SLA is the primary SLA.
   When a service option has multiple SLAs, the status of the primary SLA determines the status of the service option as a whole, regardless of the status of the other SLAs. For example, suppose you create four SLAs for a service option. If the primary SLA has not reached a warning or violation when the request containing the service option is completed, then the SLA for that service option is satisfied, even if all of the other three SLAs *did* reach a warning

or violation.
Conversely, if three of the four SLAs have no warning or violation, but the primary SLA has a warning or violation, then the service option as a whole has a warning or violation.
Both warnings and violations are reflected in SLA Reports.

(Optional) Configure Automated Email Alerts for SLA Warnings and Violations

As an administrator, you can create automated actions to be initiated when a request SLA reaches warning status or violation status. Such actions can include using the predefined actions for sending email alerts and running your own custom actions, such as running command-line commands. Using automated actions can help you find the root cause of a problem sooner and correct it earlier. So, you can reduce the number of any additional related SLA warnings or violations.

To create automated email alerts for SLA warnings and violations, follow this process:

1. Select Home, Administration, Events-Rules-Actions.
2. Click the Event Type named Request SLA Alerts.
3. Decide whether to enable one or both of the predefined SLA-related rules: they are *When a Request SLA Instance is Warned* and *When a Request SLA Instance is Violated*.
4. Click Enable to enable one or both of these rules.
5. Click Enable to enable the matching action or actions for each rule that you enabled.
   The predefined (built-in) action for the SLA instance warning is named Email Alert for Warned Request SLA. Similarly, the predefined action for the SLA instance violation is named Email Alert for Violated Request SLA.
6. Click the Edit icon in the Edit column of the action. Specify the information.

   Note: The type is preset to Email. The Subject and Message fields are also preset.

7. Test the action. Submit a request with at least one SLA and letting the SLA reach warn status, violation status, or both.
8. Ensure that both actions (Email Alert for Warned Request SLA and Email Alert for Violated Request SLA) are configured

(Optional) Save SLA History and Reset SLAs

One likely reason to change your SLA definition is a change in service agreement or contract that arises after the monitoring of SLAs has already started. To handle such cases, CA Service Catalog enables you to save your current SLAs as history and reset SLAs. SLA history is *not* accessible using the GUI but *is* reflected in SLA reports.

For example, suppose that you created SLAs for a service on the first day of the month but later change the SLAs. At the end of the month, the SLA report for the entire month shows the different warning and violation settings that are used for the SLAs before and after the changes.

Important! When you change SLA settings for a service option, the change takes effect for *future* requests that include the service in which the service option resides. Requests that are in-progress are *not* affected.

Follow these steps:

1. Select Catalog, Service Offerings.
2. Expand the tree and select the service to which you want to add the SLA.
3. Click the Definition tab of the service.
4. Click the expand sign on the header next to the service option group name.
5. Locate the service option to which you want to add the SLA.
6. Click the SLA icon.
7. Click Save as History. This button is enabled *only* if the defined SLA exists.
8. When prompted, specify a reason for saving as history and resetting the SLAs.
9. Confirm the action.
   The existing SLAs are made inactive. Inactive SLAs are saved for use in both reports and in-progress requests, However, inactive SLAs are *not* applied to any future requests.
   Inactive SLAs are removed from the service and are no longer accessible through the CA Service Catalog GUI.
10. As needed, create request SLAs for use in future requests, to replace the inactive SLAs.

Note: Inactive SLAs are reflected in the SLA reports for related requests.

SLA Reports

In both the Report Builder and BusinessObjects Enterprise, you can create, configure, and view reports concerning SLA-related data. This data covers both current SLAs and inactive SLAs that have been saved as history (see page 2172).

Review the following information when you check SLA reports for warnings and violations:

- If a key SLA is warned or violated, then the service option that is associated with that SLA is warned or violated.
- If any service option in a service is warned or violated, then the service containing that service option is warned or violated.

- If any service in a request is warned or violated, then that request is warned or violated.
- For a violation, the Whole Violated Mark appears, at both the service and request levels.

Create Advanced Searches for Requests

Administrators can define the scope of user searches by clicking **Administration**, **Configuration**, **User Default**. They can specify the User Search Scope as either the business unit of the user or the entire Catalog system.

Follow these steps to create an advanced search query:

1. Click Home, Requests.
2. Click the advanced search icon.
3. Click the Search icon in the Advanced Search box to enter a new advanced search query. The fields next to the Search icon expand so that you can enter an advanced search condition in the format property - operator - value, as follows:
    a. In the first (property) search field (a drop-down list), select the property for you want to search for, such as Action By User ID, Business unit Name, Request Priority, or Service Option Element Name.
    b. In the second (operator) search field (a drop-down list), select the operator to use for your search, such as Equals, Not Equals, Contains, Starts With, Ends With, or In. *In* is a special operator that you can use to select or specify multiple values as search criteria.
    c. In the third (value) search field, type or select your search criteria, as follows:

- For most properties, you type custom search criteria directly into this field. Examples include actual request IDs, user names, and business units.
  For example, to search for the request whose ID is 101, specify the following in the search fields:
  property: Request ID operator: Equals value: 101
  Similarly, to search for three requests whose IDs are 101, 102, and 103, specify the following in the search fields:
  property: Request ID operator: In value: 101,102,103

  
  Note: Use a comma to separate multiple values in the value field.

- If you are a Service Delivery administrator, and you plan to share the advanced search query with other users:
    - For the properties that include the user ID, specify the value as the $USERID$ variable.
    - For the properties that include the business unit ID, specify the value as the BU$ variable.

When other users run this query, the Catalog system dynamically replaces the variable with the user ID or business unit ID of the user running the query. This dynamic replacement is useful for complex advanced search queries that other users find beneficial but lack the expertise to create.

- For certain properties, this field changes to a drop-down list, and you select the value you want from the list. For example, if you are searching for a property related to the request status, you select the request status you want from the drop-down list. If your implementation includes custom statuses, they appear in this list.
  For example, to search for requests whose status is Approved, specify the following in the search fields:
  property: Request Current Status operator: Equals value: Approved
  Similarly, to search for requests whose statuses are Approval Done or Approval Not Needed, specify the following in these fields:
  property: Request Current Status operator: In value: Approval Done and Approval Not Needed

- If you are searching for a property related to the dates, if required, you can include multiple dates in your query by using operators such as Before or After, and by using multiple search conditions.
  For example, to find request created between July 27, 2011 and July 30, 2011, inclusive, specify both of the following conditions in your query:
  property: Request Date Created operator: After or On value: 07/27/2011
  property: Request Date Created operator: Before or On value: 07/30/2011

- To find requests related to inactive users, specify one or both of the following properties: *Requested For User Status* and *Requested By User Status*. For example, to find requests created by an inactive user, specify the following
  property: Requested By User Status operator: Equals value: Inactive

  Note: For queries involving inactive users, you must specify these properties first, before you specify any other search criteria.

You have completed this search condition.

4. Click the Plus sign (+) after the third search field to specify another search condition, if required.

5. Click the Remove (-) icon after the third search field of any additional search conditions that you want to remove from the advanced search query, if required.
   You have finished specifying this advanced search query.

Only Service Delivery administrators can share queries. A shared query appears as a saved query for all users when they click the Load icon. All users in all business units can view and run shared queries, but cannot modify them.

Follow these steps to share an advanced search query:

1. Click the Save icon.

2. Enter meaningful data in the Save Query dialog.

3. (Optional) Click Share to share the query with other users.

Note: The Catalog system includes several predefined shared queries at installation time. Service Delivery administrators can optionally unshare or delete any queries that do not apply to their implementation.

You can load an advanced search.

Follow these steps to load an advanced search:

1. Click the Load icon.

2. Filter the list to display all queries, shared queries only, or personal queries.

3. Select a query and click Search**.**

Use Widgets for Request Management

Service Managers work with application administrators, such as portal administrators and solution designers to embed CA Service Catalog widgets and let users access request life cycle functions.

You can embed CA Service Catalog widgets that fit either a broad or special-interest context. For example, on a web page that features virtual desktop services, you can embed the Browse widget to let catalog users view the services in the catalog. You can also add the Request widget to enable the users to request the virtual desktop services they want. Similarly, on a service desk page, you can use the Status, Request List, Edit Request widgets. These widgets work together to let request managers approve and reject their requests pending action. This setup enhances the user experience for both catalog users and request managers.

Embedding CA Service Catalog widgets provides the following benefits:

- Segregate the request life cycle functions from other software, including other portals and portlets.
- Simplify the process. Users can easily access the catalog, create and submit requests, and manage requests.
- Create different pages for a special folder, interest, or user group.

Follow these steps:

- Step 1 - Review the Prerequisites and Guidelines for Widgets Implementation (see page 2177)
- Step 2 - Understand the CA Service Catalog Widgets (see page 2179)
- Step 3 - Implement the Widgets in Liferay or SharePoint (see page 2182)
- Step 4 - Test the Widgets (see page 2196)

Step 1 - Review the Prerequisites and Guidelines for Widgets Implementation

This article contains the following topics:

Prerequisites for Embedding Widgets

To use CA Service Catalog widgets in other applications, verify that you meet these prerequisites:

General Prerequisites

- Understand the difference between widgets and portlets: Widgets are snippets of code that you can embed in an HTML page. The widget provides a UI that is typically a service. Portlets are mini Java Web applications that a Java portal server like Liferay hosts. Portlets can be embedded in other pages but the portlets require a portal server to function. Examples of widgets that are embedded in other applications include the Facebook Like button, Google embedded maps, and Twitter feeds.
  The CA Service Catalog widgets can include CSS, HTML, and JavaScript code in a script. Portal applications that use widgets include Liferay and SharePoint.

  Note: CA Service Catalog widgets are configured out-of-the-box with Unified Self-Service.

- (Recommended) Configure the portal or application in which you want to use widgets to use Single Sign-On (SSO). Typically, you use either Windows NTLM domain authentication or an SSO application, for example, CA SiteMinder. Configure CA Service Catalog to implement SSO using the same method as the portal or application.

- Decide which of the following widgets to use on which pages of your portal or application, and in what context.

  - Browse Widget
  - Request Widget
  - Status Widget
  - Request List
  - Edit Request

  For example, you can use the Browse and Request widgets together to let catalog users request a service.

You must also be:

- A proficient user and administrator of CA Service Catalog.
- A proficient user and administrator of the portal or application from which you want to call the widget.

- Familiar with JavaScript, HTML, and web page design.

Portal Prerequisites

- Ensure that you can create containers, portlets, and other required elements in the portal. For example, Liferay. The container stores the portlet, and the portlet calls the CA Service Catalog widget.
- Verify that your portal follows JSR-168 and JSR-286 standards for portlets, if you want to use widgets without coding source directly. The CA Service Catalog portlets follow these standards so that you can deploy them on any standard Java Portal container. Portals that meet these standards let you configure the function of the widgets using menu options rather than source code. The portal software then translates your menu selections into the required JavaScript automatically.

Guidelines for Widgets Implementation

Review the following guidelines so that you can implement widgets efficiently:

Portal Pages

- Do not use the Request and Edit Request widgets on the same portal page.

  Important! Placing both widgets on the same page can result in an error that indicates that one of the widgets cannot render forms or process JavaScript correctly. So, catalog users cannot complete and submit requests and request managers cannot approve and reject requests pending actions.

  To address this limitation, embed the widgets as designed in this scenario:

  - On page 1, embed the Browse and Request widgets.
  - On page 2, embed the Status, Request List, and Edit Request widgets.

- All widgets on the same portal page *must* connect to the same CA Service Catalog host. For example, the Browse and Request widgets must specify the same CA Service Catalog host.
- Specify uniform configuration parameters for all widgets on the same page.
  For example, suppose the value of the Business Unit parameter of the Status widget is SaoPaulo12. In that case, the value of this parameter for the Request List, and Edit Request widgets must also be SaoPaulo12.
- Ensure that your request URL does not exceed 8KB. You can, however, configure this value as follows.

  1. a. Include the maxHttpHeaderSize attribute in the connector tag of the server.xml file that is at USM_HOME/view/conf path.

     b. Specify the new value for the maxHttpHeaderSize attribute. For example, specify maxHttpHeaderSize=16384 to allow request URL up to 16KB.

- Use the CA Service Catalog UI and not the widgets to transfer, delegate, take, return, hold, resume, and push through requests.
- The following functionalities are not available in the widgets:
  - Pending Override icon
  - Gold brick icon for assigning assets from catalog request
  - Display Service Health option

Liferay and SharePoint

The Liferay procedures in this scenario are for Liferay Portal Community Edition 6.1.2 CE. For more information about how to configure portlets for other supported versions of Liferay, see your Liferay documentation.

The SharePoint procedure in this scenario is for Microsoft SharePoint 2013. For more information about how to configure portlets for other supported versions of Microsoft SharePoint, see your Microsoft SharePoint documentation.

- To embed widgets in portlets on Liferay pages, you can use *either* source code *or* menu options. The menu options are provided through CA Service Catalog WAR files.
- To embed widgets in portlets on Microsoft SharePoint pages, use source code *only*.

If you are using other portal software, see the documentation of that portal for more information.

Accessibility

Widgets and portlets are accessible to users with visual disabilities using a screen reader such as JAWS. This access affects widgets and portlets *only*. If you intend to utilize this access, ensure that the *container* is also accessible.

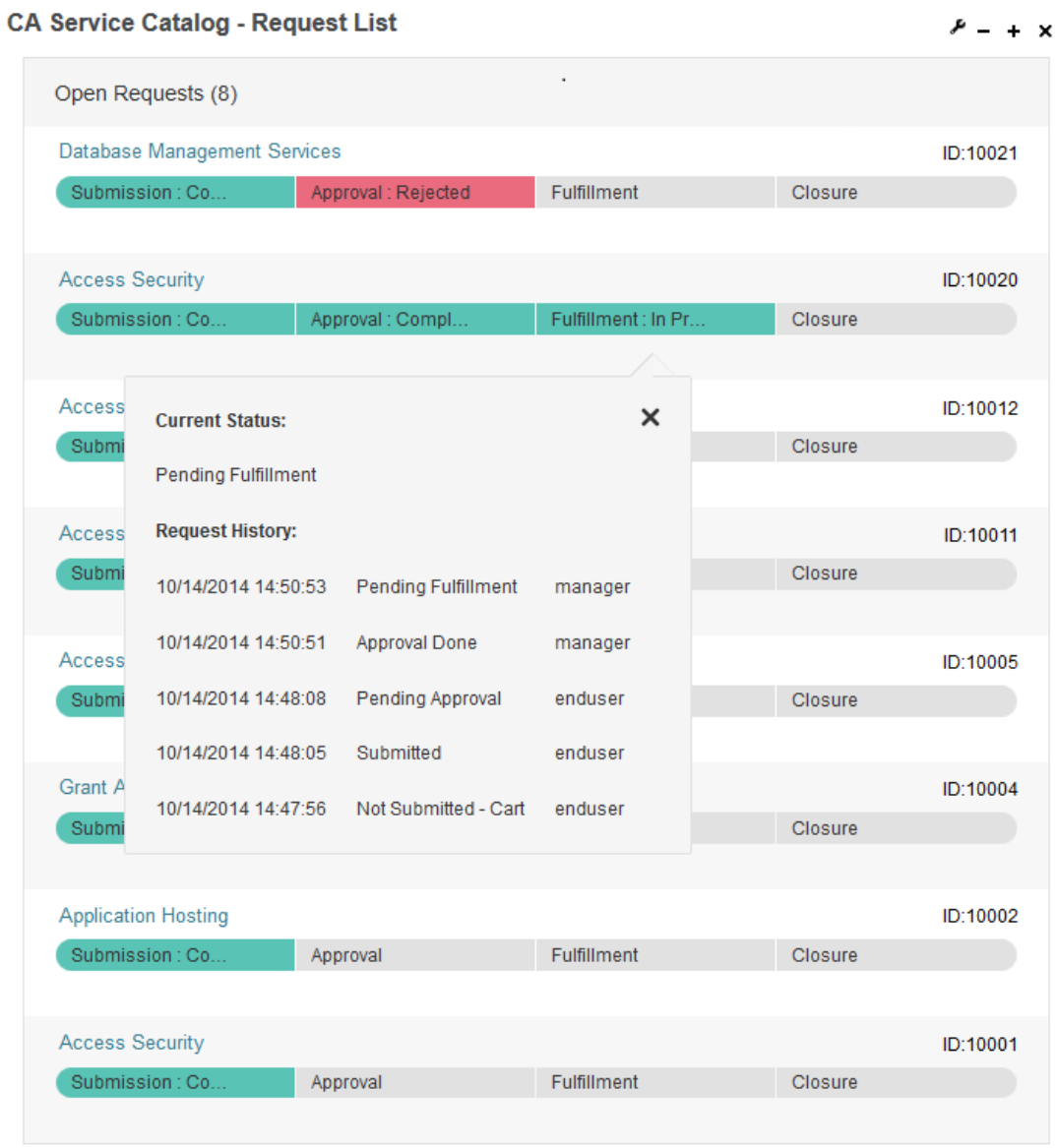
The keyboard shortcuts are as follows:

- Press Ctrl+Shift+Z to reach the first service offering from the category tree in the browse widget.
- Press letter V (small letter) to open the popup window when you click the links in the list widget.
- Press Ctrl+Shift+O to reach the first button in button area when a request form is loaded and the focus is at any place in between the form.

Step 2 - Understand the CA Service Catalog Widgets

Before implementing widgets, understand which widget to use when. On the first portal page, you embed the Browse and Request widgets. On the second portal page, you embed the Status, Request List, and Edit Request widgets.

The Request List widget displays the state that the request is in. Click on the bar to see the current status and request history of the request as shown in the following graphic:



Request List widget

- Use the Browse Widget to Display Services to Users (see page 2180)
- Use the Request Widget to Let Users Request Services (see page 2181)
- Use the Status, Request List, and Edit Request Widgets to Let Users Manage Their Unsubmitted Requests (see page 2181)
- Use the Status, Request List, and Edit Request Widgets to Let Users Manage Submitted Requests (see page 2181)
- Use the Status, Request List, and Edit Request Widgets to Let Users Manage Their Open Requests (see page 2181)
- Use the Status, Request List, and Edit Request Widgets to Let Approvers Approve or Reject Requests (see page 2181)

Use the Browse Widget to Display Services to Users

Use the Browse widget to offer services to users. You can use the Browse widget to offer the entire catalog or one specific folder or list of services. In this scenario, you offer the entire catalog through the Browse widget. Users can click any folder to display the services in the folder. Users can view the predefined folders and featured services to view their content.

Use the Request Widget to Let Users Request Services

Use the Request widget to let users request the services that you offer through the Browse widget. In this scenario, you add the Request widget next to the Browse widget. When the users click any service, the Request widget displays the service, including any forms. Users can complete the form and can submit the request.

For example, the user clicks the service "To host an application". The Request widget displays the service, so that the user can complete the form and can request the service. This action occurs automatically when you use the Browse and Request widgets on the same page and you select **Send local event which other widgets can listen** in the **Open In** parameter of the Browse widget.

Use the Status, Request List, and Edit Request Widgets to Let Users Manage Their Unsubmitted Requests

Use the Status and Request List widgets together, to provide the following function: When users click **Cart** on the status widget, the Request List widget opens the cart. **Cart** displays the number of items that the user has added to the cart but not submitted.

When the page includes Edit Request widget, users can view, add attachments, add notes, and change certain request details. Users *cannot* add more services, service option groups, or service options to the request.

Use the Status, Request List, and Edit Request Widgets to Let Users Manage Submitted Requests

Use the Status and Request List widgets together, to provide the following functions:

- Let users click **Open** to manage their open requests. Click **Open** to see the number of requests that the user has submitted but that have not been approved or rejected.
- Let users click **Closed** to view their completed or cancelled requests.

When the page includes Edit Request widget, the user can also act on these requests.

Use the Status, Request List, and Edit Request Widgets to Let Users Manage Their Open Requests

Use the Status and Request List widgets together, to display the *open requests* of the user when user clicks **Open**. Open requests are requests that the user has submitted but that the aprover has not yet approved or rejected. When the page includes the Edit Request widget, users can also make updates: Users can view, update (add notes or attachments), or cancel requests.

The user clicks **Open** on the Status widget, and the Request List widget opens the submitted requests.

Use the Status, Request List, and Edit Request Widgets to Let Approvers Approve or Reject Requests

Use the Status and Request List widgets together, to let users who have request approval rights open the requests pending action in their queues when they click **Pending** in the Status widget.

When the page includes the Edit Request widget, request approvers can also approve or reject these requests.

Step 3 - Implement the Widgets in Liferay or SharePoint

You can implement the CA Service Catalog widgets in Liferay or SharePoint. In Liferay, you can implement the widgets using the menu options (see page 2182) or using the source code (see page 218). In SharePoint, you can implement the widgets *only* using the source code (see page 2192).

Important! We recommend using the menu options to implement the widgets in Liferay.

(Recommended) Configure Widgets in Liferay using Menu Options

In Liferay 6.1.2 CE, as a CA Service Catalog administrator you deploy the CA Service Catalog WAR files and then configure the widgets using the menu options.

Follow these steps:

- Step a - Deploy the WAR files in Liferay 6.1.2 CE (see page 2182)
- Step b - Configure the Widgets (see page 2183)
  - Key Parameters for the Browse Widget (see page 2186)
  - Key parameters for the Request Widget (see page 2186)
  - Key Parameters for the Status Widget (see page 2187)
  - Key Parameters for the Edit Request Widget (see page 2188)
  - Key Parameters for the Request List Widget (see page 2188)

Step a - Deploy the WAR files in Liferay 6.1.2 CE

Deploy the CA Service Catalog Web Application Archive (WAR) file in Liferay 6.1.2 CE. The WAR files let you configure the display and behavior of CA Service Catalog widgets in portlets.

Follow these steps:

1. Copy the following WAR files stored in the *usm_home**filestore**portlets* folder from the CA Service Catalog computer to the deploy folder of the Liferay computer. The deploy folder is in the Liferay install location.
   - browse.war
   - request.war
   - request-list.war
   - request-edit.war
   - status.war

Note: All widgets on a page must use the same CA Service Catalog computer. If you are using a cluster, specify the computer name of the load balancer.

2. Run the startup.bat file on the Liferay computer.

Note: The startup.bat file is in tomcat-7.0.40\bin folder of the Liferay install location.

3. Log into Liferay portal with the credentials provided by your Liferay administrator.
   CA Service Catalog folder is displayed when you click **Add**, **More**. The WAR files have been deployed in Liferay.

Step b - Configure the Widgets

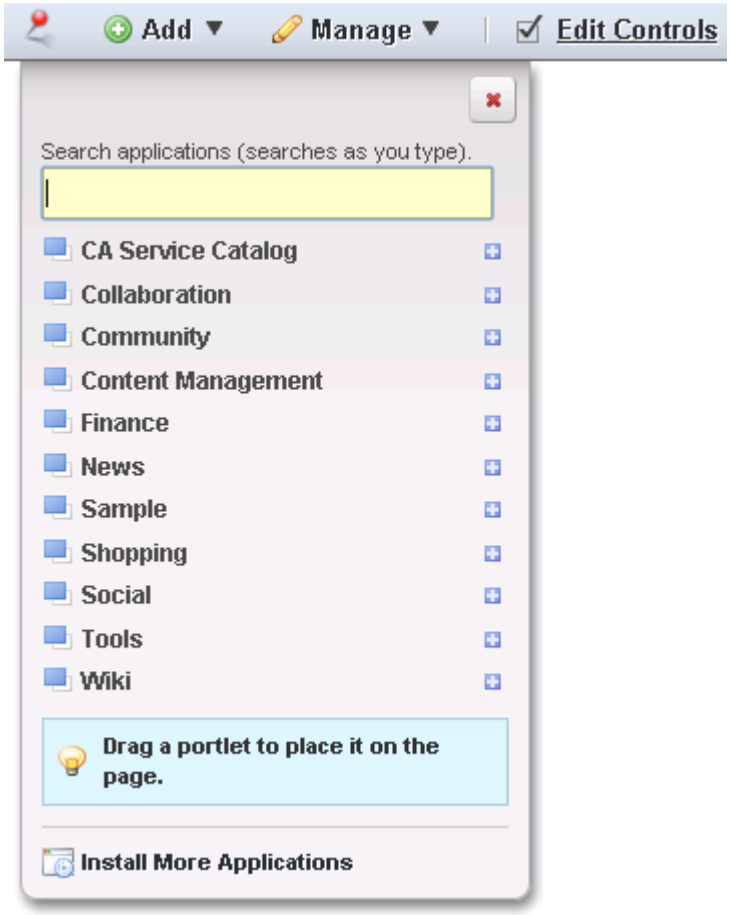
Use the CA Service Catalog WAR files to configure the display and behavior of CA Service Catalog widgets in portlets by using menu options.

Follow these steps:

1. Log into Liferay Portal with the credentials provided by your Liferay administrator.

2. Click **Add**, **Page** to create a page for your widgets.

3. Click **Add**, **More** on your portal page.
   The list of preconfigured portlets including a folder for CA Service Catalog appears as displayed in the following graphic:



List of Preconfigured Portlets

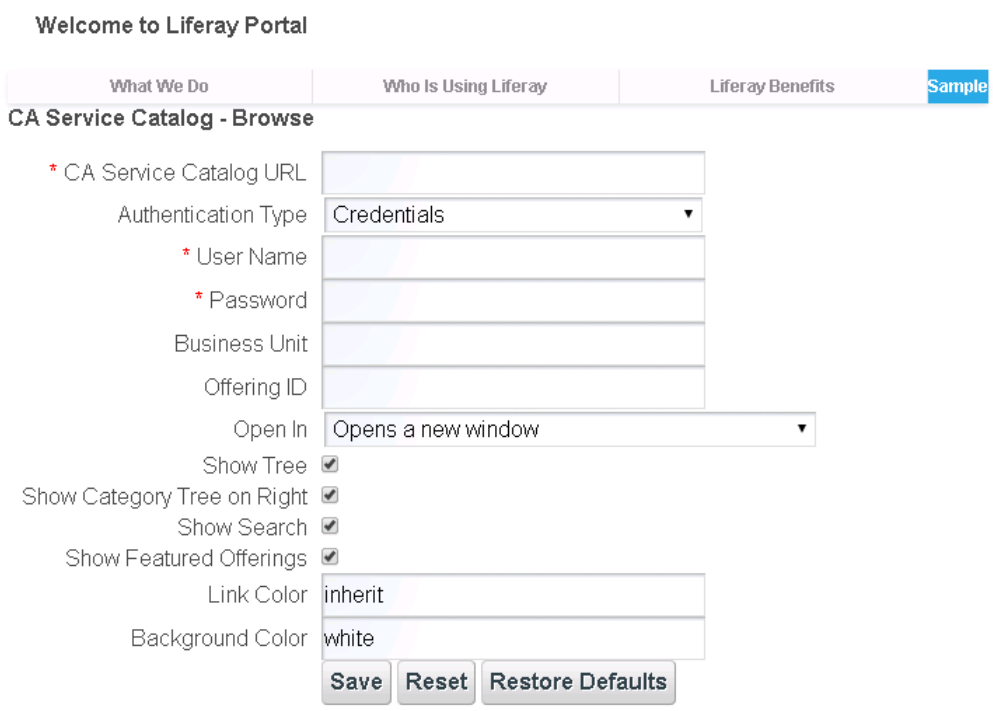
4. Expand **CA Service Catalog** on the list.

5. Select the widget you want to implement and click **Add**. Alternatively, drag-and-drop the widget onto the location you want.

6. Ensure that **Edit Controls** at the top of the page is selected.

7. Mouse over the widget, click the wrench (Options) icon, and select **Preferences** from the drop-down list.

8. Review and modify the parameters for the different widgets, as shown in the following graphic:



Modify the Widget Parameters

The key parameters for the different widgets are in the following sections:

- Key Parameters for the Browse Widget (see page 2186)
- Key Parameters for the Request Widget (see page 2182)
- Key Parameters for the Status Widget (see page 2182)
- Key Parameters for the Edit Request Widget (see page 2182)
- Key Parameters for the Request List Widget (see page 2188)

Note: There are other parameters available for the widgets. For example, background color or link color for the browse widget. You can modify any of these parameters depending upon your requirements.

9. Save your settings and review the portlet.
   The widget has been configured in Liferay.

Note: Embed the Browse and Request widgets on the first page (the Service Catalog page). These widgets work together to let catalog users browse the catalog and request services. Embed the Status, Request Edit, and Request List widgets in the second page (the Service Request page).

For each widget, ensure that:

Catalog URL=http://*host-name*:*port-number*/usm specifies the same CA Service Catalog host name and CA Service Catalog port number that you deployed the WAR Files in Liferay. Include the "/usm" in the URL for the portlet to render correctly.

Authentication Type specifies how to authenticate users. We recommend Single-Sign On for widgets.

Key Parameters for the Browse Widget

The key parameters for the Browse widget follow:

- **Business Unit**
  Specifies the business unit that catalog users can access while utilizing this Browse widget. Catalog users can browse services that they are entitled to. If you do not specify a value, the Catalog system uses the default business unit of the user accessing the widget.

- **Offering ID**
  Specifies the object ID of a single folder only or list of services that the Browse widget displays. You can specify either a single folder or a comma-separated list of services, using their object IDs.

  Note: The folder or list of services that you specify must exist in a business unit that the user can access. Do not provide both folder IDs and service IDs in the list.

- **Open In**
  Specifies how a service opens in the Request view when the user clicks the service on the Browse widget.
  Values:

  - **Opens a new window**
    Opens the service in the catalog, on a new page. The user requests the service on that page.

  - **Raise request in top most frame**
    Performs the same function as **Opens a new window**, except that the service opens in the top-most frame of the browser. If the service is a frame, then the first associated frame in service option element is selected.

  - **Raise request in same page**
    Opens the service in the catalog, on the same page.

  - **Send local event which other widgets can listen**
    Specifies that another widget on the same page listens to events from the Browse widget and responds to them. When the user clicks a service, the Request widget responds by opening the service. Add the Request widget to this page to enable this function.

  - **URL**
    Opens the service using a custom URL. The URL can include a placeholder for the object ID of the service. For example, http://www.google.com?id={action}

Key parameters for the Request Widget

The key parameters for the Request widget follow:

- **Business Unit**
  Specifies the business unit that catalog users can access while utilizing this Request widget. Users can request services that they are entitled to. If you do not specify a value, the Catalog system uses the default business unit of the user accessing the widget.

- **Offering Id**
  Specifies the service to display when the Request widget opens initially. When the user clicks a service in the Browse widget, the Request widget displays that service.

  Allowed Values: Valid Offering ID that must exist in a business unit that the user can access. If you specify -1 or leave this parameter blank, the widget displays nothing.

Key Parameters for the Status Widget

The key parameters for the Status widget follow:

- **Business Unit**
  Specifies the business unit that catalog users can access while utilizing this Status widget. Users can view the status of the requests that they are entitled to.

  - Users who are not request managers can view the status of their own requests only.

  - Request managers can view the status of both their own requests and the requests pending action that is assigned to them.

  If you do not specify a value, the Catalog system uses the default business unit of the user accessing the widget.

- **Layout**
  Specifies how the options on the Status widget are displayed.
  Box Layout displays the options as buttons in a single row.
  Row Layout displays the options in each row in a table with a description.

- **Open In**
  Specifies how a target opens when the user clicks it on the Status widget. In this scenario, when the user clicks a service, another widget responds by opening the target. The targets are as follows:

Option	Target Function	Widget
Cart	Shopping Cart	Edit Request
Open	Open Requests	Request List
Closed	Closed Requests	Request List
Pending	Requests Pending Action	Request List

  For example, to enable these target functions to complete correctly when users click the option **Cart** in the cart, add the Edit Request widget .

Values:

-

- **New window**
  Opens the target on a new page.

- **Top frame**
  Performs the same function as **New window**, except that the target opens in the top-most frame of the browser. If the target is a frame, then the first associated frame in the service option element is selected.

- **Same page**
  Opens the target in the catalog, on the same page.

- **Other Widget**
  Indicates that another widget on the same page listens to events from the Status widget and responds to them.

- **URL**
  Opens the target using a custom URL. The URL can include a placeholder for the object ID of the source context, for example, the service.
  An example follows:

```
http://www.google.com?id={action}
```

Key Parameters for the Edit Request Widget

The key parameters for the Edit Request widget follow:

- **Business Unit**
  Specifies the business unit that catalog users can access while utilizing this Edit Request widget. Users can edit requests that they are entitled to.
  If you do not specify a value, the Catalog system uses the default business unit of the user accessing the widget.

- **Request ID**
  Specifies the request to display when the Request List widget opens initially.
  When the user clicks an option on the Status widget, the Request List widget displays the matching item: the cart, open requests, completed requests, or requests pending action.
  Allowed Values: Valid Request ID that must exist in a business unit that the user can access. If you specify an invalid Request ID or leave this parameter blank, the widget displays nothing.

Key Parameters for the Request List Widget

The key parameters for the Request List widget follow:

- **Business Unit**
  Specifies the business unit that catalog users can access while utilizing this Request List widget. Users can list and view requests that they are entitled to.
  If you do not specify a value, the Catalog system uses the default business unit of the user accessing the widget.

- **Type**
  Specifies that the default setting for this Request List widget is to display pending requests (requests pending action). Other options include open, closed, or recent requests.

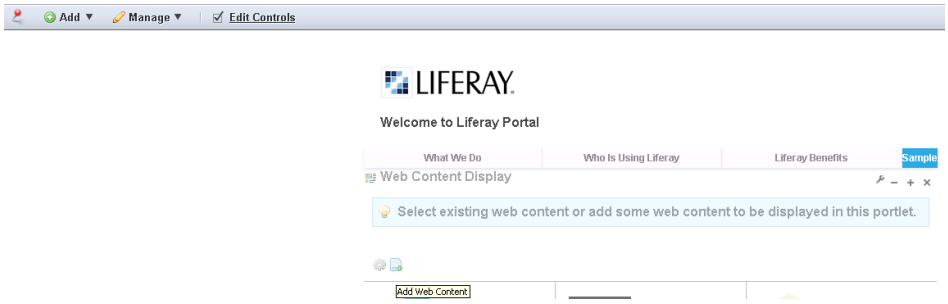
Configure Widgets in Liferay using Source Code

In Liferay 6.1.2 CE, as a CA Service Catalog administrator you can also call the widget by creating the portlet and specifying the source code. To configure the display and behavior of the widget in your implementation, follow the source code examples as a model.

Important! Ensure that you review the source code HTML example files for the widgets you want to implement before modifying the parameters. The source code HTML files are available at USM_HOME\view\webapps\usm path.

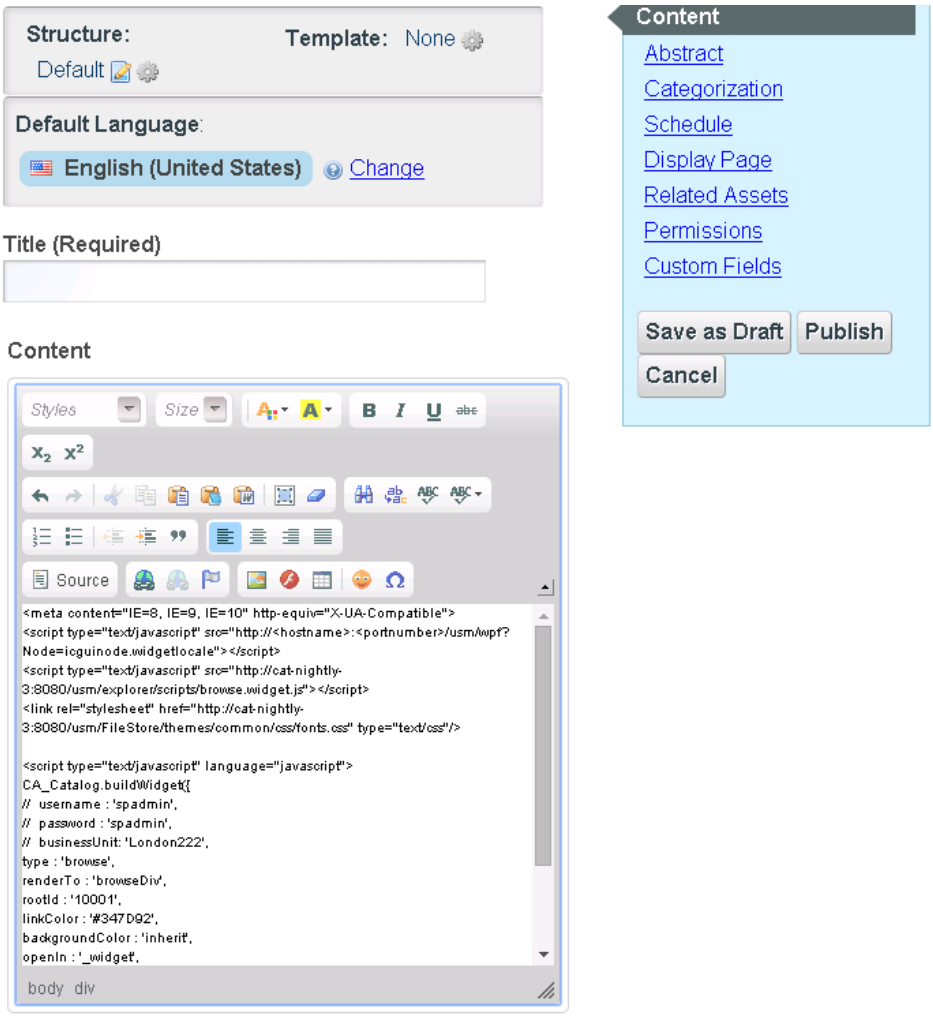
Follow these steps:

1. Log into Liferay Portal with the credentials provided by your Liferay administrator.
2. Click **Add**, **Page** to create a page for your widgets.
3. Perform these actions to create the portlet in the portal page:
   a. Click **Add**, **Web Content Display**.
   b. Click **Add Web Content** as shown in the following graphic:



Liferay Portal Page

   c. Copy the source code for the widget that you want to embed in the **Content** section as shown in the following graphic:



Content section of Liferay Portal Page

The following HTML files are available for the widgets:

- browse html

  Specifies the HTML code for the Browse widget

- broswe_request html

  Specifies the combined HTML code for the Browse and Request widgets.

- status

  Specifies the HTML code for the Status widget

- status_list

  Specifies the combined HTML code for the Status and Request List widgets.

- status_list_editrequest

Specifies the combined HTML code for the Status, Request List, and Edit Request widgets.

Note: Embed the Browse and Request portlets on the first page (the Service Catalog page). Embed the Status, Request Edit, and Request List portlets in the second page (the Service Request page).

d. Specify the host name and the port number of the CA Service Catalog computer in each line of the source code for the different widgets as follows:

```
<script type="text/javascript" src="http://<hostname>:<portnumber>/usm
/explorer/scripts/browse.widget.js"> </script>
```

Update each of the following lines in the source code for the different widgets with the host name and port number information of the CA Service Catalog computer:

- browse.html file:

```
<script type="text/javascript" src="/usm/wpf?Node=icguinode.
widgetlocale"></script>
<script type="text/javascript" src="/usm/explorer/scripts/browse.
widget.js"></script>
<link rel="stylesheet" href="/usm/FileStore/themes/common/css/fonts.
css" type="text/css"/>
```

- browse_request.html file:

```
<script type="text/javascript" src="/usm/wpf?Node=icguinode.
widgetlocale"></script>
<script type="text/javascript" src="/usm/explorer/scripts/browse.
widget.js"></script>
<script type="text/javascript" src="/usm/explorer/scripts/request.
widget.js"></script>
<script type="text/javascript" src="/usm/gwt/fdRenderer/fdRenderer.
nocache.js"></script>
<link rel="stylesheet" href="/usm/FileStore/themes/common/css/fonts.
css" type="text/css"/>
```

- status.html file:

```
<script type="text/javascript" src="/usm/wpf?Node=icguinode.
widgetlocale"></script>
<script type="text/javascript" src="/usm/explorer/scripts/status.
widget.js"></script>
<link rel="stylesheet" href="/usm/FileStore/themes/common/css/fonts.
css" type="text/css"/>
```

- status_list.html file:

```
<script type="text/javascript" src="/usm/wpf?Node=icguinode.
widgetlocale"></script>
<script type="text/javascript" src="/usm/explorer/scripts/status.
widget.js"></script>
<script type="text/javascript" src="/usm/gwt/requestList/requestList.
nocache.js"></script>
<script type="text/javascript" src="/usm/explorer/scripts/request-
list.widget.js"></script>
<link rel="stylesheet" href="/usm/FileStore/themes/common/css/fonts.
css" type="text/css"/>
```

- status_list_editrequest.html file:

```
<script type="text/javascript" src="/usm/wpf?Node=icguinode.
widgetlocale"></script>
<script type="text/javascript" src="/usm/gwt/fdRenderer/fdRenderer.
nocache.js"></script>
<script type="text/javascript" src="/usm/explorer/scripts/status.
widget.js"></script>
<script type="text/javascript" src="/usm/explorer/scripts/request-
list.widget.js"></script>
<script type="text/javascript" src="/usm/explorer/scripts/edit.
request.widget.js"></script>
<link rel="stylesheet" href="/usm/FileStore/themes/common/css/fonts.
css" type="text/css"/>
```

e. Specify the other required fields and close the window.

> **Note:** There are other parameters available for the widgets. For example, background color or link color for the browse widget. You can modify any of these parameters depending upon your requirements.

The new portlet gets added to Liferay.

4. (Optional) Perform these actions to edit the portlet in the portal page.

   a. Ensure that **Edit Controls** at the top of the page is selected.

   b. Mouse-over the portlet, and click the pencil (Edit Web Content) icon.

   c. Click **Source** in the Content window.

   d. Modify the parameters in the source file.
   The portlet is modified.

5. Close the Source container and click **Publish** to review the updated portlet.
   The widget is configured in Liferay using source code.

Configure Widgets in SharePoint using Source Code

In Microsoft SharePoint 2013, as a CA Service Catalog administrator you call the widget by creating the portlet and specifying the source code. To configure the display and behavior of the widget in your implementation, follow the source code examples as a model:

> **Important!** Ensure that you review the source code HTML example files for the widgets you want to implement before modifying the parameters. The source code HTML files are available at USM_HOME\view\webapps\usm path.

Follow these steps:

1. Verify with your Microsoft SharePoint administrator that a site page has been created for your organization. Ensure that you can access this site page.

2. Log into your Microsoft SharePoint site page with the credentials provided by your SharePoint administrator.

3. Perform these actions to create the portlet in the portal page:

    a. Click **EDIT** in the upper right corner of your SharePoint page.

    b. Click **INSERT**, **Embed Code** to insert the source code of the widget you want to embed in the page.

    c. Copy the source code for the widget that you want to embed. The following HTML files are available for the widgets:

    - browse html

      Specifies the HTML code for the Browse widget

    - broswe_request html

      Specifies the combined HTML code for the Browse and Request widgets.

    - status

      Specifies the HTML code for the Status widget

    - status_list

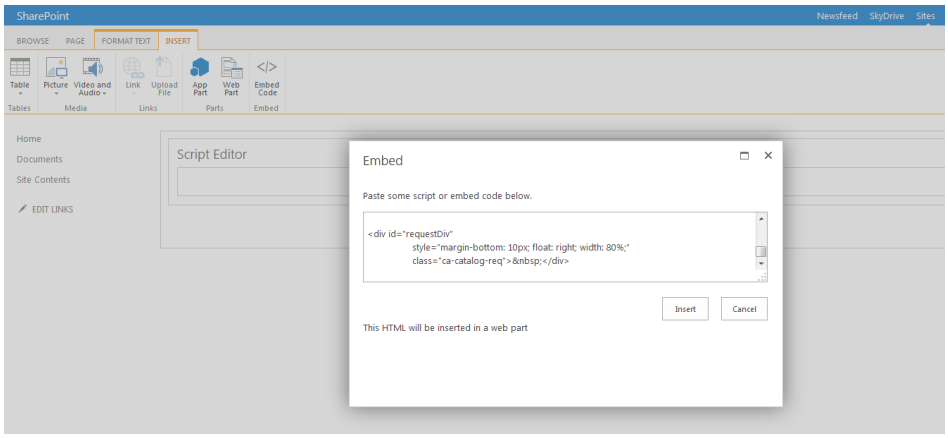
      Specifies the combined HTML code for the Status and Request List widgets.

    - status_list_editrequest

      Specifies the combined HTML code for the Status, Request List, and Edit Request widgets.

    Note: Embed the Browse and Request portlets on the first page (the Service Catalog page). Embed the Status, Request Edit, and Request List portlets in the second page (the Service Request page).



Embed code

d. Click **Insert**.

e. Specify the host name and the port number of the CA Service Catalog computer as follows:

```
<script type="text/javascript" src="http://<hostname>:<portnumber>/usm
/explorer/scripts/browse.widget.js"> </script>
```

Update each of the following lines in the source code for the different widgets with the host name and port number information of the CA Service Catalog computer:

- browse.html file:

```
<script type="text/javascript" src="/usm/wpf?Node=icguinode.
widgetlocale"></script>
<script type="text/javascript" src="/usm/explorer/scripts/browse.
widget.js"></script>
<link rel="stylesheet" href="/usm/FileStore/themes/common/css/fonts.
css" type="text/css"/>
```

- browse_request.html file:

```
<script type="text/javascript" src="/usm/wpf?Node=icguinode.
widgetlocale"></script>
<script type="text/javascript" src="/usm/explorer/scripts/browse.
widget.js"></script>
<script type="text/javascript" src="/usm/explorer/scripts/request.
widget.js"></script>
<script type="text/javascript" src="/usm/gwt/fdRenderer/fdRenderer.
nocache.js"></script>
<link rel="stylesheet" href="/usm/FileStore/themes/common/css/fonts.
css" type="text/css"/>
```

- status.html file:

```
<script type="text/javascript" src="/usm/wpf?Node=icguinode.
widgetlocale"></script>
<script type="text/javascript" src="/usm/explorer/scripts/status.
widget.js"></script>
<link rel="stylesheet" href="/usm/FileStore/themes/common/css/fonts.
css" type="text/css"/>
```

- status_list.html file:

```
<script type="text/javascript" src="/usm/wpf?Node=icguinode.
widgetlocale"></script>
<script type="text/javascript" src="/usm/explorer/scripts/status.
widget.js"></script>
<script type="text/javascript" src="/usm/gwt/requestList/requestList.
nocache.js"></script>
<script type="text/javascript" src="/usm/explorer/scripts/request-
list.widget.js"></script>
<link rel="stylesheet" href="/usm/FileStore/themes/common/css/fonts.
css" type="text/css"/>
```

- status_list_editrequest.html file:

```
<script type="text/javascript" src="/usm/wpf?Node=icguinode.
widgetlocale"></script>
<script type="text/javascript" src="/usm/gwt/fdRenderer/fdRenderer.
nocache.js"></script>
<script type="text/javascript" src="/usm/explorer/scripts/status.
widget.js"></script>
<script type="text/javascript" src="/usm/explorer/scripts/request-
list.widget.js"></script>
<script type="text/javascript" src="/usm/explorer/scripts/edit.
request.widget.js"></script>
<link rel="stylesheet" href="/usm/FileStore/themes/common/css/fonts.
css" type="text/css"/>
```

Note: There are other parameters available for the widgets. For example, background color or link color for the browse widget. You can modify any of these parameters depending upon your requirements.

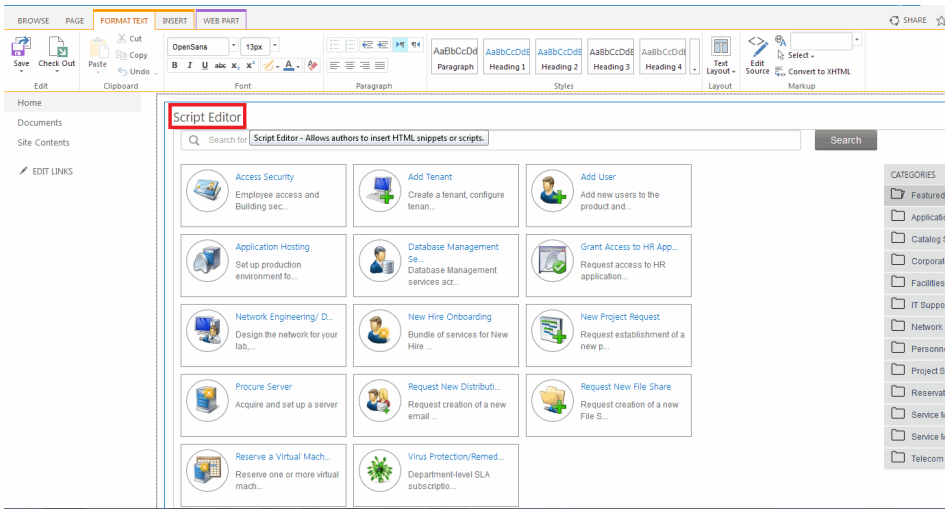
f. Click **SAVE**.

The widget is added to your Microsoft SharePoint page.

4. (Optional) Perform these actions to edit the portlet in the portal page.

   a. Click **EDIT** in the upper right corner of the SharePoint page.

   b. Click **Script Editor**.

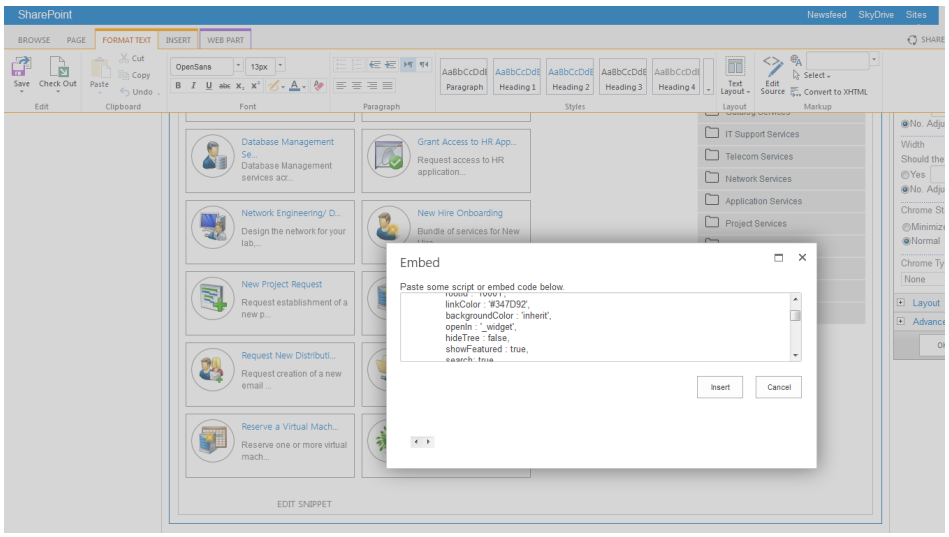


Script Editor

c. Click **WEB PART**, **Web Part Properties**.

d. Scroll to the end of the page and Click **EDIT SNIPPET** in Script Editor.

e. Modify the required parameters and click **Insert**.



Modify parameters

f. Click **SAVE**.
The widget is modified.

Step 4 - Test the Widgets

Verify that the widgets appear and function as intended on portal pages or other pages on which you embedded them.

Follow these steps:

1. Access the pages that include the widgets.

2. Verify the following functions on the first page:
   - The Browse and Request widgets appear as intended.
   - The widgets work together to let catalog users view and request services.
3. Verify the following functions on the second page:
   - The Status, Edit Request, and Request List widgets appear as intended.
   - Catalog users can perform the following tasks:
     - Review the status of their submitted requests.
     - Add notes and attachments for submitted requests that have not yet been approved or rejected.
   - Request managers can manage their requests pending action by approving or rejecting them.

You have tested the widgets.

Request Management from a User Perspective

After you have submitted your cart, you have launched your new request into its life cycle. Each requested service option in the request has a status that reflects its current step in the request life cycle. The overall request also has a milestone status that reflects the aggregate values of the statuses of the requested service options. The milestone statuses are:

- Not Submitted
- Submitted
- Pending Approval
- Approved/Rejected
- Pending Fulfillment
- Fulfilled
- Completed/Cancelled

Each status range contains various detailed status values. The status values are customizable by your catalog administrator. During the approval and fulfillment phases for your request, you can receive emails informing you of the progress of your request through its life cycle. The business process for approval and fulfillment, the status values used and whether you receive emails depends on the approval and fulfillment business processes of your service provider.

For example, you request a Desktop service which includes a Standard Desktop service option and Microsoft Visio service option. Your request includes one service which contains two service options. If your service provider requires manager approval, the first step is for your manager to approve or reject your request for the Desktop service. After approval phase is complete for the two service

options Standard Desktop and Microsoft Visio, the fulfillment phase begins. If the fulfillment process for these two service options includes checking available inventory, an asset manager checks the inventory.

Assuming both the Standard Desktop and a Microsoft Visio license are found in inventory, the status of each service option changes to Filled From Inventory. The next step in the fulfillment process is to notify IT Services to configure and deliver the Standard Desktop and Microsoft Visio so the status of each service option changes to Notified IT Services. After each service option is configured and delivered to you, the status of each service option changes to Fulfilled. After each service option in the request is set to Fulfilled, the status of all service options is set to Completed. The request is considered completed or closed.

For this example, for each requested service option, you can view the following status values over time (in chronological order):

- Not Submitted - Cart
- Submitted
- Pending Approval
- Approved
- Approval Done
- Pending Fulfillment
- Check Availability
- Filled From Inventory
- Notified IT Services
- Fulfilled
- Completed

Manage Requests

You can view, modify, copy, and search requests. View requests to check their status, tracking, audit trail, and other details. You can also email copies of requests. The details of a request that you can view and modify vary according to:

- Your role
- The request status
- The configuration options set by your catalog administrator

Follow these steps:

1. Log in to CA Service Catalog, as follows:

a. Enter the URL for CA Service Catalog, in the format http://*computer-name*:*port-number* . Your catalog administrator provides the URL.
If CA Service Catalog is configured to use single sign-on, you are automatically authenticated and the initial page appears. Otherwise the Log In page appears.

b. If the Log In page appears, enter your assigned user name and password.

> **Note:** If you have a user ID in multiple business units, click Advanced. Specify the business unit that you want to log in to.

2. Click Home, Requests.

> **Note:** The Requests page can either display requests directly or provide access to them indirectly through the My Requests drop-down list. Administrators optionally configure the page to use either setup.

3. Click the My Requests drop-down if the page does not list requests and select the option of your choice.

4. If applicable, click the list of requests that contains the request that you want to copy. For example, if you want to copy a completed request, click Completed Requests.

5. Click the name of the request that you want, and proceed as follows:

   - View and optionally update the request, as applicable.

   - Copy the request.

     > **Note:** The notes and attachments for the original request are not copied to the new request. The status of the new request is Not Submitted, so that you can delete the existing services or can add new services in the request.
     > Update the fields as needed, including the *Requested By* and *Requested For* users.

   - To search for requests by request ID or according to the predefined categories on the screen, use the Request Lookup section of the Requests window. You can view only the requests that your role permits.

Review the following information to understand what you can do when you view and can modify requests:

All Statuses

- View the requested services and service options, and other details of the request.
  View the status, which appears in the Status column of any request list, for example, My Recent Requests, Completed Requests. The request status also appears when you view the details of a request.

- View the request status history, by clicking the name of the status in the request details or the Status column.
  Status values appear for the entire request and for each service and service option in the request.
  Review the numbers, names, and meanings of default status values (see page 2108).

- Display and add and attachments.

- Refresh the display.

- Copy the request, as explained earlier in this topic.

- Email a copy of the request.
  To email the details of a request, click the Email button or link, specify the details, and click Send.
  Optionally click Include Request Snapshot to include details of the request in the email.
  Otherwise, the email contains only the text that you specify for the Subject line and the Message Body.
  In the address fields, you can enter email addresses, user IDs, account names, or the *last name, first name* values of user names. Separate multiple entries with a semi-colon (;). If you enter an account name, the Catalog system uses the email address on the account profile.

- View and edit the additional information sections.

- View the subscriptions for service options, if applicable.

Not Submitted Requests

- Submit the request.

- Add or delete services.

- Delete the request.

Open Requests

An open request is one whose status is not Completed or Cancelled.

- View the status history.

- View the details of a request.

- Edit the request.

- Email the request.

Administrators can configure the display of columns on the Open Requests page to display some or all of the following columns:

- ID - Assigned by the system
- Name
- Requested By
- Requested For
- Priority
- Date Created
- Date Modified
- Status

Requests Pending Action

Request managers can approve, reject, fulfill, and perform several other actions for the requests pending action that are assigned to them.

Completed Status

- Cancel a requested service.
- Cancel the request which cancels all the services in the request.

Tracking

If permitted by your role and the configuration options set by your catalog administrator, you can view and click the Tracking tab. This tab displays any CA Process Automation process instances that are related to the requested services and service options. This tab also provides the status and other details of these processes.

Audit Trail

If permitted by your role and the configuration options set by your catalog administrator, you can view and click the Audit Trail tab. This tab displays each service option element and its status changes over time. Each service option is comprised of service option elements.

Request a Service

Users browse or search the catalog, view services, and request the services that they want. The entries in the service catalog that you view are managed by your service provider's catalog administrator. Your catalog administrator can choose to feature certain services from the catalog when you select a category or other service. If so, you can view the Featured Services section of the window appear when you select a related category or service.

The catalog is organized by a category hierarchy created by your catalog administrator. As you drill down into a category, the sub-categories contained in that category appear in the Browse section. Services can be contained in any category or in no category (shown by clicking the Not Categorized link in the initial Browse window). After you have selected a category that contains services, they appear in the Catalog Services section of the window. To further examine or select a service, click its name in the Catalog Services section of the window.

After you have selected a service by clicking its name, the Service Options page appears. This page displays all the service options available with the service. Related service options are organized into a service option group. A service can include several service option groups, each displayed in its own collapsible section of the Service Options page. Some service option groups require a choice of one or more options (presented using a radio button). Other service option groups allow you to select one or more check boxes with the option of not selecting any check boxes. The third type of service option group automatically includes the service options displayed and you cannot clear the service options.

Follow these steps:

1. Log in to CA Service Catalog, as follows:

    a. Enter the URL for CA Service Catalog, in the format http://*computer-name*:*port-number* . Your catalog administrator provides the URL.
    If CA Service Catalog is configured to use single sign-on, you are automatically authenticated and the initial page appears. Otherwise the Log In page appears.

    b. If the Log In page appears, enter your assigned user name and password.

    Note: If you have a user ID in multiple business units, click Advanced. Specify the business unit that you want to log in to.

2. Select **Home**, **Requests**.

3. Browse or search the catalog to find the service you want.
    For example, if you search for "Asset Service", all the services that contain "Asset Service" in any of the following attributes are displayed in the search results:

    - Service Offering Name
    - Offering Description
    - Option Group Name
    - Option Group Description
    - Option Name
    - Option Description

4. Select the required service offering.

5. Select the options that you want. Complete the fields and confirm your selections as needed.

6. (Optional) Update the *Requested For* field if your role permits and if applicable. Request this service for a different user or account.

7. Click Submit if the service includes a Submit button (not a shopping cart).

> **Note:** Service designers configure each service (see page 2997) to use *either* a shopping cart or a Submit button as the method for users to request the service. If the service uses a cart, you can add more services to a cart, remove services, or save the cart.

If one or more service options or services in your request requires approval, the Catalog system sends them to the required request manager or managers.

Occasionally, you cannot submit a service. For example, because a form does not appear correctly or the Submit or Check Out button does not function. In such cases, contact your administrator. Your administrator can typically fix such problems. For example, by updating forms for the service or by updating configuration settings for your business unit or your user ID.

Add Notes or an Attachment

You can add notes or an attachment for a request or a service option, if the administrator for your business unit has enabled these features for your role. If you want to add notes for a request or service option but do not see the corresponding option on the UI, contact your administrator. The UI behavior varies slightly depending on whether the service uses a shopping cart or one-click submit. The service designer selects one of these options when configuring the details of the service (see page 2997).

> **Note:** To enable these features, administrators select **Catalog**, **Configuration**, **Request Management Configuration**. To let users add notes for a request, use the *Access Control: Show General Information* option. To let users add notes for a service option, use the Allow Notes at Service Option Level option.

Follow these steps:

1. Click **Home**, **Requests**.

2. Perform the action that applies:

   - If the request is already submitted, click My Request, Open Requests, find the request, and open it.

   - If the request is not yet submitted and includes a service that uses a shopping cart click, Click Cart (if necessary) to display the request in the cart. Next, click Checkout.

- If the request is not yet submitted and includes a service that uses one-click submit, go to the next step. You select such services from the catalog and submit them using the same single page. So, you add notes while completing the fields on this page.

3. Add notes or an attachment to a service option, as follows:

   a. Click Show Details in the My Selections box.
   This box appears near the top left portion of the screen.

   b. Find the service option and click the Add Note icon or the Add Attachment in the Action column.

   c. Enter the text of the note or browse to select a file and attach. Click OK. For an attachment, verify the Display Name and also provide a Description.

4. Add notes or an attachment to the entire request, as follows:

   a. Verify that the service contains only one service option. If the service contains multiple service options, you cannot add notes to the entire request.

   b. Scroll down to the Notes box or the Attachments box on the right side of the page. The Notes box appears under the Request Information box and above the Attachments box.

   c. Click Add or browse to select a file and attach.

   d. Enter the text of the note and click OK. For an attachment, verify the Display Name and also provide a Description.

   Note: Use any of the rich text options available on the Add Note dialog to enhance the appearance of your note. You cannot delete or alter a note after you click OK. To delete an attached file, locate the file in the Attachments box, scroll right, and click the Delete icon. To update the display name or description of an attached file, click the Edit icon.

   You have added notes and/or attachment.

   Note: CA Service Catalog sends an email notification to end users and approvers when a note and/or attachment is added or edited for a request or an issue. CA Service Catalog also provides you the option of configuring the Request Details Link for E-Mail Notification. This capability is available only if you have installed the CA Service Catalog 14.1.01 patch updates from CA Support.

   For more information on Request Details Link for E-Mail Notifications parameter, refer to Request Management Configuration parameters (https://wiki.ca.com/display/CASM/.Other+Parameters+v14.1).

Manage Requests Pending Action

When a user submits a request, it enters the approval and subsequent fulfillment phase. Your service provider determines the business processes for approval and fulfillment of the services, and service options in the catalog. During approval and fulfillment, usually a person is assigned an approval or fulfillment task.

You can receive an email notification if a request approval or fulfillment task is assigned to you or to a group of which you are a member. You can view the requests which have an approval or fulfillment task that you are assigned. To do so, view your Pending Action list. Click the **Pending My Action** link in the **Request Lookup** section of the Requests window.

The Requests Pending Action list displays the list of requests which have an approval or fulfillment task that you are assigned. You can optionally filter this list of assignments by user name, group name, or all.

Request administrators can *search* for all requests, including requests that are assigned to other users. Request administrators have one of the following roles: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Catalog Administrator, and Request Manager. If the requests are already assigned to a user for approval or fulfillment, administrators can either complete these requests or they can transfer them to other users.

Rules for Requests Pending Action

Here, the term *request pending action* refers to one or more services or service options in a request that are pending approval or pending fulfillment. In both single-service and multi-service requests, all services are part of the request, but the term request pending action applies only to the services or service options that are pending approval or pending fulfillment. Specifically, pending *approval* status applies to *services* only, while pending *fulfillment* status applies to *service options* only.

- Both CA Service Catalog administrators and non-administrator users can transfer or delegate requests pending action in their own queues to other users. When you either transfer or delegate a request pending action, the user who receives the request becomes the new assignee. The major difference between transferring and delegating follows: When you delegate a request, it stays in both your queue and the queue of the new assignee. When you transfer a request, it leaves your queue and moves to the queue of the new assignee.

- Thus, as an administrator, you can decide to delegate a request pending action if you want to monitor it within your own queue. Conversely, you can decide to transfer a request pending action if you do not want to monitor it. After you delegate a request, the new assignee (User B) or an administrator can transfer the request to someone else (User C). When User B or another transfers the request, the request moves from both your queue and User B's queue to User C's queue only.

- Only requests pending action that is assigned to a user can be delegated. When a request pending action is assigned to a user and a group, only the one that is assigned to a user can be delegated. The one assigned to a group cannot be delegated.

- A request pending action can be delegated only once. This limitation includes auto-delegation; a request that has already been delegated manually cannot be auto-delegated. Therefore, before you delegate a task to a user, ensure that the user does not have auto-delegation enabled. However, the request can be transferred multiple times. You can delegate requests to an individual user only, not to a group.

- A request pending action is transferred or completed by the primary assignee of a pending action, by administrators, and by a user with the required access control settings. A request pending action can be transferred to only one user or one group.

- Both administrators and non-administrative users can also take ownership of a request pending action that is assigned to a group queue to which they belong. Users can return to the group queue a request pending action that they have previously taken but have not completed.

- A request pending action can only be returned by the primary owner of a taken pending action. The administrator (or any other user) cannot return a request pending action on another user's behalf.

To manage requests pending action, follow this process:

1. Act on requests pending action that can be assigned to you or other request managers, as follows:
   - Approve or reject (see page 2207)
   - Fulfill (see page 2210)
   - Transfer (see page 2212)
   - Delegate or auto-delegate (see page 2214)
2. Act on requests pending action that can be assigned to you, other request managers, or a group queue:
   - Take or return (see page 2217)
   - Ignore, retry, or override alerts (see page 2218)
   - Hold or resume (see page 2219)
   - Cancel (see page 2221)

Typically, the Status drop-down list includes several options. The names of these options and the order in which they appear are specified in the requestshared.xml file. For more information about how to update the values and the order of the options, see the Modify the Request Status List (see page 2006) section.

Note: Warning messages can appear if a user with the Services Manager role handles a requests pending action, for example, by approving and rejecting requests. In such cases, the approvals and rejections proceed successfully even though the warning messages appear.

To prevent such warning messages from appearing, follow these steps:

1. Log in to CA Service Catalog as a Service Delivery administrator or business unit administrator.
2. Change the default access rights of the Services Manager role for a specific business unit, as follows:
    a. Log in to the business unit.
    b. Select **Catalog**, **Configuration**, **Request Management Configuration**.
    c. Add the **Access Control: Add Request** setting to this role.
    d. Save your changes.

Approve or Reject Requests Pending Action

Request managers approve and reject the requests pending action that is assigned to themselves or other request managers. Approving or rejecting requests pending action is an essential step in the process of managing requests from creation through fulfillment.

All CA Service Catalog users can approve or reject requests pending action that is assigned to them.

Follow these steps:

1. Click Home, Requests. If applicable, click the My Requests drop-down list on the Requests page to display requests. The Requests page can either display requests directly or provide access to them indirectly through the My Requests drop-down list. Administrators optionally configure the page to use either setup.
2. Click Pending My Action.
3. Locate the request and click the Approve/Reject icon in the Actions column.
4. View the details of requested services, including their statuses.
5. Focus on the services for which you are assigned an approval task.

    Decide which items in the request to approve or reject.
6. If you have *not* implemented multi-item approval (see page 2116), perform this step only.
7. In the Item Status drop-down list, select the appropriate status to approve or reject each service, and click OK. The statuses are typically named Approved and Rejected, respectively.

- If you have *not* implemented discrete approval (see page 2120), the following rules apply:
  - Rejecting a service rejects the entire request. The request is returned to the user who submitted it. That user decides whether to update the request and resubmit it or accept the rejection as final.
  - Once all services in the request are approved, the request moves the request to the next phase of the request life cycle. For example, the second level of approval (if applicable) or the fulfillment stage. After you have approved a service, the approval processes of your service provider can require a second level of approval. In such a scenario, the second-level approver is assigned an approval task.
- You can optionally implement discrete approval so that you can approve or reject the following *individually*:
  - Services in a request
  - Service options in a service

If the approval task was assigned to more than one user or a group, once any assigned user completes that pending action, the request is removed from the Pending Action list for all assigned users. If the request contains multiple services, it is not removed until either all services are approved or one service is rejected.
You are returned to the Request Details window. If you return to the Pending Action list, you can see that the request is removed from your list.

8. If you have implemented multi-item approval perform this step only.
9. Perform one or both of the following actions:

- Select all or multiple services in the request and click Approve or Reject.
  This option appears when multi-item approval is implemented but discrete approval is *not* implemented.
- Select all or multiple service options in each service and click Approve or Reject.
  This option appears when both multi-item approval and discrete approval are implemented.

Approve or Reject the Requests Pending Action of Other Users

Only CA Service Catalog administrators and other users with the required access control setting can approve or reject requests pending action that is assigned to other users. The access control setting *Access Control: Proxy Action* under Catalog, Configuration, Options, Request Management Configuration determines the such roles.

Note: For more information, see the section Set CA Service Catalog Configuration Options (see page 1449).

Follow these steps:

1. Click Home, Requests. If applicable, click the My Requests drop-down list on the Requests page. The Requests page can either display requests and the search box directly or provide access to them indirectly through the My Requests drop-down list. Administrators optionally configure the page to use either setup.

2. Search for requests, using the Advanced Search.

3. In the Query drop-down list, perform the following actions:

    a. Ensure that Action Request is selected.

    b. (Optional) Enter the user ID of interest, in the Userid field.

    c. Click Search.

4. Click the Approve/Reject icon next to the name of the service of interest, in the Actions column.

    Note: The Item Status drop-down list is disabled. You enable it and use it in the next steps.

5. Click the Override (Push-Through) icon in the Actions column.

6. Confirm that you want to override a pending action that is not assigned to you.
   The Item Status drop-down list is enabled, meaning that you can now approve or reject each service in the request.

7. (If the request contains multiple services) Click the alert status icon. Enable the Item Status drop-down list for each service that you want to approve or reject.
   The status of each service option matches the status of the service during the approval phase of the request life cycle.

8. Decide which items in the request to approve or reject.

9. If you have *not* implemented multi-item approval (see page 2116), perform this step only.
   In the Item Status drop-down list, select the appropriate status to approve or reject each service, and click OK. The statuses are typically named Approved and Rejected, respectively.

    - If you have *not* implemented discrete approval (see page 2120), the following rules apply:

        - Rejecting a service rejects the entire request. The request is returned to the user who submitted it. That user decides whether to update the request and resubmit it or accept the rejection as final.

        - Once all services in the request are approved, the request moves the request to the next phase of the request life cycle. For example, the second level of approval (if applicable) or the fulfillment stage. After you have approved a service, the approval processes of your service provider can require a second level of approval. In such a scenario, the second-level approver is assigned an approval task.

- You can optionally implement discrete approval so that you can approve or reject the following *individually*:
  - Services in a request
  - Service options in a service

  If the approval task was assigned to more than one user or a group, once any assigned user completes that pending action, the request is removed from the Pending Action list for all assigned users. If the request contains multiple services, it is not removed until either all services are approved or one service is rejected.

10. If you have implemented multi-item approval perform this step only.
    Perform one or both of the following actions:
    - Select all or multiple services in the request and click Approve or Reject.
      This option appears when multi-item approval is implemented but discrete approval is *not* implemented.
    - Select all or multiple service options in each service and click Approve or Reject.
      This option appears when both multi-item approval and discrete approval are implemented.

Fulfill Requests Pending Action

Request managers fulfill the approved requests pending actions that are assigned to themselves or other request managers. Fulfilling requests pending action is the final step in the process of managing requests from creation through fulfillment.

All CA Service Catalog users can fulfill requests pending action that is assigned to them.

Follow these steps:

1. Click Home, Requests. If applicable, click the My Requests drop-down list on the Requests page. The Requests page can either display requests directly or provide access to them indirectly through the My Requests drop-down list. Administrators optionally configure the page to use either setup.
2. Click Pending My Action.
3. Locate the request and click the Fulfill icon in the Actions column.
4. View the details of requested services. Focus on the services for which you are assigned a fulfillment task.
   The status of each service option matches the status of the service during the fulfillment phase.
5. Decide and select the next status for each service for which you are assigned a fulfillment task. The exact statuses available can vary, based on the business processes of your service provider. Two significant statuses are Fulfilled and Fulfillment Cancelled, both of which end the fulfillment process for that service option.

- If you are using CA APM and the service is eligible for asset assignment, select the available inventory of assets. Assign assets or indicate that no assets are available for assignment. Using the assign assets functionality changes the status of the related service option.

- If you are *not* using CA APM or the service is *not* eligible for asset assignment, in the Item Status drop-down list, select the appropriate status for each service.

6. Optionally add notes or attachments as supporting documents.

7. When you are finished, click OK.
   You are returned to the Request Details window. If all pending action assigned to you have been completed, the request is removed from your list. If the fulfillment task was assigned to more than one user or a group, once any assigned user completes that pending action, the request is removed from the Pending Action list for all assigned users. If the request contains multiple services, it is not removed until either all services are either fulfilled or have their fulfillment that is cancelled.

Note: The fulfillment processes of your service provider can require more fulfillment steps. In such cases, the next fulfiller is assigned a fulfillment task.

Fulfill the Requests Pending Action of Other Users

Only CA Service Catalog administrators and other users with the required access control setting can fulfill requests pending action that is assigned to other users. The access control setting *Access Control: Proxy Action* determines such roles. This setting is under Catalog, Configuration, Options, Request Management Configuration.

Follow these steps:

1. Click Home, Requests. If applicable, click the My Requests drop-down list on the Requests page. The Requests page can either display requests and the search box directly or provide access to them indirectly through the My Requests drop-down list. Administrators optionally configure the page to use either setup.

2. Search for requests, using the Advanced Search.

3. In the Query drop-down list, perform the following actions:

   a. Ensure that Action Request is selected.

   b. (Optional) Enter the user ID of interest in the Userid field

   c. Click Search.

4. Click the name of the request of interest to open it.

5. View the details of requested services. Focus on the services whose fulfillment status you want to update.
   The status of each service option matches the status of the service during the fulfillment phase.

6. Click the alert status icon in the Actions column.

7. Confirm that you want to override a pending action that is not assigned to you, when prompted.
   The Item Status drop-down list is enabled, meaning that you can now update the fulfillment status of the service.

8. Click the alert status icon. Enable the Item Status drop-down list for each service whose fulfillment status you want to update, if the request contains multiple service. The status of each service option matches the status of the service during the fulfillment phase.

9. Decide and select the next status for each service whose fulfillment status you want to update. The exact statuses available can vary, based on the business processes of your service provider. Two significant statuses are Fulfilled and Fulfillment Cancelled, both of which end the fulfillment process for that service option.

   - If you are using CA APM and the service is eligible for asset assignment, select the available inventory of assets. Assign assets or indicate that no assets are available for assignment. Using the assign assets functionality changes the status of the related service option.

   - If you are *not* using CA APM or the service is *not* eligible for asset assignment, in the Item Status drop-down list, select the appropriate status for each relevant service.

10. Optionally add notes or attachments as supporting documents, and click OK.
    You are returned to the Request Details window. If you return to the Pending Action list after all pending action assigned to you have been completed, the request is removed from your list. If the fulfillment task was assigned to more than one user or a group, once any assigned user completes that pending action, the request is removed from the Pending Action list for all assigned users. If the request contains multiple services, it is not removed until either all services are either fulfilled or have their fulfillment cancelled.

Note: The fulfillment processes of your service provider can require more fulfillment steps. In such cases, the next fulfiller is assigned a fulfillment task.

Transfer Requests Pending Action

Request managers can transfer the requests pending actions that are assigned to themselves or other request managers. You can transfer a request pending action that is assigned to you or another user. For example, when you or other user become sick or otherwise are unavailable to perform or approve an assigned task.

All users can transfer their own requests pending action.

Follow these steps:

1. Click Home, Requests.

2. Click Pending My Action.
   To open the request of interest, click the request name.
   The Requests Details window appears, displaying the details of the request you just opened. The details for the selected request appear, with a Requested Services section at the top of the screen. That section lists all services in the request. If the request contains multiple services, you can transfer them either individually or in groups of two or more.

   Note: A service can be transferred if you can select it. If you cannot select the service, it cannot be transferred. For example, a multiservice request can contain one or more services that are not pending approval or fulfillment and therefore cannot be transferred.

3. Select the service or services and click Transfer.
   The Search User window appears.

4. Review the list of users and select *one* user to whom the selected services are transferred.
   You return to the Requested Services section. In the Item Status column, the selected request or requests are marked for Transfer to *username. username* is the user to whom you transferred those requests.

5. Verify that the correct user is designated for the transfer and click OK.

Transfer the Request Pending Action of Other Users

Only CA Service Catalog administrators and other users with the required access control setting can transfer requests pending action that is assigned to other users. The access control setting *Access Control: Proxy Action* determines such roles. This setting is under Catalog, Configuration, Options, Request Management Configuration The *Access Control: Transfer Request Pending Action* setting determines the roles that have access to the Transfer button. This button is hidden from other roles.

Follow these steps:

1. Click Home, Requests. If applicable, click the My Requests drop-down list on the Requests page. The Requests page can either display requests and the search box directly or provide access to them indirectly through the My Requests drop-down list. Administrators optionally configure the page to use either setup.
   Search for requests, using the Advanced Search.

2. In the Query drop-down list, perform the following actions:

   a. Ensure that Action Request is selected.

   b. (Optional) Enter the user ID of interest, in the Userid field.

   c. Click Search.

3. To open the request, click the request name.
   The Requests Details window appears. The Requested Services section lists all services in the request. If the request contains multiple services, you can transfer them either individually or in groups of two or more.

   Note: A service can be transferred if you can select it. If you cannot select the service, it cannot be transferred. For example, a multiservice request can contain one or more services that are not pending approval or fulfillment and therefore cannot be transferred.

4. Click the Transfer button at the top of the window.

   Note: The Item Status drop-down list is disabled. You enable it and use it in the next steps.

5. Click the alert status icon in the Actions column.

6. Confirm that you want to override a pending action not assigned to you, when prompted.

7. If the request contains multiple services, click the alert status icon and enable the Item Status drop-down list for each service that you want to approve or reject.
   The status of each service option matches the status of the service during the approval phase.

8. Select the service and click Transfer.
   The Search User window appears.

9. Review the list of users and select *one* user to whom the selected services are transferred.
   You return to the Requested Services section. In the Item Status column, the selected request or requests are marked for Transfer to *username. username* is the user to whom you transferred those requests.

10. Verify that the correct user is designated for the transfer and click OK.

Delegate or Auto-Delegate Request Pending Action

Request managers can *delegate* their requests pending action. Request managers can *auto-delegate* requests pending actions that are assigned to themselves or other request managers. For example, when you or others are unavailable to perform or approve an assigned task. Auto-delegation is useful for managers who monitor requests but who do not address requests directly. Thus, auto-delegation helps ensure that requests are addressed in a timely manner. A request pending action can be delegated only once.

Only the owner of the request pending action can delegate, if the owner has the required access control setting. The access control setting named **Access Control: Delegate Request Pending Action**. This setting is under Catalog, Configuration, Options, Request Management Configuration.

Follow these steps:

1. Click Home, Requests. If applicable, click the My Requests drop-down list on the Requests page to display requests. The Requests page can either display requests directly or provide access to them indirectly through the My Requests drop-down list. Administrators optionally configure the page to use either setup.

2. Perform *one* of the following actions:

   - Click **Pending** in **My Request(s)**.
     Click the **Delegate** button for the request pending approval or fulfillment.

   - Click **Find Requests** in **My Request(s)**.

     a. Search in the Request Lookup section.

     b. Verify that **Action By User ID** is selected.

     c. Enter your user ID in the search field and click **Search**.
     The Search Results window appears, displaying all requests that are assigned to you.

     d. Click the **Delegate** button for a request pending approval or fulfillment.

   The details for the selected request appear, with a Requested Services section at the top of the screen. That section lists all services and service options in the request. If the request contains multiple services and service options, they can be delegated either individually or in groups.

   Note: A service can be delegated if you can select it. If you cannot select the service, it cannot be delegated. For example, a multi-service request can contain one or more services or service options that are not pending approval or fulfillment. Such a request cannot be delegated.

3. Select the service or service options and click **Delegate**.
   The Search User Accounts window appears.

   Note: The Search User scope is based on the administration configuration of either all users or only users in the same business unit. For more information about setting this configuration, see the User Default (see page 1484)section.

4. Review the list of users and select *one* user to whom you delegate the selected services or service options.
   You return to the Requested Services section. In the Item Status column, the selected service or service options are marked for delegation to *username. username* is the user whom you selected.

5. Verify that the correct user is named for the delegation and click OK.

Use auto-delegation and specify all of your newly assigned or transferred requests pending action are automatically delegated to another user.

Note: The access control setting **Access Control: Allow Request Auto-Delegation via User Profile** determines whether users can view and change auto-delegation settings, according to their user roles. For more information, see the Administration Configuration Settings (see page 1477).

Follow these steps:

1. Move the cursor to the top right portion on the screen. Click the Profile button next to the Help button.
   The User Profile window appears; the fields are read-only.

2. Click the Edit button.

3. Click the down-arrow icon next to the Request Auto-Delegation heading.
   The Request Auto-Delegation setting for your user ID opens, so that you can view and optionally change it.

4. To remove an existing auto-delegation (if applicable), click the red "minus sign" icon.

5. To add or change auto-delegation, click the magnifying glass icon.
   The Search and Select User Search dialog appears.

6. Click the name of the user to designate for auto-delegation.
   The dialog closes, and you return to the Edit User Profile window. The user that you selected is named in the Delegate field.

7. Verify that the correct user is designated for auto-delegation and click OK. Click Done.

Auto-Delegate the Requests Pending Action of Other Users

Use auto-delegation and specify that any *new* requests assigned to a specific user are automatically delegated to a different user. Here, *new* request means any newly assigned or transferred pending action.

Follow these steps:

1. Click Administration, Users.

2. Enter search criteria in the User ID field to find the user whose requests you want to auto-delegate to another user.

3. Click the name of the user whose requests you want to auto-delegate, and click Edit.

4. Click the drop-down icon next to the Request Auto-Delegation heading.
   The user in the Delegate field is the one to whom requests are currently auto-delegated.

5. To remove an existing auto-delegation (if applicable), click the red "minus sign" icon.

6. To add or change auto-delegation, click the magnifying glass icon, and review the list of users.

7. Click the name of the user to designate for auto-delegation.

8. Verify that the correct user is designated for auto-delegation and click OK. Click Done.

Take or Return a Request Pending Action

From the Take/Return window, you can take or return ownership of requests pending action. You can take ownership from a group queue or the queue of another user in the same business unit or sub-business unit. Similarly, you can return ownership of requests pending action from your queue to the queue of your group. You can take or return ownership of requests pending action that is assigned to your group.

The Take and Return functions work *only* if you are logged in as a user of the group to which the request pending action is assigned. Only CA Service Catalog administrators and other users with the required access control setting can do so. The access control option *Access Control: Take/Return Request Pending Action* under Catalog, Configuration, Options, Request Management Configuration determines such roles. For more information about setting this option, see the Request Management Configuration (see page 1450) section.

Follow these steps:

1. Click Home, Requests. If applicable, click the My Requests drop-down list on the Requests page to display requests. The Requests page can either display requests directly or provide access to them indirectly through the My Requests drop-down list. Administrators optionally configure the page to use either setup.

2. Click Pending My Action.

3. Click the Take/Return button for a request pending approval or fulfillment.
   The Take/Return window shows the details for the selected request, including a Requested Services section. That section lists all services and service options in the request. If the request contains multiple services or service options, they can be taken or returned individually or in groups.

   Note: A service or service option can be taken or returned if you can select it. If you cannot select the service or service option, it cannot be taken or returned. For example, a multi-service request can contain one or more services or service options that are not pending approval or fulfillment. Therefore, the service or service option cannot be taken or returned.

4. (To *take* one or more services from a request pending action) Select the services or service options. Click Take.
   The request is marked and your user ID can take it.
   If a request is already taken, the status indicating “taken by *username*” appears. Therefore, you cannot take it. Other users in the same group can still approve or fulfill a taken service, if

necessary. Either the user who has taken the service must return it or an authorized user must transfer it to the new assigned user. If a request is not taken but the Take option is not available, then the action is not assigned to your group.

5. (To *return* one or more service or service options from a request pending action) Select the services or service options. Click Return.
   The only services that you can return are services already marked as taken by your user ID.

6. Click OK to perform the take or return action.
   Your action is confirmed: Any requests that you have taken are marked as taken by your user ID. Similarly, any requests that you have returned are no longer marked as taken.

Ignore, Retry, or Override Alerts

During the submitted state or the approval process, requests can occasionally become marked with an alert status indicating a potential problem. For example, because of a system error or a user error. The alert is indicated in the Status column of several request windows. If the role of a user does not permit access to this option, then that user cannot see the status, even if the user's request is stuck. We recommend that you ignore, retry, or override (push through) alerts as soon as you become aware of them. Only CA Service Catalog administrators and other users with the required access control setting can ignore, retry, or override alerts.

The access control option *Access Control: Push Through Request* determines such roles. This setting is under Catalog, Configuration, Options, Request Management Configuration. The access control option named *Access Control: Display Request Warning* determines which roles are able to see the warning icon indicating that a request is stuck. For more information about setting this option, see the Request Management Configuration (see page 1450) section.

Follow these steps:

1. Click Home, Requests. If applicable, click the My Requests drop-down list on the Requests page to display requests. The Requests page can either display requests directly or provide access to them indirectly through the My Requests drop-down list. Administrators optionally configure the page to use either setup.

2. Find the "alert" request on any of the following windows: Open Requests, Completed Requests, Pending My Action, Request Search, or Recent Requests Lists.
   The request can be marked with an alert status, because of one or more information-only alerts that are logged during the request flow. In this case, ignore the alerts, as follows:

   a. Open the window that includes the alert request.

   b. In the Action column, click the Actions drop-down and select Push Through from the list.
      The Push Through Request window appears, and the Push Through Request tab is selected by default.

      The details for the selected request appear, with a Requested Services section at the top of the screen. That section lists all services in the request. If the request contains multiple services, they can be pushed through. You can push them either individually or in groups of two or more at a time.

c. In the Override Status column, select the status for the request to acquire from the drop-down list.

d. Click Save.

3. For each stuck service, click the Item Status drop-down list. Select the Approval or Fulfillment status that best meets your needs.
   The options for any service vary, according to its status. To view all available options, use the drop-down list.

4. Click OK.
   Each service whose status you changed has its alerts that are removed (overridden). The service is "pushed through" to the selected status.

   Note: If a request is in queued status before being pushed through, it carries its (queued) prefix state along with new status of the request. Push Through can be performed for both queued and nonqueued requests.

   The alerts are made inactive, and the status is removed.
   When the status of a requested service is either Pending or Completed, you can either ignore or push through the alert.

Hold and Resume Requests, Services, or Service Options

Holding requests, services, or service options ensures to anyone monitoring a request that the processing of the request, service, or service option has been *intentionally* suspended. Only CA Service Catalog administrators and other users with the required access control setting can hold and resume requests.

The access control setting *Access Control: Hold/Resume Request* determines such roles. This setting is under Catalog, Configuration, Options, Request Management Configuration. For more information about setting this option, see the Request Management Configuration (see page 1450) section.

How Hold and Resume Actions Work

Reasons for holding a request include:

- The temporary unavailability of the requestor or approver.
- The temporary unavailability of requested items, such as the items being in back-ordered status.

When a service option is held, the monitoring of time stops for any request SLAs attached to the service option. The request SLAs are stopped to prevent related SLA warnings and SLA violations from being issued.

When an item is held, no status changes can occur for it until you *resume* it. That is, you change its status to Resume. When you resume an item, it returns to its last previous status before it was held.

If you hold only selected services within a request or only selected service options within a service, the services or services options that you did not hold continue the normal request life cycle, except that they cannot reach Completed status until the held items are resumed and are also completed.

When resumed, service options that were formerly held, move to a temporary Resume status. The service options then automatically move back to the status they were at before they put on Hold. Checking Resume status is useful for history purposes. Doing so helps you set up optional rules and actions, automated processing using CA Process Automation, or automatic email notifications.

Automatic Email Notifications

You can use the events, rules, and actions (see page 3040) for sending automatic email notifications when a request, service, or service option is held or resumed.

The events *Request Change* and *Request/Subscription Item Change* include two rules that are related to hold-resume functions:

- When Status is Hold
- When Status is Resumed

For the *Request Change* event, the *When Status is Hold* rule includes an action that sends an automatic email notification when a request is held. Similarly, the *When Status is Resumed* rule includes an action that sends an automatic email notification when a request is resumed.

For the *Request/Subscription Item Change* event, the *When Status is Hold* rule includes an action that sends an automatic email notification when a service option is held. Similarly, the *When* Status is Resumed rule sends includes an action that sends an automatic email notification when a service option is resumed.

Hold and Resume Requests, Services, or Service Options

Follow these steps:

1. Click Home, Requests. If applicable, click the My Requests drop-down list on the Requests page to display requests. The Requests page can either display requests directly or provide access to them indirectly through the My Requests drop-down list. Administrators optionally configure the page to use either setup.

2. Click Pending My Action or Open Requests. Alternatively, click Advanced Search for requests.
   The Requests Pending Action window appears, or the Open Requests window appears.
   Click the Hold/Resume icon for the request you want.
   The Hold/Resume window appears including a Requested Services section. That section lists all services and service options in the request. If the request contains multiple services or service options, you can hold or resume them either individually or in groups.

3. To *hold* one or more services or service options, select the services or service options and click Hold.
   Each service option that you selected is marked *to be held* by your user ID.
   If a request is already held, the status indicating “held by *username*” appears next to the Item Status field of the request item. Therefore, you cannot hold it again. The *username* identifies the user who has held the request.

4. To *hold* an entire request, select the All check box for the request and click Hold.
   All service options in the request are marked *to be held* by your user ID.

5. Add a note to the request for the services or service options that you held explaining why you held them. Provide any information that helps other administrators determine when to resume a service or service option.

Verify that all reasons have been addressed before resuming the request.

- To *resume* one or more services or service options, select the services or service options and click Resume.

  Note: When you resume a previously held service or service option, the monitoring of time is resumed for any request SLA attached to the service or service option.

  The only services that you can resume are those services already marked as held.

- Click Save to perform the hold or resume action.

Cancel a Request

Administrators can cancel a request for several possible reasons. For example, the wrong items were requested or the requested items are no longer wanted or needed.

Only CA Service Catalog administrators and other users with the required access control setting can see the Cancel button. The access control setting *Access Control: Cancel Request* determines such roles. The setting is under Catalog, Configuration, Options, Request Management Configuration. For more information, see the Set CA Service Catalog Configuration Options (see page 1449) section.

You can cancel a request *only* if the status of the request has not exceeded the status that *Allow Cancellation Through* specifies. This setting is in the Catalog, Configuration, Options, Request Management Configuration. This setting defines the status through which a request can be canceled. After the request moves to the next status, it cannot be canceled.

Note: By default, for the event *Request/Subscription Item Change*, for the rule *When Status is Canceled*, an action is enabled. The action aborts CA Process Automation instances when a request is canceled. For best performance, keep this default setting. For more information about setting this option, see the Set CA Service Catalog Configuration Options (see page 1449) section.

Follow these steps:

1. Click Home, Requests. If applicable, click the My Requests drop-down list on the Requests page to display requests. The Requests page can either display requests directly or provide access to them indirectly through the My Requests drop-down list. Administrators optionally configure the page to use either setup.

2. Click the list of requests that contains the request that you want to cancel. For example, if you want to cancel a request pending action, click Pending My Action.

3. Click the request that you want, and click Cancel.

> **Note:** If the requirements for cancellation are not met, the Cancel button is disabled. The request cannot be canceled. Moreover, items in the same request can be at different statuses. Some items may have exceeded the *Allow Cancellation Through* status while others have not yet done so. In such cases, you can cancel *only* the items that have *not* exceeded the *Allow Cancellation Through* status.

4. Confirm the cancellation and click OK.

Delegate Catalog

This article contains the following topics:

Delegating the use of your catalog to another user (a delegate) lets the delegate browse your catalog. The delegate can also create and submit requests on behalf of you (the delegator). Administrators assign this right to individual roles by setting the configuration option named *Access Control: Add Request* in the Request Management Configuration section of the Administration Configuration page. For more information about this parameter, see the Access Control Parameters (see page 1450) section.

The catalog of a delegator typically contains services that are not available in the catalog of the delegate.

Delegators are typically executives or managers but can be any user whose role permits creating and submitting requests. Delegates are typically employees who report to the delegator. But the delegates can also be any user whose role permits creating and submitting requests.

> Typically, a delegate creates and submits requests for the delegator from the catalog of the delegator. In such a scenario, the *Requested For field* shows the name of the delegator. The field cannot be changed.

History, auditing, and logging records for a request show that the delegate created and submitted the request on behalf of the delegator.

Comparison to Related Features

Delegation of catalogs is related to, but not the same as, the following features:

- Requesting a service for another user, using your own catalog. Specify the name of the other user in the *Requested For* field when you view and change more information in the request before submitting it.
- Delegating a request (see page 2214). You manually delegate a request pending action, from either yourself or another request manager, to a different request manager. The delegated request manager can then approve, reject, or transfer the request.
- Auto-delegating your own requests pending action or auto-delegating requests pending action of other users. The auto-delegated request manager can then approve, reject, or transfer the request.

In contrast to these features, delegating the use of your catalog lets another user browse your catalog. The other user can create, edit, and submit requests on your behalf.

Limitations of Catalog Delegation

The following limitations apply when you delegate the use of your catalog to another user:

- Delegates must create and submit requests themselves from the catalog of the delegator catalog.
- Delegates *cannot* change the Requested For field to request services for any user other than the delegator.
- Users who have a role that cannot create a request (such as Service Manager) *can* delegate their catalogs. However, delegates of such users *cannot* browse or create requests from the catalogs of those delegators. Therefore, as a best practice, users whose roles prohibit them from creating requests do *not* delegate their catalogs.
- All users can delegate the use of *their own catalog* to another user. If you have the Super Business Unit Administrator or Service Delivery Administrator role, you can delegate the use of either *your own catalog* or *the catalog of any other user ID* to another user. If an administrator delegates the use of your catalog to another user, the Catalog system does not automatically notify you or the other user. However, in such cases, the delegate does appear in the list of delegates on your User Profile page. You can manually remove that delegate. As a best practice, administrators who perform such actions notify affected users personally.

Important! The delegate must have a role in the business unit of the delegator. Otherwise, the catalog of the delegator is not made available to the delegate.

Considerations for Business Units

You can delegate your catalog to a user in your own business unit or any other business unit. For example, the top-level (service provider) business unit.

If you delegate your catalog to a user in the same business unit, the delegate can use your catalog immediately. When the delegate logs in to CA Service Catalog, the delegate can see and select your name in the *Use Catalog Of* field of the Requests home page. (This page appears when you select Home, Requests). Then, the delegate can browse and use your catalog.

When you delegate your catalog to a user in another business unit, you must have a role in that business unit. Otherwise, the delegate cannot see and select your name in the *Use Catalog Of* field of the Requests home page and cannot use your catalog. If necessary, you or an administrator can edit your user profile to add a role for your user ID in that business unit.

For example, suppose that your organization is grouped into business units according to department. If you work in the Finance department, and you delegate use of your catalog to a user in the Human Resources department (a different business unit). Verify that you have a role in Human Resources.

Sample Scenarios

The following scenarios illustrate possible instances of delegating the use of a catalog--either your own catalog or another catalog.

- **Scenario 1**
  A CIO delegates her catalog to her executive assistant, with instructions to create and submit requests for ten items on her behalf.
  The items are not available in the assistant's catalog, so the CIO delegates use of her catalog to the assistant. The assistant uses the CIO's catalog as a delegate and requests the ten items for the CIO.
  History, auditing, and logging records for the requests show that the assistant created and submitted the requests on behalf of the CIO.

- **Scenario 2**
  An administrator (User A) delegates the use of the catalog of another user (User B) to a different user (User C). Doing so requires the Super Business Unit Administrator or Service Delivery Administrator role.
  In this scenario, the CIO requires the ten items that are requested not for herself but for a vice president who reports to her. That vice president is on leave without access to CA Service Catalog but needs the items when returning to work next week.
  In this scenario, the CIO delegates the use of the vice president's catalog (not her own catalog) to her assistant. Before the vice president returns to work, the assistant uses the vice president's catalog as a delegate and requests the ten items for the vice president.
  Scenario 3
  The CIO begins to create a request for herself but must stop and save the request to address an emergency issue. When she realizes that the issue requires long, uninterrupted effort, she stops the effort. She cancels the request, and instructs her assistant to create and submit the request as a delegate.
  History, auditing, and logging records for the request show that the delegator created the request, but the assistant edited and submitted the request on behalf of the delegator.

Administrators configure CA Service Catalog to let users (*delegators*) delegate their catalog to other users (*delegates*). Delegates work on behalf of delegators who are unable or unavailable to create and submit their own requests. The catalog of a delegator typically contains services that are not available in the catalog of a delegate.

1. Administrators configure CA Service Catalog to enable the delegation of catalogs (see page 222).

2. Delegators edit their profile to delegate the use of their catalogs (see page 2226) to one or more delegates.
   The delegates use the catalog of a delegator (see page 2227) to create, edit, and submit requests.
   If necessary, delegates, delegators, and administrators work together to manage unsubmitted requests that delegates (see page 2228) create.

Step 1 - Enable or Disable Delegation of Catalogs

Users with the Super Business Unit Administrator or Service Delivery Administrator role can enable or disable delegation of catalogs within the business unit--and any subbusiness units--to which their role applies. Users with other roles can optionally delegate the use of their catalogs to any other user. Delegation of catalogs is enabled by default, but enable it explicitly if it was disabled earlier.

Follow these steps:

1. Click Catalog, Configuration, Request Management Configuration.

2. Locate the option *Enable Delegation of Catalog*. Set this option to Yes to enable the feature or No to disable it.

   - If this option is set to No, enable it. To enable it, click the Edit icon, select the check box, and click Update Configuration.

   - If this option is set to Yes, disable it. To disable it, click the Edit icon, clear the check box, and click Update Configuration.

When this option is enabled, no users are *required to* delegate use of their catalogs. When this option is enabled, users can *optionally* delegate use of their catalogs.

Note: Delegating a catalog does *not* affect the Catalog configuration of the CA Service Catalog, such as the *Use Service Provider Catalog Only* and *Pass Through Catalog* parameters. Similarly, the delegation of a catalog is *not* directly related to the configuration options named *Access Control: Add Request*, *Access Control: Edit Request that also exists* in the same Request Management Configuration section as Enable Delegation of Catalog.

Step 2 - Delegate the Use of a Catalog

When you delegate the use of your catalog to other users, they can browse your catalog. They can also create and submit requests on your behalf. Typically, you delegate the use of your catalog to other users when you are unavailable to perform this work yourself but the work must continue with minimal supervision. As a prerequisite, review the limitations of delegation of catalogs.

Follow these steps:

1. Verify with your Super Business Unit Administrator or Service Delivery Administrator that this feature is enabled.
2. Click Home, Administration, Users.
3. Click the Search button on the Users search dialog.
   The user IDs that you can update appear.
4. Click the Edit icon for the user ID you want to edit.
5. Click the Open icon for the Delegate Use of Catalog box.
6. Click the Search icon next to the Delegates field.
7. Click the user ID to which you want to delegate use of your catalog.
8. Click the Add icon.
   The user ID you selected is moved from the Delegates field to the list of delegates underneath it. The user ID is added to your list of delegates.

   Important! The delegate *must* have a role in the business unit of the delegator. Otherwise, the catalog of the delegator is *not* made available to the delegate.

   Also:

   - Delegates *cannot* edit and submit existing requests that the delegator creates.
   - A single user can be a delegate for multiple delegators.
   - Delegates can create and submit requests using the catalog of the delegator.
9. If applicable, add another delegate by clicking the Search icon and repeating the previous two steps.
10. When you are finished adding delegates, click OK.

If you delegated the use of your own catalog, all delegates you selected can browse your catalog. They also can create, edit, and submit requests on behalf of you. If you are a Super Business Unit Administrator or Service Delivery Administrator who delegated the use of the catalog of another user, the delegates you selected can browse the catalog. They also can create, edit, and submit requests on behalf of that user.

Step 3 - Use the Catalog of a Delegator

When another user specifies you as a delegate, you can use the catalog of the delegator instead of your own. The catalog of the delegator likely includes more services and service options than your own. You can access the catalog and can browse it. You can use the catalog to create, edit, and submit requests on behalf of the delegator.

Follow these steps:

1. Click Home, Requests.
2. Click the Use Catalog Of drop-down list.
   The list displays your delegators, the users for whom you are a delegate in your currently logged in business unit or one of its subbusiness units.
   If no users appear:
   - Contact users for whom you are a delegate. Verify that they have delegated the use of their catalogs (see page 2226) to you.
   - Verify the business unit in which the delegator has specified you as a delegate. Verify that you have a role in the business unit.
   - Verify that the delegation of catalogs (see page 2225) option is enabled.
3. Select the delegator.

You can now browse the catalog of the delegator and create, edit, and submit requests on behalf of the delegator. History, auditing, and logging records show that the delegate created, edited, and submitted the request on behalf of the delegator.

Remove a Delegate

When you remove a user from your list of delegates, the user can no longer browse your catalog. The user also cannot create and submit requests on your behalf. Remove a user from your list of delegates when appropriate for business reasons. For example: the delegate leaves the organization, or you transfer to another department, or you no longer need the user as a delegate. Typically, you remove delegates from using your catalog. If you are a Super Business Unit Administrator or Service Delivery Administrator, you can remove delegates from using the catalog of another user.

Follow these steps:

1. Click Home, Administration, Users.
2. Click the Search button on the Users search dialog.

3. Click the Edit icon for the user ID you want to edit.
   To reveal the list of delegates for a user, select the Open icon for the Delegate Use of Catalog check box.

4. Select the user or users whom you want to remove as delegates.

5. Click the Delete icon.

6. Click OK.

Step 4 - Manage Unsubmitted Requests Created by Delegates

A delegate can create and save requests using a catalog of a delegator. The delegate can also submit the requests later, on behalf of the delegator. However, before the delegate submits the request, the following events can occur:

- The delegator (or an administrator) removes a delegate (see page 2227) from using the catalog of the delegator.
- An administrator disables the delegation of catalogs (see page 2225) in one or more business units or throughout the Catalog system.

In both cases, delegates are *not* notified automatically, and delegates are no longer able to submit the requests. The only exception is that delegates whose roles permit them to override alerts (see page 2218) can optionally "push through" the request to the next status and so, submit the request. Similarly, delegates can optionally delete such requests, because delegates own the requests.

Delegators can view requests that are made on their behalf (whether submitted or not) in the Open Requests queue. However, delegators *cannot* delete or submit such requests. The only exception is that delegators whose roles permit them to override alerts can optionally "push through" the request to the next status and so, submit the request.

Delegators and delegates decide together how to manage saved but requests not submitted, so that such requests do not remain open. Options are as follows:

- Delete the request. Only the delegate can delete the request.
- Push through the request. The delegate, delegator, or an administrator with the required role (upon request).
- Temporarily make the user as a delegate.
- Ask an administrator to re-enable the delegation of catalogs in your business unit long enough for the delegate to submit the request.

Change Management

Change Management for CA SDM is a set of features for Change Managers and Change Advisory Board (CAB) members to coordinate the review and approval of change requests for CI components and services. For example, Change Managers can review and approve all changes to CI components and services to ensure that no new security vulnerabilities are introduced into the production environment. The Change Manager leads the CAB and is responsible for the ultimate approval of change requests.

Change Management includes the following components:

- **Change Calendar:** Displays a graphical view of change events (see page 2292), including all scheduled, failed, and in-progress change requests for CIs and services in a configurable calendar view (see page 2267). The calendar also displays black-out dates, which are freeze periods. Users can create a change order from the context menu on the daily, weekly, and monthly calendar views. The Change Manager, Level 2 Analysts, and CAB members use this feature.

- **Change Scheduler:** Displays scheduled time periods (see page) during which CI changes can or cannot occur in the Change Calendar. The Change Manager uses this feature to view and create change schedules and CI associations during the time period.

- **Conflict Analysis and Collision Detection:** Analyze change orders to help identify potential implementation conflicts (see page 2245) that could increase risk of failure. The Change Manager uses this feature.

- **CAB Console and Reporting:** Displays a dashboard (see page) that facilitates quick online approvals of change orders that require CAB approval. In CA SDM, the Change Manager can generate a report with details about the proposed requests for changes ready for CAB review and electronically distribute the reports to all CAB members.

  Users with appropriate privileges can display Compliance, Forecast, Trend, and Volume predefined reports for change management in Business Intelligence Launch Pad with CA Business Intelligence.

- **Risk Assessment:** Provides the ability to attach risk assessments for each change request submitted. The Risk Survey Option lets you create surveys to evaluate risks, and associate them with change categories. The risk survey lists a series of single or multiple choice questions.

- **Impact Explorer:** Displays CI-to-CI relationships for CIs that are attached to a change order. Impact Explorer is launched from the Change Order Detail page to facilitate on-demand impact analysis (see page 2253). The Change Manager uses this feature.

- **Change Verification:** Verifies that changes execute accurately and no unauthorized changes occur, so that CMDB contains an accurate and current representation of all managed CIs.

Configuration Audit and Control Facility

This article contains the following topics:

Configuration Audit and Control Facility (CACF) combines Change Management, Configuration Management (CMDB), and Discovery Management to provide change verification. Change verification helps ensure that the CMDB reflects any changes accurately, and the Discovery Management tools verify the changes.

Select the Configuration Management tab to define change specifications, CIs, and view the Verification log.

You administer the CACF components in the Configuration Control node in the CMDB section of the Administration tab and define and view CACF change specifications from the Change Order, CI and Incident forms.

The CMDB Administrator defines the CIs and attributes to manage and defines the policy for updating those CIs and attributes.

The Administrator must consider allowing standard changes, defining authoritative and trusted sources of data, and defining which CIs and CI attributes are under CACF management. If an incorrectly executed change or rogue change occurs (also referred to as a variance), CA SDM can accept the new value, create an Incident, or copy the data to the TWA for later processing. CA SDM can also use any combination of these actions.

The Configuration and Change Administrators *must* define a change verification strategy for your environment. For more information, see Planning and Implementing Change Verification topic.

How to Define Policies for Change Verification

Complete the following recommended steps to begin using CACF in your CA SDM environment:

1. Review the Managed Change States in the CA SDM environment. Update the default Managed Change States or add states as necessary to suit your change management strategy. Change verification initiates when the status of a Change Order changes to a Change State that CACF manages, such as Verification in Progress.

2. Identify the available CI Managed Attributes that you want CACF to manage for change verification.

   - For example, you want to manage changes to Memory Installed (phys_mem) so that the attribute *must* have a matching Change Order for the test* server. You also consider changes to IP Address (alarm_id) as normal and always allowed.

   - For example, you want to manage changes to Memory Installed (phys_mem), MAC Address (mac_address), and IP Address (alarm_id) so that the attribute must have a matching Change Order for prod*. You do not want MDR1 to update IP Address and prefer MDR2 to complete this update. When you have a problem, create an Incident. Closing the Change Order also closes the Incidents automatically.

3. Determine what CIs or subset of the CIs in your system that you want to monitor.
   For example, you want to control all servers name test* and prod*. In addition, you control what CIs based on CI Class and CI Location.

4. Determine what MDRs and sources of data that you want to monitor.
   For example, you want to restrict data from MDR1 for the IP Address attribute from updating any CIs.

5. Determine the appropriate verification policy to manage the following types of change:

   - The CI changes that match change orders.

   - The CI changes that match the attributes in a Change Order, but do not match the value.

   - The CI changes that you consider as rogue updates.

   - Then CI changes that you consider as rogue inserts.

6. Determine the appropriate update behavior that CACF takes when it detects a variance for a policy:

   - Always allow the attribute update request.

   - Allow the attribute update only when a corresponding change specification is specified for the update.

   - Always cancel the entire transaction.

   - Keep the existing attribute value.

   - Write data to the TWA.

   - Create an Incident when CACF detects a variance.

   - Automatically close any Incidents after Change Order verification.

For more information about change verification planning and implementation, see Planning and Implementing Change Verification topic.

Example Change Specification in the Pending Verification Status

In this example, the Configuration Administrator established a verification policy for the Memory Installed (phys_mem) attribute to Allow Update Only if Matches Change Specification. CACF monitors a change specification for this attribute with the status Verification Pending, and sets the Change Specification to the Verified or Failed Verification status.

The following steps describe the lifecycle of this change specification:

1. A Change Order requests an update to the Memory Installed (phys_mem) attribute of a CI.
2. You create a change specification for the Memory Installed (phys_mem) Managed Attribute with a Planned Value of 4gb with the initial status as Verification Pending.
3. The Change Order moves to a status with change verification active such as Verification in Progress.
4. The change specification waits for a discovery tool to discover CI details and export the values to the CMDB.
5. One of the following actions occurs after the discovery tool exports the value to the CMDB:
   - The value for Memory Installed matches the 4gb value that you specified in the change specification. CACF sets the status from Verification Pending to Verified. CACF closes the Change Order.
   - The value for Memory Installed does not match the value that you specified. CACF sets the status from Verification Pending to Failed Verification.

Example Change Specification in the Verified Status

In this example, CACF verified a change specification and set the status to Verified. This change specification contained an initial status such as Verification Pending.

The following steps describe the lifecycle of this change specification:

1. A Change Order requests an update to the Serial Number (serial_number) attribute of a CI.
2. Create a change specification for the Serial Number managed attribute and enter **12345** as the planned value.
3. The Change Order moves to a managed state so that Change Verification is active.
   For example, Verification in Progress.
4. The change specification waits for a discovery tool to discover CI details and imports the updated Serial Number values to the CMDB.
5. The discovery tool exports the value to the CMDB and matches the value that you specified in the change specifications.

6. CACF sets the status to Verified.
   Note: If the CI update to the attribute does not match the planned value, CACF considers the update as a variance and sets the status to Failed Verification.

Example Change Specification in the Set After Change Verified Status

In this example, CACF updates the CMDB with the value that you want to use after the Change Order exits a managed change state with change verification active. For example, your environment uses Verification in Progress as the managed change state with change verification active enabled.

The following steps describe the lifecycle of this change specification:

1. A Change Order requests an update to the Serial Number (serial_number) attribute of a CI.
2. You create a change specification, specify Serial Number, and enter a planned value for an attribute.
3. You set the Change Order state to from RFC to Verification in Progress to Closed.
4. The CI attribute value is updated with the planned value after the Change Order exits a state with Change Verification Active (Verification In Progress) to a state that does not have change verification active (Closed).
5. The change specification sets to Was Set to Planned Value to indicate that the set was completed successfully.

Example Accept the Planned Value

In this example, the Change Analyst researches the correct attribute value for a CI and accepts the planned value.

Follow these steps:

1. Open a Change Specification that an end user created in your environment.
2. View the detail page to see the planned value for the CI attribute that the Change Analyst modified.
3. Research the attribute value for the CI.
   For example, your research indicates that the Change Analyst entered the correct value.
4. Click Accept Planned Value to update the CI with the corresponding planned value.
   CACF sets the state of the Change Specification to Accepted Planned Value.

Example Accept the Discovered Value

In this example, the Change Analyst determines that the CI has been updated to a correct attribute value for a CI and accepts the discovered value.

Follow these steps:

1. Open a Change Specification that a Change Analyst created in your environment.

2. View the detail page to see the planned value for the CI attribute that the Change Analyst specified.

3. Research the attribute value for the CI.
   For example, discovery indicates that the Change Analyst entered the incorrect value.

4. Click Accept Discovered Value.
   The CI updates with the discovered value and CACF sets the status of the change specification from Verification Pending to Accepted Discovered Value.

5. If you configured the managed state to enable the Promote Change Order After Verification option, CACF closes the Change Order after all change specifications are in a final state.

Example Manage Changes from an Unauthorized MDR

In this example, the Configuration Administrator established a verification policy to manage changes from an unauthorized MDR named MDR1. The policy rejects all updates to CIs from MDR1.

The following steps describe the lifecycle of this verification policy:

1. You create a Verification Policy with an MDR Name pattern of MDR1 and an Update Behavior of Always Cancel Entire Transaction.

2. Enable all Change Order alignment options.

3. Specify Any Managed Attribute and an asterisk (*) for all filters.

4. When the discovery tool (MDR1) runs and exports the data to the CMDB, the verification policy rejects all the updates.

How to Archive and Purge Audit Data

We recommend that you archive and purge obsolete Verification Log entries, CACF audit history, and CI audit history as part of your periodic database maintenance.

The CACF CA Business Intelligence reports typically present monthly reports with a yearly summary. The default archive purge time value for the archive purge rules for the log, CACF audit history, and CI audit history tables is 30 days. Use the same value in the archive and purge rules to help ensure data consistency between verification log entries, Incidents, and Change Orders. You can probably change the 30 day default to something more in keeping with your reporting requirements.

Complete the following actions to archive and purge audit data:

1. Use the current Incident rule to archive and purge inactive Incidents older than *nn* days.
   CA SDM archives and purges verification log entries only after archiving and purging associated Incidents. If you associate a Change order with an Incident, CA SDM does not check if the Change Order is active.

2. Use the current Change Order rule to archive and purge inactive Change Orders older than *nn* days.
   CA SDM archives and purges verification log entries and change specifications only after archiving and purging associated Change Orders. If you associated an Incident with a Change Order, CA SDM does not archive and purge the Change Order.

3. Use the Rogue Change Verification Log rule for rogue changes that did not create an Incident. Use this rule to archive and purge verification log entries older than *nn* days. By definition, rogue changes are not associated with Change Orders.

4. Use the CMDB Audit rule to archive information that is shown in the Change Specification History, Verification Policy History, Managed Change State History, and Managed Attribute History tabs show in the respective Change Specifications, Verification Policy, Managed Change State, and Managed Attributes detail forms. CA SDM stores this information in the ci_audit table.

Change Manager Responsibilities

This article contains the following topics:

The Change Manager is responsible for the overall enterprise change management process and for the ultimate approval of change orders. They also generate the change management metrics analysis reports and they do the following tasks:

- Review change requests and add appropriate stakeholders and approvers as needed.
- Facilitate resolution of issues, such as detecting collisions and scheduling conflicts in the calendar.
- Review installation, back-out, and fallback plans for accessibility and soundness.
- Understand the risk of each change and ensure that the appropriate risk level is assigned to the change.
- Monitor changes for their respective areas to ensure that they comply with Technology Change Management requirements.
- Represent their respective areas and communicate the impact of high-level risk changes at weekly CAB meeting.
- Facilitate in reviews after the installation is complete for problem installations and failed changes.
- Serve as the escalation point for change requesters, stakeholders, approvers, implementers, and support groups.

How the Change Manager Role Works

Change Managers are responsible for monitoring change orders to ensure that the operation team members comply with business policies and processes. The Change Calendar can facilitate resolution of issues such as change order conflicts by scheduling black-out dates and freeze periods during which a CI or a set of CIs can be changed. Change Managers also do the following tasks:

1. Oversee the CAB Console from which online and quick approvals of change orders and requests for changes are managed.
2. Organize CABs with members appropriate for the change orders under consideration and conduct regularly scheduled CAB meetings to review incoming change orders.
3. Create reports with details about the proposed requests for changes ready for CAB review and electronically distribute the reports to all CAB members.
4. Perform a real-time review of each request for change and update the record with the CAB decision during the CAB meeting.
5. Use BusinessObjects Business Intelligence Launch Pad to manage Compliance, Forecast, Trend, and Volume reports and create on-demand reports.
6. Represent their respective areas and communicate the impact of high-level risk changes at CAB meetings.
7. Evaluate the risk of each change and ensure that the appropriate risk level is assigned to the change.

Define Tasks for the Change Manager Role

You can define tasks for the Change Manager role.

Follow these steps:

1. On the Administration tab, select Security and Role Management, Role Management, Role List.
   The Role List page appears.
2. Select the Change Manager role.
   The Change Manager Role Detail page appears.
3. Click Edit.
   The Change Manager Update Role page appears.
4. Use the following tabs and fields to configure tasks and access permissions for the Change Manager role:
   - Authorization
   - Function Access
   - Web Interface
   - Knowledge Management

- KT Document Visibility
- Tabs
- Report Web Forms
- Go Resources
- Tenant Read Access
- Tenant Write Access

5. Click Save, Close Window.
   The Change Manager role record is updated.

Configure Change Manager Options

You can configure options for the Change Manager role.

Follow these steps:

1. Select Options Manager on the Administration tab.
2. Expand the Change Order Mgr node.
   The Option List appears.
3. Right-click the option that you want and select Edit from the context menu.
   The Update Option page appears.
4. Edit the option as appropriate.
5. Click Save, Close Window.
   The updated option appears on the Options list.

Change Categories, Status, and Risk Levels

You can define how change orders operate within your service environment. You can edit the default values that are installed with CA SDM, or can define your own.

Follow these steps:

1. Select Service Desk, Change Orders on the Administration tab.
2. Expand the Change Order node and select *one* of the following items:
   - Categories
   - Change Types
   - Closure Codes
   - Conflict Status

- Risk Level
- Risk Survey
- Status
- Workflow Task Status Code
- Workflow Task Types

The List page for the selected item appears.

3. Select the item to edit.
   The Update Details page appears.
4. Use the controls available on the tabs at the bottom of the page to define how change orders operate within your environment.
5. Click Save, Close Window.
   The updated item appears in the list.

View the Change Order Scoreboard

The Change Order scoreboard shows the change orders, conflicts, and scheduled tasks that are assigned to Level 2 Analysts, Change Managers, Change Coordinators, or CAB members. Users can view their assigned and unassigned records by priority.

Follow these steps:

1. Navigate to Change Orders on the CA SDM scoreboard.
2. Expand the folders to reveal nested folders for the following items:
   - Assigned or unassigned Open and Closed items
   - Resolved or unresolved conflicts
   - Scheduled tasks that start today or next week.
3. Select the folder for the items you want to see.
   The List page appears.
4. (Optional) Click Show Filter and complete one or more of the fields to specify search criteria that restrict the list to comments of interest.
5. Click Search.
   The List page displays summaries of the items that match your search criteria.
6. (Optional) Click the Edit in List button to display some additional fields that can be associated with an item.

Define a Change Order Stored Query

Defining the stored queries that are available to users on the Change Order scoreboard is an administrative task. You can modify the predefined stored queries that are installed with CA SDM, or can define your own.

Follow these steps:

1. Select Service Desk, Application Data, Stored Queries on the Administration tab.
   The Stored Query List appears.

2. Select the stored query that you want to edit.
   The Stored Query Detail page appears.

3. Click Edit.
   The Update Stored Query page appears.

4. Edit the field values as appropriate.

5. Click Save, Close Window.
   The updated stored query appears in the Stored Query List.

Example: Define a Stored Query to List Change Orders Assigned to a CAB to Which the Logged In User Belongs

This example demonstrates how you can create a stored query that lists only change orders that are assigned to a CAB to which the logged in user belongs.

Follow these steps:

1. Navigate the Scoreboard to the Update Stored Query page.

2. Edit the field values as follows:

   a. Select Scoreboard Usage.

   b. Set Type to Change Order.

   c. Enter the Where clause:

   ```
   cab.[group]group_list.member IN (@cnt.id) AND active = 1
   ```

3. Click Save, Close Window.
   The stored query appears in the Stored Query List.

CAB Responsibilities and CAB Groups

Contents

CAB Responsibilities

The Change Advisory Board (CAB) coordinates the review and approval or rejection of change requests for CI components and services. The CAB members are responsible for the following tasks:

- Reviewing all major changes to production systems.
- Attending all relevant CAB meetings as required by the Change Manager.
- Reviewing all submitted requests for changes to determine their impact, resources that are required to implement them and any ongoing costs.
- Participating in scheduling and coordination of the Change Calendar.
- Helping to ensure that all changes are adequately assessed and prioritized.
- Participating in reviews after the installation is complete.

CAB Approvals

If the CAB Approval field is set to YES, the CAB must approve a change order before implementing the change order. During the approval process, the change manager clicks Approve or Reject. If you want to use different status values, you can update the Approve or Reject button code using Web Screen Painter.

How the CAB Process Works

The CAB is responsible for reviewing all major changes to production systems. The CAB members are notified that a change request requires their approval, and they take the following actions:

1. List change requests that the CAB must review.
2. Open the CAB Console and view the information that is contained in the request.
3. View the business justification, implementation plan, configuration items, and supporting documentation that is associated with the request and decide to approve it or reject it.
4. Approve or reject the change order, and the next change order in the list appears automatically.
   The person requesting that the change is notified automatically that the CAB status is updated for the change request.

Manage CAB Groups

You can create and manage the CAB groups with members appropriate for the change orders under consideration. The CAB can include members from the application team, development manager, component owner, QA, support, and any additional parties deemed necessary.

Before you implement a CAB group, configure the appropriate contacts for your business structure.

Create a CAB Group

1. On the Administration tab, select Groups.
   The Group Search page appears.
2. Click Create New.
   The Create New Group page appears.
3. Complete the fields as appropriate.
4. Click Save.
   The CAB Group appears on the Group List page.

Assign Members to the CAB Group

1. On the Group Detail page, select the Members tab.
2. Click Update Members.
   The Contact Search page displays.
3. Enter the search criteria to display the desired contacts and click Search.
   The Members Update page displays, listing the contacts that matched the search criteria.
4. From the list on the left, select the contacts that you want to assign to this group. To select multiple items, hold down the Ctrl key while clicking the left mouse button.
5. When you have selected all the contacts that you want, click the selection button (>>).
   The selected contacts move to the Members list on the right.
6. Click OK.
   The Group Detail page displays, with the selected contacts listed on the Members tab.

Add the CAB Group to a Change Category

Note: Ensure that the Category_Defaults option is installed, so that the CAB field on change orders defaults to a CAB group.

1. On the Administration tab, select CA SDM, Change Orders, Categories.
   The Change Category List appears.

2. Select a category from the list.
   The Update Change Category page appears.

3. Select the appropriate CAB group from the CAB field.

4. Complete other fields as appropriate.

5. Click Save.
   The Change Category Detail page displays a successful save message.

6. Click Close Window.
   The CAB group is associated with the change category and the change order.

CAB Console and Reporting

Contents

The CAB Console is a dashboard that facilitates online and quick approvals of change orders that require CAB approval. The Change Manager and other CAB members use the console to view details about a change order (and its associated Workflow tasks and configuration items) and approve or reject the change order. The CAB Console lets team members review, approve or reject a change order, and continue to the next change order quickly. For change order requests, the CAB can deal with the request by satisfying it directly or by escalating/referring the request to an appropriate group.

The Change Manager can use CA SDM built-in summary and detail reporting options to accomplish the following tasks:

- Report approved and rejected change orders.
- Report change orders awaiting approval.

To print or view summary and detail reports, first select the records that you want to include in the report. You can select specific records for a report using the search feature of the list pages.

For example, from the Change Order list you can search for a list of change orders that are awaiting CAB approval that you can then use to generate a report. For more information, see Summary and Detail Reports (see page 3230).

Work with the CAB Console

The CAB Console provides Change Managers and CAB members with a visual rendering of the approval process for a selected change request. The CAB deals with the request in the most appropriate manner, either by satisfying the request directly or by escalating/referring the request to an appropriate group.

Approve or Reject Change Orders

Change Managers can quickly approve or reject change orders that are awaiting CAB approval, without needing to open each change order.

Follow these steps:

1. On the Service Desk tab, search for change orders that include values to indicate that CAB Approval is required and that the approval is not completed. For example, you can use the following values:

   - YES for the CAB Approval drop-down list.
   - Not Approved for the Status field.

   The Change Order List page shows change orders that are awaiting CAB approval.

2. Do one of the following steps:

   - Click CAB Console.
     The CAB Console appears and shows the change order details in read-only form for the first change order in the list.
   - Right-click any change order and select CAB Console from the shortcut menu.
     The CAB Console appears and shows the change order details in read-only form for the change order you selected.

3. Review the change order details and decide whether to approve or reject the change order.
4. (Optional) Enter the comments about the approval or rejection in the Comments field.
5. Click Approve Change or Reject Change.
   The first change order status is changed, any comments are saved, and the details for the next change order in the list appear automatically.

   You can use the Previous and Next buttons to navigate to next or previous change orders without updating the change.

6. Continue reviewing change orders, and approving or rejecting them until you reach the final change order in the list.
   The change orders are approved or rejected and their statuses are changed to Approved or Rejected, respectively.

7. Close the CAB Console.

Change CAB Console Properties

Using Web Screen Painter, you can change the CAB Console properties that appear on web forms in the CAB Console. For example, you can do the following actions:

Note: For more information, see Installing Web Screen Painter (see page 498) and Using the Web Screen Painter (see page 1898).

- Rename the Approve and Reject buttons. This button is the property on the order_approval_console.htmpl (change orders) web forms.
- Modify the status values of the Approve and Reject buttons by changing the 'REJ' or 'APR' values.
  - The ‘Reject Task’ button calls a function approve_reject(‘REJ’).
  - The ‘Approve Task’ button calls a function approve_reject(‘APR’).

You can only associate an active transition with a button. Do not deactivate a predefined status transition that is associated with a button. Otherwise, the predefined status transition no longer functions.

Follow these steps:

1. In Web Screen Painter, open the CAB Console form that you want to change.
   Web Screen Painter opens and displays the form.
2. On the Design tab, right-click the control that you want to change, and select Properties.
   The Properties - *control* page appears.
3. Change the properties that you want by entering a new value for each one.
   Changes take effect as soon as you click outside the field, and when you close the Properties page.
   The Web Screen Painter displays a brief summary of the significance of a property in a note that appears at the bottom of the Properties form when you select the property.

Example: Modify the CAB Console for Change Workflow Tasks

This example shows how to modify the task status using Web Screen Painter.

1. In Web Screen Painter, open the orderwf_approval_console.htmpl web form.
   Web Screen Painter opens and displays the form.
2. On the Design tab, right-click the Reject Task button, and select Properties.
   The Properties - Button page opens.

3. Find the function approve_reject('REJ').
   'REJ' is the status code for the Task status Reject.

4. Enter a new value for 'REJ'.
   Changes take effect as soon as you click outside the field, and when you close the Properties page.
   The Web Screen Painter displays a brief summary of the significance of a property in a note that appears at the bottom of the Properties form when you select the property.

Change Management Reporting

The Change Manager with appropriate privileges can use Business Intelligence Launch Pad to accomplish the following tasks:

- Report change volume by operating system, change category, group, implementer, risk, status, implementation date, affected configuration items (CIs), and changes originating from incident or problem tickets.
- Report successfully implemented changes grouped by change category, urgency, priority, impact, % successful vs. total for the specified period, and for the group of the change requestor
- Report failed changes grouped by category, urgency, priority, impact, reason for back out, % failed vs. total for the specified period, and the change requestor's group.
- Report the total number of change requests grouped by change category Change Coordinator, Change Manager, risk level, priority, and affected CIs for a specific time period.

You can navigate to the predefined reports in the left pane of the Business Intelligence Launch Pad window to view, schedule, modify, or run the report or to view the history and properties for a report. For more information about using Business Intelligence Launch Pad, see CA Business Intelligence Reports (see page 3182).

Conflict Analysis and Collision Detection

Contents

Conflict analysis detects and shows collisions that occur when two or more changes to the same configuration item are scheduled for implementation at the same time. The change management team handles scheduling collisions in the following ways:

- Uses the change calendar to see RFC-related CI collisions and makes adjustments to them to reduce potential impact.
- Searches for and detects collisions in a log.

You use the conflict status to help manage and identify conflicts. CA SDM provides the following default conflict statuses:

- **Researching**

Indicates the conflict is being researched by a user.

- **Resolved**

Indicates the conflict was researched and resolved by a user.

- **Unresolved**

Indicates the conflicts was not researched and resolved.

Resolve Scheduling Collisions

Conflict analysis detects and shows collisions that occur when two or more changes to the same configuration item are scheduled for implementation at the same time. You handle scheduling collisions as follows:

1. Navigate to the Change Order Detail page, and click the Conflicts tab.
   The Conflict List page appears.

2. Click Conflict Analysis.
   CA SDM detects scheduling collisions and the Conflict List page lists Schedule Collisions.

   The Conflict List and Change Calendar report any collisions to change orders. Each entry in the list or calendar represents a single collision that puts that change order at risk of failure. Collisions are detected only *after* you click Conflict Analysis for a change order.

3. Click Edit, and then click the Scheduler button.
   The Schedule for Change Order page appears and lists CIs that have scheduling collisions.

4. Investigate and resolve the collisions by updating the Schedule Start Date and Schedule End Date of a change order.

   The implementation schedule is the period between the Schedule Start Date and Schedule End Date of a change order.

5. Record your investigation of the collision.

Detect and Investigate Conflicts

You can detect and investigate change order conflicts to resolve scheduling problems.

Follow these steps:

1. Click the Conflicts tab on a change order.
   The Conflict List page appears.

2. Click Conflict Analysis.

   You can use the Search facility to search the Conflict List, however, searching does not run Conflict Analysis. Click Conflict Analysis to create or remove Conflict List entries.

   The conflicts that are detected for the change order are listed. The following listed information is not self-explanatory:

   - **Type Conflicting Change**
     Displays the type of change that is causing a conflict, for example, Scheduling Collision.

   - **Configuration Item Conflicting Change Summary**
     Identifies the configuration item that is causing the conflict and displays the configuration item summary.

3. Click a change or configuration item link.
   The details about the change or configuration item appear.

4. Investigate the cause of the conflict.

5. (Optional) Adjust the change schedule.

   The change schedule is the period between the Schedule Start Date and Schedule End Date. You have detected and investigated conflicts.

Define Conflict Logging

You can configure the Activity Log to generate entries when conflicts are created or updated so that you can track them. The Activity Log is predefined to generate entries when a conflict is updated. The Options Manager controls the Activity Log.

Follow these steps:

1. On the Administration tab, navigate to Options Manager, Change Order Mgr.
   The Option List page appears.

2. Install the following options:

   - **conflict added**
     Generates the Activity Log entries when conflicts are added.

- **conflict updated**
  Generates the Activity Log entries when conflicts are updated.

3. Save and restart the CA SDM server.
   Conflict logging is defined.

Report Change Order Conflicts

You can report details about change orders including information about change order conflicts, such as the conflict type, the change order that is affected by a conflict, and other conflict details.

Follow these steps:

1. Select the Service Desk tab.
2. Search for change orders.
3. Click Reports, Details.
   The Change Order Detail report appears.
4. (Optional) Scroll toward the end of the report to see conflict details.

Implement the Risk Survey

Contents

Risk assessments let you identify, evaluate, and quantify the risks of change orders that belong to change categories, before modifying a system or service in your environment. You create risk surveys to evaluate risks, and associate the surveys with change categories. When a user creates a change order and specifies a change category, the survey that is associated with that category is available for completion and submission.

The risk survey lists a series of single or multiple choice questions. Each answer has a weightage value. When creating a change order, the user selects the appropriate answers and submits the survey. The evaluated risk level is based on the weightages of answers that are selected by the user.

Implement the risk survey as follows:

1. Establish risk levels for your organization.
2. Create a risk survey (see page) or select from the default list (see page 2251). Create or modify risk survey questions and answers.

3. Modify risk ranges for the risk survey (see page 2251).
4. Associate the risk survey with a change category (see page 2252).
5. After you associate a risk survey with a change category, the Risk Survey button appears for the requester when they save a change order using the specified change category.
6. View the evaluated risk based on the risk survey results.
7. (Optional) Override the evaluated risk value from the Activities menu.

Create a Risk Survey

You can create a risk survey to assess risks for change orders that belong to a change category.

Follow these steps:

1. On the Administration tab, click Service Desk, Change Orders, Risk Survey.
   The Risk Survey Template List appears.
2. Click Create New.
   The Create New Risk Survey page appears.
3. Complete the following fields:
   - **Risk Survey Name**
     Specifies the name of the risk survey.
   - **Include Comments**
     Specifies to include comments in the survey.
   - **Comment Label**
     Specifies the caption to display for comments in the survey.
   - **Active?**
     Specifies if the survey is active or inactive.
   - **Risk Survey Description**
     Specifies a description of the risk survey.
4. Click Save.
   The Risk Survey Detail page appears. You can add questions (see page 2249) and answers to the survey (see page 2250).

Add Risk Survey Question

You can add questions to a survey to help assess risks for change orders that belong to a change category.

Follow these steps:

1. Open a risk survey, click the Questions tab, and click Add Question.
   The Create New Risk Survey Question Template page appears.

2. Complete the following fields:

   - **Sequence**
     Defines the order in which the question appears on the risk survey.

   - **Include Comments**
     Adds a text box to the end of the survey form for customer free-form comments.

   - **Comment Label**
     Adds a label to the comments text box.

   - **Active?**
     Specifies if the question is active or inactive.

   - **Multiple Response Question?**
     Indicates that this question has multiple answers.

   - **Question Text**
     Specifies the question text that appears in the survey.

3. Click Save.
   The question is added to the risk survey.

4. Close the page or create answers.

Add a Risk Survey Answer

After you save a risk survey question, you can add answers to the question to help assess risks for change orders that belong to a change category.

Follow these steps:

1. Open a risk survey, click the Answers tab, and click Add Answer.
   The Create New Risk Survey Answer Template appears.

2. Complete the following fields:

   - **Sequence**
     Defines the order in which the answer appears on the risk survey question.

   - **Active?**
     Specifies if the answer is active or inactive.

   - **Weightage**
     Specifies a numerical value that calculates risk.

   - **Answer Text**
     Specifies the answer text that appears in the survey.

3. Click Save.
   The Risk Survey Question Template detail page appears and the Answers tab updates with your answer.

4. Close the page or create more answers.

View a Default Risk Survey

CA SDM provides default risk surveys that you can associate with change categories.

Follow these steps:

1. Navigate to Service Desk, Change Orders, Risk Survey.

2. Select General from the Risk Survey Name column.
   The General Risk Survey Detail page appears..

3. Click View Survey.
   The risk survey appears, listing questions, answers, and weightage values for each answer. This survey applies to general changes within your organization.

4. Close the survey.

5. The General Risk Survey Detail page appears; close it.

Modify Risk Ranges

You can update risk range values for a survey. The sum of all selected answer weightages are compared with each risk range and the risk level are calculated.

Follow these steps:

1. Click Edit on the Risk Survey Template Detail page.

2. Click Edit in List to edit list items of risk range.

   The Minimum and Maximum Value fields appear.

3. Click on each row to modify minimum and maximum values. The values cannot overlap or you are unable to save the risk survey. Specify the range of values for each category of change that is based on the questions and their weight as follows:

   - High Risk Level -- 21-25
   - Medium-High Risk Level -- 16-20
   - Medium Risk Level -- 8-15
   - Low Risk Level -- 0-7

4. On the Risk Range tab, click Save(Y).

   The Risk Range List page updates.

5. Set the risk survey to Active.

6. Save and close the window.

Associate Risk Survey with a Change Category

You can associate a risk survey to help assess risk for change orders that belong to a change category.

Follow these steps:

1. Navigate to Service Desk, Change Orders, Categories.
   The Change Category List appears.

2. Click a change category in the Symbol column.
   The Change Category Detail page appears.

3. Click Edit.
   The Update Change Category page appears.

4. Click Risk Survey.
   The Risk Survey Template Search appears.

5. Search for the appropriate survey.
   Select the survey from the Risk Survey Name column.
   The Update Change Category page appears.

6. Click Accept.
   The change category updates and is associated with the risk survey.

Example: Deploy a Risk Survey

This example demonstrates how to deploy a default risk survey on your system using a default change category.

Follow these steps:

1. Navigate to Service Desk, Change Orders, Categories.
   The Change Category List appears.

2. Select Add.IT.Other from the Symbol column.
   The Add.IT.Other Category detail page appears.

3. Click Edit.
   The Add.IT.Other Update Change Category page appears.

4. Click Risk Survey.
   The Risk Survey Template Search appears.

5. Search for the risk survey. In this example, search for General and select the risk survey to add it to the detail form.
   The Risk Survey field populates with General.

6. Save and close the window.

If a user creates a change order using the Add.IT.Other category, the Risk Survey button when they save the change order.

Impact Explorer

This article contains the following topics:

Impact Explorer is an advanced tool for managing and controlling change within an organization. Impact Explorer allows the Change Manager to explore CIs that are attached to a change order and also interact directly with an attached CI or its child CIs.

Impact Explorer provides these advantages:

- Displays all CIs that are attached to a change order.
- Displays all child and peer-to-peer relationships for attached CIs.
- Provides the ability to attach any related CI to the change order.
- Displays a Descendants List of successively related CIs for any attached CI.
- Provides the ability to launch CMDB Visualizer for a CI.

Launch Impact Explorer

You can access Impact Explorer from the Config. Items tab of any change order.

Follow these steps:

1. Open a Change Order Detail page.
2. Select the Config. Items tab.
3. Click Impact Explorer.
   The Impact Explorer page appears.

If you close the Change Order Detail page, the Impact Explorer page also closes. If Impact Explorer is launched from multiple change orders, multiple Impact Explorer pages are displayed.

Explore Attached CIs

The Impact Explorer tree contains a node for each CI that is attached to a change order. A plus (+) symbol indicates that a CI has at least one child CI.

If more than 100 CIs are attached to the change order, only the first 100 are displayed. To view the next 100 CIs, click More...

To display the relationships for an attached CI, click the plus (+) symbol for the CI. The related CIs appear in the tree. In addition to the related CI names, the tree also displays relationship types in brackets.

View a CI in Impact Explorer

The Impact Explorer tree displays a node for each CI that is linked to a change order. A plus (+) symbol indicates that a CI has at least one child CI.

Follow these steps:

1. Click a CI node in the left pane.
   The Configuration Item Detail page appears in the right pane.

You can also display the CI Detail page in the right pane by right-clicking on the CI and selecting View from its context menu.

2. Click the change order node at the top of the left pane.
   The Change Order Detail page appears.

If the change order has more than 100 attached CIs, only the first 100 are displayed. To view the next 100 CIs, click More...

Add a Related CI to a Change Order

To maintain CI relationships, you may want to attach a related CI to the change order.

Follow these steps:

1. Click the Config. Items tab for a change order.
   The Configuration Items List page appears.

2. Click Impact Explorer.
   The Impact Explorer tree displays attached CIs.

3. Click any plus (+) for an attached CI node.
   CIs related to the node appear.

4. Right-click it a related CI and select Add to Change Order from the context menu.
   The new attached CI appears in the Config. Items tab for the change order.

Display the CI Descendants List

For any CI, you can display lines of related CIs (named *descendants*). In addition to basic information about each CI, the CI Descendants List displays relationship levels, with the originating CI as level 1. CI children begin at level 2, and their children at 3, and so on. If a CI is encountered more than once among the relationships, only its closest relationship level is displayed.

Example: Multiple Descendant Paths for One CI

Due to multiple relationships, a descendant search finds the same related CI at level 2 and also at level 4. The descendant CI is displayed only at level 2.

To list descendants for a CI

1. From a Change Order Detail page, select the Config. Items tab.

2. Click Impact Explorer to display attached CIs.

3. Expand a CI node if needed.

4. Right-click a CI and select List Descendants.
   The CI Descendants List is displayed.

Launch CMDB Visualizer from Impact Explorer

Impact Explorer provides the capability to launch CMDB Visualizer from an attached or related CI.

Follow these steps:

1. From a Change Order Detail page, click Impact Explorer.
   The Impact Explorer page displays.

2. Right-click any CI and select Launch Visualizer from its context menu.
   CMDB Visualizer is launched with the CI as the focus.

Configuring Impact Explorer

An Administrator can configure the Impact Explorer as follows:

- Specify the number of child CIs displayed for an attached CI.
- Specify the number of relationship levels that are displayed in the CI Descendants List,
- Suppress the display of child CIs,

The number of child CIs displayed is configurable by adding a NX_IMPACT_EXPLORER_MAX_CHILD_NODES setting to the NX.env configuration file. The default is 100.

Example: Configure the Display of Child CIs

Using the following setting, Impact Explorer only displays ten children at a time for an attached CI:

@NX_IMPACT_EXPLORER_MAX_CHILD_NODES=10

The default depth of the CI Descendants List is nine (9) levels. The depth is configurable by adding a NX_IMPACT_EXPLORER_MAX_LEVELS setting to the NX.env configuration file.

Example: Configure the Number of Descendant Levels

Using the following setting, the CI Descendants List displays the originating CI and only its relationally adjacent child CIs:

@NX_IMPACT_EXPLORER_MAX_LEVELS=2

Use the following Options Manager option to suppress the display of a certain type of child CI:

IMPACT_EXPLORER_EXCLUDE_HIER=boolean

If the IMPACT_EXPLORER_EXCLUDE_HIER option is installed and set to Yes, child CIs that are related through the CMDB Relationships tab of a CI Detail page are not displayed in the Impact Explorer tree or in the CI Descendants List.

Child CIs that are related through CA CMDB are still displayed.

Define a Change Order Stored Query

Defining the stored queries that are available to users on the Change Order scoreboard is an administrative task. You can modify the predefined stored queries that are installed with CA SDM, or can define your own.

Follow these steps:

1. Select Service Desk, Application Data, Stored Queries on the Administration tab.
   The Stored Query List appears.

2. Select the stored query that you want to edit.
   The Stored Query Detail page appears.

3. Click Edit.
   The Update Stored Query page appears.

4. Edit the field values as appropriate.

5. Click Save, Close Window.
   The updated stored query appears in the Stored Query List.

Example: Define a Stored Query to List Change Orders Assigned to a CAB to Which the Logged In User Belongs

This example demonstrates how you can create a stored query that lists only change orders that are assigned to a CAB to which the logged in user belongs.

To create the stored query:

1. Navigate the Scoreboard to the Update Stored Query page.
2. Edit the field values as follows:
   a. Select Scoreboard Usage.
   b. Set Type to Change Order.
   c. Enter the Where clause:

```
cab.[group]group_list.member IN (@cnt.id) AND active = 1
```

3. Click Save, Close Window.
   The stored query appears in the Stored Query List.

Change Orders

Contents

Change orders are requested changes that vary from the original scope of a specific project or task.

Create a Change Order

You can either create a change order from scratch or use an existing template.

Important! Depending on your role, you do not have access to all the functionality described in this section. For example, some predefined roles can edit records but cannot create new ones. Other roles, such as Configuration Viewer, can view Change Order information, but cannot create or edit change orders.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Service Desk tab, click the File menu and select the ticket type that you want to create. For example, to create a request from scratch, click File, New Request. To create a request from a template, Click File, New Request from Template.
2. Complete the Change Order Fields (see page 2260) as appropriate for the change order.
3. Use the controls available on the Change Order Tabs (see page 2264) as appropriate.
4. Click one of the following buttons:

   Auto Assign -- Triggers an auto assignment task, and updates the activity log. This button appears only when the ticket specifies a category or area that has auto-assignment enabled.

   Create Incident – Opens the Create New Incident page so you can create an associated incident ticket. This button appears only when you create change orders and requests.

   Find Similar -- Opens the Find Similar page to search for similar problems.**Quick Profile** -- Displays the contact information for the specified user in the **Affected End User** field. You can also view their environment details and their entire ticket history.

   Use Template -- Displays a list of available templates for the selected ticket type. You can select the template that you want to use for creating this ticket.

Note: You can use the Quick Profile to identify a contact to be the affected end user of your new ticket. Quick Profile allows you to search for a contact, and view the history of the issues, requests, change orders, incidents, and problems that are assigned to that contact. When you have identified a contact, you can create the incident ticket directly from the Quick Profile.

Create a Change Order from an Incident, Problem, or Request

While creating or editing an incident, problem, or request, you can define a change order to be associated with the incident, problem, or request.

Follow these steps:

1. On the Create New or Update page for your incident, problem, or request, click Create Change Order.
   The Create New Change Order page displays.

The Create New Change Order page opens only if all the required fields are defined for your incident, problem, or request.

2. Complete the fields as appropriate for the change order.
   See Change Order Fields (see page 2260) for field definitions.

3. Use the controls available on the tabs at the bottom of this page to process the change order as appropriate.
   See Change Order Tabs (see page 2264) for more information.

4. Save and close the window.

Create a Change Order from the Calendar

You can create a Change Order from the context menu on the daily, weekly and monthly calendar views. The context menu also allows you to create a Change Order from a template.

You cannot create a change order by right clicking on a range of dates in the weekly view.

Follow these steps:

1. Right click a date on the calendar.
   The context menu appears.

2. Select one of the following:

   - **Create Change Order**
     The Create Change Order detail page appears and pre-populates the following fields:

     - Requester and Affected End User (always set to the login user)
     - Schedule Start Date (set to midnight of the selected day)
     - Scheduled Duration (always set to 00:00:00)

   - **Create Change Order from Template**
     The Change Order Template list view appears.
     Select a template and the Change Order detail page appears with pre-populated fields.

3. Complete the fields as appropriate for the change order.
   See Change Order Fields (see page 2260) for field definitions.

4. Use the controls available on the tabs at the bottom of this page to process the change order as appropriate.
   See Change Order Tabs (see page 2264) for more information.

5. Click an execution option. Following are options that are not self-explanatory:
   Create Incident
   Opens the Create New Incident page so you can create a incident ticket associated with this change order.
   Quick Profile
   Displays the contact information for the user entered in the Affected End User field.
   If you are creating a change order, a list of available users appears. You can select the user that is in the Affected End User field.
   Use Template
   Displays a list of available change order templates. You can select the template you want to use for creating this change order.

Change Order Fields

The following fields are required to create or update a change order:

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Note: When the Change Order is in Edit mode, the Update CI button is disabled to prevent the possibility of duplicate CIs being added. To add CIs to a Change Order, save the Change Order, and the Update CI button is available for your use.

- **Change Reference Number**
  This is a unique reference number assigned by CA Service Desk Manager for all change order tickets. This is used by analysts and customers to refer to a particular change order ticket.

- **Requester**
  Specifies the name of the person who initiated the ticket. This person must be a defined contact. You can enter a value directly or click the magnifier to search for the name.

- **Affected End User**
  Specifies the contact name of the person who is affected by the record. If the contact is assigned to a special handling type, special handling indicators are displayed. You can enter a value directly or click the magnifier to search for a contact name.

- **Category**
  Indicates the general category of the change within your IT environment (for example, Change.IT. Server.Configuration or Move.IT.Workstation). Change categories provide default values that are entered automatically on all change orders assigned to the category. In addition to the predefined change categories, your system administrator may define custom change categories. You can enter a value directly or click the magnifier to search for a category. When you edit the Category and a CA Process Automation workflow is already running, the workflow cancels.

If a risk is associated with the specified change category, a Risk Survey button appears when you save the change order. This option opens a risk survey questionnaire for that change category.

Your system administrator has the option of adding custom properties to change order categories. If custom properties have been added, they are displayed on the Properties tab when you create, edit, or view a change order. Some custom properties require that you enter a value.

- **Status**
  Specifies the status code of the record. For example, you can list only the tickets with a status code of Fix in Progress, or can Close Requested. You can enter a value directly or click the magnifier to search for a status. The blue button (on the left side of the Status field) lets you change the current status to the next default status.

- **Priority**
  Specifies the priority ranking of the record. The ranking determines the amount of attention the ticket receives. The predefined priority levels are 1 (highest) through 5 (lowest). Your system administrator or an active priority calculation can generate the appropriate Priority values for various installations and tenants. When priority calculation is enabled, this field updates based on Impact, Urgency, Affected Service, and Affected User settings. When your administrator disables priority calculation and uninstalls the urgency_on_employee option, Self Service Users see the Priority field on the Request Detail page.

- **Type**
  Specifies the ITIL change type as Standard, Normal, or Emergency. A default value may be defined the change category.

- **Risk**
  Identifies the risk level of the change order. The risk level is determined by evaluating the risk survey associated with the change order.

Detail Fields

- **Created By**
  Specifies the name of the person who created or reported the record. This field is filled automatically with the current user's login information when the record is created.

- **Assignee**
  Specifies the name of the person who is assigned to handle the record. You can enter a value directly or click the magnifier to search for a name. Selecting an assignee populates the groups that the assignee belongs to in the **Group** field.

- **Group**
  Specifies the group that is responsible for this record. Your system administrator defines groups of contacts that are responsible for different types of issues, requests, incidents, or problems. Any contact who is part of the group can handle the record after it is assigned to the group. You can enter a value directly or click the magnifier to search for a group. Selecting a group populates the **Assignee** field with the corresponding assignee name, which belong to the group.

- **CAB**
  Specifies the group that is responsible for reviewing Requests for Changes (RFCs). The CAB provides multiple perspectives necessary to ensure proper decision making about implementing changes. The CAB can include members from the application team, development manager, component owner, QA, support, and any additional parties deemed necessary. You can enter a value directly or click the magnifier to search for a group.

- **Impact**
  Specifies an impact code, such as 1 -- Entire Organization, that indicates how a ticket affects work being performed. For example, a ticket that requires a network outage for several hours would have a higher impact than a ticket that takes a printer off-line. Your system administrator can modify the default impact codes, so they can vary from one installation to another

- **Active**
  Indicates whether the record is Active or Inactive. This value applies to the current record only, not the associated template.

- **Need By Date**
  Displays the date that the change order needs to be completed by. You can enter the date in mm /dd/yyyy hh:mm am | pm format, or click the calendar icon to select a date.

- **Call Back Date/Time**
  Indicates the date on which a follow-up call for this change order should be made. On the date you specify, the change order displays on your scoreboard under the Today's Issue Callbacks category. You can enter the date in mm/dd/yyyy hh:mm am | pm format, or click the calendar icon to select a date.

- **Root Cause**
  Identifies the code associated with the core reason why the ticket was opened. Your service desk can use generic root cause codes, such as Hardware Failure or Software Failure, or more specific codes, such as Network.Cable, Network.Card, or Network.Response. You can enter a value directly or click the magnifier to search for a code.

- **Organization**
  Specifies the company, division, or department that is associated with the change order. You can select a value from the drop-down list.

- **Project**
  Identifies the project. You can associate a change order with a project in order to establish a connection to an external project in another product such as CA Clarity PPM or CA SCM. The Project you enter in this field contains the external project information, such as the project name or ID, to make the connection and integration between CA SDM and the external project. You can enter a value directly or click the search icon to search for a project.

- **Closure Code**
  Indicates the final outcome of a completed change as Successful, Unsuccessful, or Successful with Errors. You can also create custom closure codes.

- **Business Classification**
  Classifies the change order into Major, Minor, or Significant. The classification helps to assess the change order magnitude.

- **External System Ticket**
  Specifies an identification for a ticket that belongs to an external system that integrates with CA SDM. This field stores hyperlinks and displays functional links in read-only mode.

Summary Information Fields

- **Order Summary**
  Gives an abbreviated description of the change order.

- **Spelling**
  Checks the spelling of the text you enter in the Order Summary field.

- **Order Description**
  Gives a detailed description of the change order.

- **Spelling**
  Checks the spelling of the text you enter in the Order Description field.

- **Schedule Start Date**
  Specifies the start date and time a change order appears on the Change Calendar pages. This field is optional, but must contain a date value if the Schedule Duration field contains a date value. Changes without an implementation date do not appear on the Change Calendar pages.

- **Schedule Duration**
  Indicates the amount of time required to implement the change in hours and minutes.

- **Schedule End Date**
  Indicates the end date and time a change order appears on the Change Calendar pages. This field is read-only. Its value is calculated from Schedule Start Date and Schedule Duration values.

- **CAB Approval**
  Indicates (Y/N) whether the change requires approval from a CAB. You can specify which changes are to be considered for CAB approval, by doing any of the following:

  - Set this option at change creation time or any subsequent time throughout the approval process.

  - Add an Action macro to set this field to Yes or No for use within classic workflow.

- **Open Date**
  Indicates the date and time at which the record was first created, in the time zone of the server. This field is filled in automatically when the change order is created. The date and time appear in mm/dd/yyyy hh:mm am | pm format.

- **Actual Start Date**
  Indicates the date and time at which the word Pending appears in the Status field for the change order. The date and time appear in mm/dd/yyyy hh:mm am | pm format.

- **Last Modified Date/Time**
  Displays the date that this change order was last modified.

- **Last Modified By**
  Displays the name of the last person who edited the change order.

- **Resolve Date**
  Indicates the date and time at which the change order is resolved. The date and time appear in mm/dd/yyyy hh:mm am | pm format.

- **Close Date**
  Indicates the date and time at which the change order is closed. The date and time appear in mm /dd/yyyy hh:mm am | pm format.

Change Order Tabs

The following tabs are available on the Create Change Order, Change Order Detail, and Update Change Order pages:

Related Tickets

- **Related Orders:** Allows you to create a parent/child relationship between the change order and another CA SDM record.

- **Incidents / Problems:** Attaches related incidents (see page 2266) and problems to a change order for analysts to reference.

- **Caused Requests:** Attaches requests that the change order causes for analysts to reference.

Configuration Management

- **Configuration Items:** Links configuration items (see page 2274) (CIs) to a change order to provide information to analysts about the system that the ticket affects. Configuration Items are automatically added to this list when a Change Specification is created.

- **Change Specifications:** Lists the change specifications (see page 2622) that are associated with the CI and the verification status. Change specifications are highlighted in red if they have failed verification or require manual verification.

- **Verification Log:** Displays logged information about change verification (see page 2230) activity for this Change Order. For example, this log identifies a CI where CACF detected a variance or rogue change. Verification log entries highlighted in red indicate the corresponding change specification is either Failed Verification or Manual Verification Active and may need further attention from the user.

Additional Information

- **Properties:** Defines custom properties for change order categories.

- **Workflow Tasks:** Associates workflow tasks with a change order. For more information, see Define a Category or Area (see page 1054) topic.

- **Service Type:** Allows you to attach a service type event (see page 2313) to indicate the level of support for the ticket.

- **Attachments:** Attaches a document or a link to a URL to the change order.
- **Conflicts:** Identifies change orders that conflict with the one being viewed. For more information, see Conflict Analysis and Collision Detection (see page 2245) topic.
- **Templates:** Allows you to create a template (see page 2315) using the current ticket as a model.
- **Costs / Plans:** Calculates estimated cost and duration of the entire change order by adding the estimated cost and duration (see page 2273) of each task.

Logs

- **Activities:** Displays a log of the activities performed to resolve the change order. For more information, see Add an Activity from the Ticket Management (see page 2308) topic.
- **Event Log:** Displays a record of significant actions that occur regarding the change order.
- **Support Automation:** Displays the assistance session log and lets you invite the end user to an assistance session.

If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

View Global Change Order Queue List

This window only appears in a multi-site installation and allows you to search and list change orders across the regions defined to your multi-site setup.

The Global Queue list forms can be used by analysts that work tickets across multiple regions. Each queue is a read-only list page that relates to tickets on remote (or local) regions. Once an item is selected from the queue, the analyst is re-directed to the appropriate regions to continue to process the ticket. Only enough information is replicated to allow analysts to make decisions on which ticket to process.

Only tickets that are assigned to groups belonging to a Global Group are selected for replication. Once selected for replication, it is replicated from that point forward even if no longer assigned to a Global Group. A Global Queue ticket is marked Inactive if no longer assigned to a Global Group. Marking the Global Queue ticket inactive does not affect the status of the original ticket that the Global Queue ticket references.

- **Change #**
  Specifies the number assigned to the change order.
- **Priority**
  Specifies a priority ranking for the change order.
- **Queue**
  Specifies is the name of the multi-site Region. This value is for display purposes only.

- **Status**
  Displays a specific status code for the change order. For example, you may want to list only the tickets with a status code of Fix in Progress, or Close Requested. Click the search icon to search for the status of interest.

- **Open Date**
  Displays the date the change order was opened. This field also displays the region of the ticket.

- **Contacts**
  Displays contacts associated with the change order, such as the assignee and end user.

- **Category**
  Displays the category of the change order. Categories designate an area of responsibility, such as adding or moving a workstation, and auto-populate certain fields on the tickets assigned to that category.

Attach Incidents, Problems, or Requests to a Change Order

You can attach related incidents, problems, or requests to a change order so that they can be referenced when editing or reviewing the change order.

Follow these steps:

1. On the Service Desk tab, browse to Change Orders, Assigned or Unassigned. Select the priority for the change order you want to edit.
   The Change Order List displays.

2. Select the change order.
   The Change Detail page displays.

3. Choose the Incidents/Problems tab and click Attach Incidents.

4. Complete the appropriate search fields, and click Search.

5. Select the incidents/problems/requests you want to attach to the change order, and click  .
   The selected items are added to the list on the right.

   > **Note:** Use the CTRL or SHIFT keys plus the left mouse button to select multiple incidents.

6. Click OK.
   The selected items appear in the Related Requests List on the Incidents/Problems tab of the Change Detail page.

Expedite a Change Order

You can use the Expedite Change Order command to change the status of unnecessary tasks to Skip so the change order can be completed quickly.

Note: Skip must be defined as a valid status for the task.

Follow these steps:

1. Select Change Orders from the Scoreboard.
   The Change Orders folder expands to reveal nested folders for Assigned, Unassigned, and All Scheduled change orders.

2. Select the appropriate folder under Assigned, Unassigned, and All Scheduled for the change order whose children you want to expedite.
   The Change Order List page appears.

3. Click the change order number.
   The Change Order Detail page appears.

4. Select Expedite Change Order from the Actions menu.
   The Expedite Change Order page appears.

5. (Optional) Enter comments in the Remarks field to explain the action.

6. Click OK.
   The Expedite Change Order page closes and the Workflow Tasks tab on the Change Order Detail page shows all unnecessary tasks with status of Skip.

How to Schedule Change Orders

Contents

You can view the schedule of all configuration items associated with a change order. Consider scheduling information when you create, edit, or view a change order, or when you update the Change Calendar. Viewing the schedule can help you avoid scheduling collisions.

Follow these steps:

1. Create or open a change order.

2. Associate CIs with the change order.

Note: If you do not associate a CI with the change order, an error appears when you click the Scheduler button.

3. Click View Scheduler.
   The Change Scheduler appears and displays the following views:

   - **Daily**
     (Default) Displays the time period of the change order for the selected date and time. If no date is associated with the change order, the view defaults on the current day.

   - **Weekly**
     Displays the time period of the change order in the current week and includes the implementation start date, which can be configured to the Change Calendar start date.

   Note: The schedule duration determines the length of shading on the schedule. For example, if you create a change order with a two hour duration, the light-yellow shading on the scheduler displays for the two hour defined duration.

4. (Optional) Click a CI to view its details. Hover over the CI name to view its full name.

5. (Optional) Modify the Implementation Start Date or Duration.

   a. Click View Schedule to preview the updated schedule.

   b. Click Update Schedule to update the schedule.

   Note: You can only modify the schedule in edit mode.

6. Save the change order.

7. Refresh the Change Calendar to view global and CI-associated change windows.

Use the Change Scheduler Example

The following example demonstrates how to use the change scheduler when creating a change order.

Follow these steps:

1. On the Service Desk tab, select File, New Change Order.
   The Create New Change Order page appears.

2. Select Update CIs on the Config. Items tab.
   The Configuration Item Search page appears.

3. Create or search for CIs.

4. Using the Affected Configuration Items Update page, add CIs to the change order.

5. Click OK.
   The Create New Change Order page updates.

6. Click the Scheduler button.
   The Schedule for Change Order page appears.

7. Select a view and do *any* of the following:

   - Click within the table cells to modify the Schedule Start Date.
   - Click Schedule Start Date to use the Date Helper.

8. Modify the Duration and click View Schedule.
   The schedule previews your changes.

9. Click Update Schedule.
   The schedule updates with your changes.

10. Save the change order.

Set the Maximum Number of CIs

You can set the maximum number of CIs that display in the change scheduler.

Follow these steps:

1. Open *NX.env*.
   You can locate this file in the following directory:

   ```
   $NX_ROOT\
   ```

2. Modify the value of *@NX_CHANGE_SCHEDULER_MAX_CI_CNT* to the maximum number you want.

   Note: By default, the variable is set to 100. If you set the maximum number of CIs greater than 100, only the first 100 display and you get a warning.

3. Save *NX.env* and cycle CA SDM.
   The maximum number of CIs is set.

Example: Set the Maximum Number of CIs to 25

With the following setting, only the first 25 CIs will display on the change scheduler.

```
@NX_CHANGE_SCHEDULER_MAX_CI_CNT=25
```

Modify Change Order Duration Background Color

You can change the background color of the change order duration. Modify the following lines in *schedule.css* to change the highlighting of the green change order duration bar.

Follow these steps:

1. Open *schedule.css*.
   You can locate this file in the following directory:

   ```
   $NX_ROOT\bopcfg\www\wwwroot\css
   ```

   Important! $NX_ROOT\sdk also contains a file called schedule.css that contains helpful comments about css controls.

2. Modify the following lines with the color code you want:

   ```
   td.noBorderBackColor{border-left:none;border-right:none;background-color:
   #F6E3CE;}
   td.withBorderBackColor{border-right:none;border-left:1px solid;background-color:
   #F6E3CE;}
   ```

3. Save *schedule.css*.

In the following example, the change duration background color is #FF0000.

Example: Modify the Change Duration Background Color to #FF0000

```
td.noBorderBackColor{border-left:none;border-right:none;background-color:#FF0000;}
td.withBorderBackColor{border-right:none;border-left:1px solid;background-color:
#FF0000;}
```

Modify Change Window Colors in the Change Scheduler

You can change colors that indicate change windows by modifying lines in *schedule.css.*

Note: If you modify *schedule.css* to change the formatting of windows on the Change Scheduler, you must also modify the schedGroup macros used by the Change Calendar if you want its formatting to be consistent with the Scheduler.

Follow these steps:

1. Open *schedule.css* in a text editor.
   You can locate this file in the following directory:

   ```
   $NX_ROOT\bopcfg\www\wwwroot\css
   ```

2. Modify the following lines with the color code you want:

   ```
   .schedConflict { background-color: #ff0000; font-size: 4px }
   .schedBusy { background-color: #0176ff; font-size: 4px}
   .schedCurrent { background-color: #008000; font-size: 4px; }
   .schedMW { background-color: #40ff40; font-size: 4px; }
   .schedBW { background-color: black; font-size: 4px; }
   .schedNone {font-size: 4px; }
   ```

```
.schedDialog { width: 100%; height: 4px; margin-left: 0px; margin-right: 0px;
margin-top: 4px; margin-bottom: 4px; }
```

3. Save *schedule.css*.
   The background color is modified.

View or Update a Change Schedule

You can view and update a change schedule to help avoid scheduling collisions, or to streamline and balance the work effort.

Follow these steps:

1. Create, edit, or view a change order.

   Note: You can only modify the schedule in edit mode.

   The Change Order Detail page appears.

2. On the Config. Items tab, click Update CIs to add CIs to the change order.

3. Click the Scheduler button.
   The Schedule for Change Order page appears.

4. Modify the Schedule Start Date and Duration as appropriate, for example, to resolve scheduling collisions.

   Note: You can edit the start date by clicking within the table cells. Clicking the table cells on the daily view shifts the schedule in 10-minute increments. Clicking the table cells on the weekly view shifts the schedule in one hour increments.

   Details of the change order display when you hover over a line in the table cells.
   The change scheduler indicates the following types of schedules:

   - Blue -- Regular change order
   - Green -- Global maintenance window or CI-associated window
   - Dark Green -- Schedule of the current change order
   - Black -- Blackout window
   - Red -- If the current change order conflicts with other scheduled change orders.

Note: This indicator only displays conflicts with the current change order, not change conflicts in general. The red conflict only appears after the change order is saved. Use the highlighted change scheduler durations to determine conflicts.

For information about modifying colors in the change scheduler, see Modify Change Window Colors in the Change Scheduler (see page 2270)

5. Click Update Schedule and save the change order.

6. View the updated Change Calendar.

Update the Change Scheduler

You can update the Change Scheduler when you create or edit a change order.

Follow these steps:

1. Select the change order from the Change Order List page on the Scoreboard.
   The Change Order Detail page appears.

2. Select Activities, Update Schedule on the menu bar.
   The Update Schedule page appears.

3. Enter a new start date, duration, and date of activity.

   Note: You can enter the values directly or click the icon to open the Date Helper.

4. Change any other activities fields as appropriate.

5. Click Save.
   The Change Scheduler is updated, and the activity is recorded on the Activities tab on the Change Order Detail page.

Create Change Windows

Create change windows to avoid collisions in the Change Calendar.

Follow these steps:

1. On the Administration tab, click Service Desk, Change Orders, Change Windows.
   The Change Windows List appears.

2. Click Create New.
   The Create New Change Window page appears.

3. Complete the appropriate fields.

4. Save and close the change window.
   The change window appears in the Change Windows List.

Associate a CI with a Maintenance Window

To control when a CI undergoes maintenance, you can associate that CI to a maintenance window.

Follow these steps:

1. Navigate to the Change Window Detail page.
2. Click the Associated CIs tab.
   The Associated CIs list appears.
3. Click Update Configuration Items.
   The CI Search page appears.
4. Specify information for the required CIs.
5. Click Search
   The Available CIs page appears.
6. Move any required CIs in the Available CIs list to the Associated CIs list.
7. Click OK.
   The Change Window Detail page appears.
8. Click Save.
   The CI is associated with a maintenance window.

The change window, the CIs and the selected window associations are saved.

Accumulate Costs and Time to a Change Order

The accumulate feature allows you to calculate the estimated cost and duration of the entire change order by adding together the estimated cost and duration of each task. You can also choose to accumulate the change order and all of its children. Children are additional records entered as a result of attempting to resolve the original change order.

Follow these steps:

1. Select Change Orders, Assigned or Unassigned, and priority level on the Service Desk tab.
   The Change Order List appears.
2. Select the change order of interest.
   The Change Detail page appears.
3. Select Actions, Accumulate Change Order on the menu bar.
   The Accumulate Change Order page appears.
4. Click one of the following buttons:

- **Accumulate this Change Order and All Children**
  Calculates the estimated cost and duration of the change order by adding together the estimated cost and duration of tasks for this change order and all of its children.

- **Accumulate Only this Change Order**
  Calculates the estimated cost and duration of the change order by adding together the estimated cost and duration of tasks for only this change order.

- **Cancel**
  Closes the Accumulate Change Order page without accumulating the change order.

The estimated cost and duration are accumulated and you are returned to the Change Detail page.

5. Select the Costs/Plans tab on the Change Detail page.
   The tab displays the estimated cost and duration for the change order based on the values accumulated.

Change Order Configuration Items

Configuration items include all the hardware, software, and services associated with your system. Configuration item records uniquely identify each item and its exact location. These records are part of the inventory components that make up your database.

You can link configuration items to an issue or change order in order to give analysts information about the system that is affected by the ticket. Consider using change verification in your CMDB environment to verify that changes execute correctly.

Follow these steps:

1. On the Scoreboard, browse to Change Orders, Assigned or Unassigned. Select the priority for the change order you want to edit.
   The Change Order List displays.

2. Select the change order.
   The Change Detail page displays.

3. (Optional) Select the Change Specifications tab to view or create change specification to associate with the ticket.

4. Select the Configuration Items List tab, and click Update CIs.
   The Configuration Item Search page displays.

5. Complete one or more of the search fields, and click Search.
   A list of available configuration items displays.

6. Select the configuration items you want to link to the change order, and click  .
   The selected configuration items are added to the list on the right.

> **Note:** Use the CTRL or SHIFT keys plus the left mouse button to select multiple configuration items.

7. Click OK.
   The selected configuration items appear on the Config. Items tab on the Change Detail page.

8. Click Close Window.
   The updated change order appears in the Change Order List when you redisplay the list.

Create a Change Order Template

This article contains the following topics:

You can define a ticket, such as an incident, problem, issue, change order, or request, to serve as a model for future tickets. You can then save it as a template. Tickets that are created with that template have certain fields auto-populated with your specified values.

Create a Template from a New Ticket

You can use a new ticket to create a template to be used when creating future tickets.

Follow these steps:

1. On the Service Desk tab, click the File menu and select the ticket type for the template. For example, to create an incident template, click File, New Incident.

2. Complete the fields as appropriate for the template in the page that opens.

3. Select the Template tab at the bottom of the page.

4. Complete the following fields:

   Template Name
   This name appears in the list of available templates.

   Template Class
   (Optional) You can assign a class to the template.

   Quick Template Type
   You can use quick templates to define new requests on the Quick Profile Scratchpad. Select one of the following options:

   - None
   - Quick
   - Review Before Save

Template Active
Specifies whether the template is active or inactive in the database.

Description
Describe the template settings and intended usage. This field can be used as a filter when searching for a template. Wildcard searches are supported.

5. Click Save.

Create a Template from an Existing Ticket

You can use an existing ticket to create a template.

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.
3. Select the desired ticket from the list that appears.

> **Note:** Some roles can only access certain ticket types through the Search menu on the Service Desk menu bar.

4. Click Edit.
5. (Optional) Edit the fields as appropriate.
6. Select the Template tab at the bottom of the page.
7. Complete the following fields:

Template Name
This name appears in the list of available templates.

Template Class
(Optional) You can assign a class to the template.

Quick Template Type
You can use quick templates to define new requests on the Quick Profile Scratchpad. Select one of the following options:

- None
- Quick
- Review Before Save

Template Active
Specifies whether the template is active or inactive in the database.

Description
Describe the template settings and intended usage. This field can be used as a filter when searching for a template. Wildcard searches are supported.

8. Click Save.

Create a Change Order

This article contains the following topics:

You can create a ticket such as an incident, problem, request, issue, or change order, using various methods. This article explains these methods.

Important! Depending on your role, you do not have access to all the functionality described in this section. For example, some predefined roles can edit records but cannot create new ones.

Create a Ticket from the File Menu

You can either create a ticket from scratch or use an existing template.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Service Desk tab, click the File menu and select the ticket type that you want to create. For example, to create a request from scratch, click File, New Request. To create a request from a template, Click File, New Request from Template.

2. Fill in the fields as appropriate for the ticket. See the field definitions at the end of this page. Use the controls available on the tabs at the bottom of this page to process the ticket as appropriate.

3. Click one of the following buttons:

   Save -- Saves the incident and closes the page.

   Auto Assign -- Triggers an auto assignment task, and updates the activity log.

   Note: This button appears only when the ticket specifies a category or area that has auto-assignment enabled.
   Create Change Order -- Opens the Create New Change Order page. You can create a change order ticket that is associated with this incident.**Note:** This button appears only when you create incidents, problems, and requests.

   Create Problem -- Opens the Create New Problem page so you can create a problem ticket associated with this incident.**Note:** This button appears only when you create incidents and requests.

   Create Incident – Opens the Create New Incident page so you can create an associated incident ticket.**Note:** This button appears only when you create change orders and requests.

   Reset -- Resets all fields to the last saved values.

   Find Similar -- Opens the Find Similar page to search for similar problems.**Quick Profile --** Displays the contact information for the specified user in the **Affected End User** field. You can also view their environment details and their entire ticket history.

   Use Template -- Displays a list of available templates for the selected ticket type. You can select the template that you want to use for creating this ticket.

Create a Ticket Using Quick Profile

You can use the Quick Profile to identify a contact to be the affected end user of your new ticket. Quick Profile allows you to search for a contact, and view the history of the issues, requests, change orders, incidents, and problems that are assigned to that contact. When you have identified a contact, you can create the incident ticket directly from the Quick Profile.

Follow these steps:

1. Select View, Quick Profile on the menu bar of the Scoreboard.
   The Quick Profile Contact Search window opens.

2. (Optional) Complete one or more of the filter fields to list only the contacts of interest.

3. Click Search.
   Note: All search fields that allow text entry support use of the % wildcard character.
   The Quick Profile Contact List page lists the contacts that match your search criteria.

4. Select the user who is the affected end user of the new ticket.
   The contact pane displays contact information and the ticket history for the contact.

5. In the Scratchpad pane, do the following actions:

    a. Enter a description for the new record in the Scratchpad text field.

    b. Select the ticket type from the Type drop-down list.

    c. (Optional) Enter a Template name for the new record. You can enter a value directly or click the search icon to search for available templates.

6. Click New.
   A new window opens and displays the information that you entered in the Scratchpad.

7. Complete the empty fields as appropriate.
   See the field definitions at the end of this page.

8. Use the controls available on the tabs at the bottom of this page to process the ticket as appropriate.

Add Attachments to Tickets

You can attach a document or a link to a URL to a ticket. The document or URL provides more explanation or justification for the report.

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.

2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.

3. Open the desired ticket from the list that appears.

4. Select the Attachments tab, and then click one of the following options:

    - Attach Document

    - Attach URL

5. Follow the on-screen instructions to attach a file or URL to the incident.
   The URL or the document is added to the record and is listed on the Attachments tab of the Incident Detail page.

View Tickets

You can view summary information for tickets after you create them.

If you are using multi-tenancy, a tenant drop-down list appears in the search filter. If you select <empty> in this drop-down list, the search is public.

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.

2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.

3. Select the folder for the tickets that you want to see.

4. (Optional) Click Show Filter and complete one or more of the fields to specify search criteria that restricts the list to the tickets of interest.

5. Click Search.
   The search result displays the tickets that match the criteria.

6. Click the ticket # link to view the incident of interest.
   The detail page appears.

Create a Change Order from an Incident, Problem, or Request

While creating or editing an incident, problem, or request, you can define a change order to be associated with the incident, problem, or request.

To create a change order from an incident, problem, or request

1. On the Create New or Update page for your incident, problem, or request, click Create Change Order.
   The Create New Change Order page displays.

   The Create New Change Order page opens only if all the required fields are defined for your incident, problem, or request.

2. Complete the fields as appropriate for the change order.
   See Change Order Fields (see page 2281) for field definitions.

3. Use the controls available on the tabs at the bottom of this page to process the change order as appropriate.
   See Change Order Tabs (see page 2285) for more information.

4. Save and close the window.

Create a Change Order from the Calendar

You can create a Change Order from the context menu on the daily, weekly and monthly calendar views. The context menu also allows you to create a Change Order from a template.

You cannot create a change order by right clicking on a range of dates in the weekly view.

To create a change order from the calendar

1. Right click a date on the calendar.
   The context menu appears.

2. Select one of the following:

   - **Create Change Order**
     The Create Change Order detail page appears and pre-populates the following fields:

     - Requester and Affected End User (always set to the login user)
     - Schedule Start Date (set to midnight of the selected day)
     - Scheduled Duration (always set to 00:00:00)

   - **Create Change Order from Template**
     The Change Order Template list view appears.
     Select a template and the Change Order detail page appears with pre-populated fields.

3. Complete the fields as appropriate for the change order.
   See Change Order Fields (see page 2281) for field definitions.

4. Use the controls available on the tabs at the bottom of this page to process the change order as appropriate.
   See Change Order Tabs (see page 2285) for more information.

5. Click an execution option. Following are options that are not self-explanatory:
   Create Incident
   Opens the Create New Incident page so you can create a incident ticket associated with this change order.
   Quick Profile
   Displays the contact information for the user entered in the Affected End User field.
   If you are creating a change order, a list of available users appears. You can select the user that is in the Affected End User field.
   Use Template
   Displays a list of available change order templates. You can select the template you want to use for creating this change order.

Change Order Fields

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

The following fields require explanation:

Note: When the Change Order is in Edit mode, the Update CI button is disabled to prevent the possibility of duplicate CIs being added. To add CIs to a Change Order, save the Change Order, and the Update CI button is available for your use.

- **Requester**

  Specifies the name of the person who initiated the ticket. This person must be a defined contact. You can enter a value directly or click the magnifier to search for the name.

- **Affected End User**

  Specifies the contact name of the person who is affected by the record. If the contact is assigned to a special handling type, special handling indicators are displayed. You can enter a value directly or click the magnifier to search for a contact name.

- **Category**
  Indicates the general category of the change within your IT environment (for example, Change.IT. Server.Configuration or Move.IT.Workstation). Change categories provide default values that are entered automatically on all change orders assigned to the category. In addition to the predefined change categories, your system administrator may define custom change categories. You can enter a value directly or click the magnifier to search for a category. When you edit the Category and a CA Process Automation workflow is already running, the workflow cancels.

  If a risk is associated with the specified change category, a Risk Survey button appears when you save the change order. This option opens a risk survey questionnaire for that change category.

  Your system administrator has the option of adding custom properties to change order categories. If custom properties have been added, they are displayed on the Properties tab when you create, edit, or view a change order. Some custom properties require that you enter a value.

- **Status**
  Specifies the status code of the record. For example, you can list only the tickets with a status code of Fix in Progress, or can Close Requested. You can enter a value directly or click the magnifier to search for a status. The blue button (on the left side of the Status field) lets you change the current status to the next default status.

- **Priority**

  Specifies the priority ranking of the record. The ranking determines the amount of attention the ticket receives. The predefined priority levels are 1 (highest) through 5 (lowest). Your system administrator or an active priority calculation can generate the appropriate Priority values for

various installations and tenants. When priority calculation is enabled, this field updates based on Impact, Urgency, Affected Service, and Affected User settings. When your administrator disables priority calculation and uninstalls the urgency_on_employee option, Self Service Users see the Priority field on the Request Detail page.

- **Type**
  Specifies the ITIL change type as Standard, Normal, or Emergency. A default value may be defined the change category.

- **Risk**
  Identifies the risk level of the change order. The risk level is determined by evaluating the risk survey associated with the change order.

The following fields provide change order details:

- **Created By**
  Specifies the name of the person who created or reported the record. This field is filled automatically with the current user's login information when the record is created.

- **Assignee**
  Specifies the name of the person who is assigned to handle the record. You can enter a value directly or click the magnifier to search for a name.

- **Group**
  Specifies the group that is responsible for this record. Your system administrator defines groups of contacts that are responsible for different types of issues, requests, incidents, or problems. Any contact who is part of the group can handle the record after it is assigned to the group. You can enter a value directly or click the magnifier to search for a group.

- **CAB**
  Specifies the group that is responsible for reviewing Requests for Changes (RFCs). The CAB provides multiple perspectives necessary to ensure proper decision making about implementing changes. The CAB can include members from the application team, development manager, component owner, QA, support, and any additional parties deemed necessary. You can enter a value directly or click the magnifier to search for a group.

- **ImpactImpact**

  Specifies an impact code, such as 1 -- Entire Organization, that indicates how a ticket affects work being performed. For example, a ticket that requires a network outage for several hours would have a higher impact than a ticket that takes a printer off-line. Your system administrator can modify the default impact codes, so they can vary from one installation to another.

- **Active**
  Indicates whether the record is Active or Inactive. This value applies to the current record only, not the associated template.

- **Need By Date**
  Displays the date that the change order needs to be completed by. You can enter the date in mm /dd/yyyy hh:mm am | pm format, or click the calendar icon to select a date.

- **Call Back Date/Time**
  Indicates the date on which a follow-up call for this change order should be made. On the date you specify, the change order displays on your scoreboard under the Today's Issue Callbacks category. You can enter the date in mm/dd/yyyy hh:mm am | pm format, or click the calendar icon to select a date.

- **Root Cause**
  Identifies the code associated with the core reason why the ticket was opened. Your service desk can use generic root cause codes, such as Hardware Failure or Software Failure, or more specific codes, such as Network.Cable, Network.Card, or Network.Response. You can enter a value directly or click the magnifier to search for a code.

- **Organization**
  Specifies the company, division, or department that is associated with the change order. You can select a value from the drop-down list.

- **Project**
  Identifies the project. You can associate a change order with a project in order to establish a connection to an external project in another product such as CA Clarity PPM or CA SCM. The Project you enter in this field contains the external project information, such as the project name or ID, to make the connection and integration between CA SDM and the external project. You can enter a value directly or click the search icon to search for a project.

- **Closure Code**
  Indicates the final outcome of a completed change as Successful, Unsuccessful, or Successful with Errors. You can also create custom closure codes.

- **External System Ticket**

  Specifies an identification for a ticket that belongs to an external system that integrates with CA SDM. This field stores hyperlinks and displays functional links in read-only mode.

The following fields provide change order summary information:

- **Order Summary**
  Gives an abbreviated description of the change order.

- **Spelling**
  Checks the spelling of the text you enter in the Order Summary field.

- **Order Description**
  Gives a detailed description of the change order.

- **Spelling**
  Checks the spelling of the text you enter in the Order Description field.

- **Schedule Start Date**
  Specifies the start date and time a change order appears on the Change Calendar pages. This field is optional, but must contain a date value if the Schedule Duration field contains a date value. Changes without an implementation date do not appear on the Change Calendar pages.

- **Schedule Duration**
  Indicates the amount of time required to implement the change in hours and minutes.

- **Schedule End Date**
  Indicates the end date and time a change order appears on the Change Calendar pages. This field is read-only. Its value is calculated from Schedule Start Date and Schedule Duration values.

- **CAB Approval**
  Indicates (Y/N) whether the change requires approval from a CAB. You can specify which changes are to be considered for CAB approval, by doing any of the following:

  - Set this option at change creation time or any subsequent time throughout the approval process.

  - Add an Action macro to set this field to Yes or No for use within classic workflow.

- **Open Date**
  Indicates the date and time at which the record was first created, in the time zone of the server. This field is filled in automatically when the change order is created. The date and time appear in mm/dd/yyyy hh:mm am | pm format.

- **Actual Start Date**
  Indicates the date and time at which the word Pending appears in the Status field for the change order. The date and time appear in mm/dd/yyyy hh:mm am | pm format.

- **Resolve Date**
  Indicates the date and time at which the change order is resolved. The date and time appear in mm/dd/yyyy hh:mm am | pm format.

- **Close Date**
  Indicates the date and time at which the change order is closed. The date and time appear in mm /dd/yyyy hh:mm am | pm format.

Change Order Tabs

The following tabs are available on the Create Change Order, Change Order Detail, and Update Change Order pages:

Related Tickets

- **Related Orders**
  Creates a parent and child relationship (see page 2277) between the change order and another change order.

- **Incidents / Problems**
  Attaches related incidents (see page 2266) and problems to a change order for analysts to reference.

- **Caused Requests**
  Attaches requests that the change order causes for analysts to reference.

Configuration Management

- **Configuration Items**
  Links configuration items (see page 2274) (CIs) to a change order to provide information to analysts about the system that the ticket affects. Configuration Items are automatically added to this list when a Change Specification is created.

- **Change Specifications**
  Lists the change specifications (see page 2622) that are associated with the CI and the verification status. Change specifications are highlighted in red if they have failed verification or require manual verification.

- **Verification Log**
  Displays logged information about change verification (see page 2230) activity for this Change Order. For example, this log identifies a CI where CACF detected a variance or rogue change. Verification log entries highlighted in red indicate the corresponding change specification is either Failed Verification or Manual Verification Active and may need further attention from the user.

Additional Information

- **Properties**
  Defines custom properties for change order categories.

- **Workflow Tasks**
  Associates Workflow (see page 1068) tasks with a change order.

- **Service Type**
  Associates a service event to indicate the level of support for the ticket.

- **Attachments**
  Attaches a document or a link to a URL to the change order (see page 2277).

- **Conflicts**
  Identifies change orders that conflict (see page 2246) with the one being viewed.

- **Templates**
  Creates a change order using a template (see page) using the current ticket as a model.

- **Costs / Plans**
  Calculates estimated cost and duration of the entire change order by adding the estimated cost and duration (see page 2273) of each task.

Logs

- **Activities**
  Displays a log of the activities (see page 2287) performed to resolve the change order.

- **Event Log**
  Displays a record of significant actions that occur regarding the change order (see page 2289).

- **Support Automation**
  Displays the assistance session log and lets you invite the end user to an assistance session.

If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

Define a Category to a Change Order

For more information, see the Define a Category or Area (see page 1054) topic.

Add Activities to a Change Order

This article contains the following topics:

You can record all the actions that you are taking to resolve the ticket on the Activities tab. Activities can include actions such as research, calling a customer, and transferring responsibility to a different analyst. Some activities, such as "Initial" or "Field Update" are posted automatically when you create the ticket or update a field. Others, such as returning a call, changing the status, or transferring the ticket are posted when you select items from the Activities menu or from the Activities page itself.

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.
3. Open the desired ticket from the list that appears.
4. On the menu bar, click Activities, and then select one of the following options:
   - **Update Status** to update the status of the ticket.
   - **Callback** to record the time that is spent on the call.
   - **Research** to record the time spent conducting the research.
   - **Log Comment** to record your comments.
   - **Solution** to enter a description of the solution.
   - **Transfer** to reassign a problem to another technician.
   - **Escalate** to escalate the priority of a problem.
   - **Manual Notify** to send a manual notification to the user.
5. Edit the fields as appropriate. The following fields require explanation:

- **Internal?**
  Select this check box if the activity must only be visible to internal users.

- **Time Stamp**
  Specifies the date and time the activity began. This field shows the system date and time the activity record was opened. This field cannot be edited.

- **Date of Activity**
  The date and time the activity was performed. Defaults to the date and time the activity record was opened, but can be changed.

- **Time Spent**
  Specifies the amount of time that is spent on the activity. Enter this value in hours, minutes, and seconds (hh:mm:ss).

- **Related Ticket Activity Type**
  Specifies the type of activity that is generated for a related ticket, for example, Update Status

- **Change**
  Select an existing change order to which you want to attach the ticket.

- **Impact**
  Indicates the effect that the record has on tasks being performed. Your system administrator can modify the default impact codes, so they can vary from one installation to another.

6. Click Save.
   The activity is recorded on the Activities tab on the ticket details page.

Provide a Reason for Escalating the Ticket

If your priority calculation settings let you change Urgency and Impact values, you provide a reason for escalating the ticket. If priority calculation is not enabled, you can edit the priority field.

Follow these steps:

1. Open a ticket, such as an Incident or a Problem.
   The Ticket Detail page appears.

2. Modify the Urgency or Impact of the ticket.

3. Click Save.
   The Escalate Detail page appears and displays the current, read-only values for Priority, Urgency, and Impact.

4. Enter a reason for why you want to change the Urgency or Impact values.

5. Click Accept.
   The ticket is modified and the activity log updates with your changes.

Send a Manual Notification to a Temporary Email Address

You can send a manual notification to a temporary email address. For example, one that is not associated with a contact record.

Note: This operation is available only if the Administrator has installed the notification_allow_temp_address Update Options (Options Manager, Notifications).

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.
3. Open the desired ticket from the list that appears.
4. On the menu bar, click Activities, Manual Notify.
   The Manual Notification page appears.
5. Complete the following field, and click Add Email.
   - **Email address**
     Specifies an SMTP address for an email recipient. You can specify temporary email addresses (for example, addresses not associated with a contact record). Separate multiple addresses with a semi-colon.

   Note: This field appears only if the Administrator installed the notification_allow_temp_address Update Options (Options Manager, Notifications).
   The address is added to the Recipients list.
6. Complete the remaining fields as appropriate.

   Note: You can also add a personalized response such as a generic or administrator signature to the notification. The response is added at the end of the message text. For more information about personalized responses, see Personalized Responses (see page 2287).
7. Click Notify.
   The manual notification is sent and the activity is recorded on the Activities tab of the ticket Detail page.

View Change Order Events

This article contains the following topics:

- Event Logs (see page 2291)

The Event List contains a record of the events that are associated with the ticket. Your administrator maintains events, or procedures the system perform after a certain amount of time has elapsed. For example, an event might send a message to an analyst if a Priority 1 ticket is not resolved within an hour.

Follow these steps:

1. On the Service Desk tab, select Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.
3. Select the desired ticket from the list that appears.
4. Click the Event Log tab at the bottom of the details page.
   A list of events for this incident appears.

View the Event History

You can view the event history for a ticket to see what actions have been performed to resolve the ticket.

Follow these steps:

1. On the Service Desk tab, select Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority level for the desired ticket.
3. Select the desired ticket from the list that appears.
4. Select View, Event History on the detail page menu bar.
   The Event History window displays the following fields:

   - **Condition**
     Indicates the condition checked for by the event. CA SDM provides macros that check for standard conditions such as priorities and object status (open or closed).
   - **Event**
     Indicates the name of event that is associated with this row in the Event History list.
   - **Status**
     Indicates whether the event is active or inactive.
   - **Check Time**
     Indicates the time that the event was checked, based on time parameters that are specified in the event configuration.
   - **Time Loaded**
     Indicates the time that the event was loaded, based on time parameters that are specified in the event configuration.

View the Event Delay History

You can view the event delay history for a ticket to see descriptions of the service type event delays. Service type event delays let you suspend a service type event to prevent a service level violation.

Follow these steps:

1. On the Service Desk tab, select Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority level for the desired ticket.
3. Select the desired ticket from the list that appears.
4. Select View, Event Delay History on the detail page menu bar.
   The Event Delay History window displays the following fields:
   - **Start Time**
     Indicates the date and time the delay began.
   - **Stop Time**
     Indicates the date and time the delay ended.
   - **Actual Delay**
     Indicates the actual duration of delay.
   - **Effective Delay**
     Indicates the effective duration of delay.
   - **Service Type**
     Defines the support level that is assigned to the ticket (for example, four-hour service requirement).

Event Logs

The Event Log displays significant actions that are performed by the user, such as on tickets. For example, you submit a Knowledge Document and link it to an Incident. The Incident logs a failed status transition or detected Change Conflict. In this example, the Contact detail can display the following types of information:

- The log displays the time that the user logged in to CA SDM and when they closed the session.
- The user accepted the Terms of Usage.
- The user created a Knowledge Document.
- The user created a ticket, such as an Incident, Problem, Request, or Change Order.
- The user used a Knowledge Document to avoid creating a ticket.

Change Calendar

Contents

The *Change Calendar* provides a graphical view of change events with implementation start and end times. This calendar view of the change schedule provides analysts and managers a quick way to identify when events occur and how they affect the environment, organization, and resources.

The calendar lets you create change orders from the daily, weekly, and monthly views and also lets you view global change windows for scheduled change orders. If multiple change windows exist in a month, they are grouped, such as in a single Blackout Window group. Drill down to a weekly or daily view, or view hover information to see the individual window details.

You can only export (see page 2296) Change Order schedules, not Change Windows.

View the Change Calendar

You can configure the view of the Change Calendar page to display a calendar of the change orders of interest.

You can create a Change Order from the File menu, the Create New button on the Change Calendar page, or the context menu on the daily and monthly calendar views. The context menu also lets you create a Change Order from a template.

Follow these steps:

1. Click the Change Calendar tab.
   The Change Calendar filter fields appear.

2. Display a calendar view showing the schedule for the change orders of interest by completing the Change Calendar search fields (see page). Click Search.
   The Change Calendar provides the following filter fields to restrict the change orders displayed on the schedule:

   - **Active**
     Filters by whether the change orders are active (open) or inactive (complete).

   - **Priority**
     Filters by the priority ranking of the change orders.

- **Status**
  Filter by the status of the change order. You can enter the status directly or click the search icon to search for the desired status.

- **Category**
  Filters by the category of change order. You can enter a value directly or click the browse icon to select from defined categories.

- **Group**
  Filters by the group responsible for the change order. Your system administrator defines groups of contacts that are responsible for different types of issues, requests, incidents, change orders, and so on. Any individual contact assigned to the group can handle the record once it has been assigned to the group. You can enter the value directly or click the search icon to search for the group.

- **Parent**
  Filters by the parent change order.

- **Change Type**
  Filters by the type of change order as Emergency, Normal, or Standard.

- **CI Name**
  Filters by the name of the Configuration Item. You can enter a value directly or click the browse icon to search for the desired Configuration Item.

- **CI Class**
  Filters by the class of the Configuration Item. You can enter a value directly or click the browse icon to select from defined categories.

- **CI Family**
  Filters by one of the following Configuration Item families:

  - Computer
  - Hardware
  - Other
  - Projects
  - Service
  - Software

- **Conflict Status**
  Filters by the conflict status of a change order. You can enter a value directly or click the browse icon to select from defined categories.

- **Closure Code**
  Filters by the closure code of a change orders.

- **CAB**
  Filters by CAB member. You can enter a value directly or click the browse icon to select from defined groups.

- **CAB Approval**
  Filters by change orders that do not require CAB approval (N) or that do require CAB approval (Y).

- **Risk**
  Filters by the risk level of a change order.

- **Schedule Start Date**
  Specifies the beginning of an implementation date range for the change orders you want displayed on the schedule. If you do not enter a value in this field, the filter selects all change orders with a non-null target implementation start date. Regardless of whether or not you enter a value in this field, the initial view always includes the first change order actually selected for the schedule.

- **Schedule End Date**
  Specifies the end of an implementation date range for the change orders you want displayed on the calendar. If you do not enter a value in this field, the filter selects all change orders with a non-null target implementation end date.

- **Schedule Timezone**
  Specifies a time zone to view your search results.

  
  If no time zone is selected, the events are displayed in your current time zone.

- **Initial View**
  Select the view of the Change Order Calendar you want to see:

  - **Month**
    Displays a schedule for the full month that includes the first change order selected by the filter. The schedule shows change orders grouped by change type and schedule start and end date.

  - **Week**
    Displays a schedule for a the week that includes the first change order selected by the filter. The schedule seven consecutive days in a single column, beginning with the weekday configured as the starting weekday at your installation. The schedule shows individual change orders, and includes summary information about each one

  - **Day**
    Displays a view similar to the week view, except that it shows only a single day's change orders.

  - **n Days**
    Displays a view similar to the week view, except that it can begin on any day of the week, and continues for the specified number of days.

- **List**
  Displays a standard list page.

iCalendar Event Templates

iCalendar event templates control the information that is exported to iCalendar format. The following predefined templates are installed with CA SDM:

- Change Schedule
- KnowledgeScheduleCreation
- KnowledgeScheduleExpired
- KnowledgeScheduleReview
- KnowledgeScheduleStart

You can edit the predefined iCalendar event template codes, but you cannot delete them or create new ones.

The SchedExpMaximum variable in web.cfg controls the maximum events allowed for an export. Increasing the default (1000) could cause system instability. If you attempt to export more than the value specified in SchedExpMaximum, a message appears refusing your exporting request.

iCalendar Event Template Fields

The following fields require explanation:

- **Symbol**
  Defines the display name by which you want to identify the event template within your system.
- **Code**
  Defines a localized and independent code for the event template.
- **Record Status**
  Specifies whether the record is active or inactive.
- **Object Type**
  Displays the object type such as Change Order or Knowledge Document.
- **Alarm**
  Allows you to set a display alarm (such as 1 Day before or 1 Hour before) for each event that creates a calendar.

- **Category**
  Displays the field property for the event template. This is similar to how message templates are processed.

- **URL**
  Displays the field property for the event template. This is similar to how message templates are processed.

- **Extra Entries**
  Allows you to add other properties (not managed by CA SDM) to the event.

Export Schedules to iCalendar

CA SDM lets you export Change Orders in the standard iCalendar format. This data exchange lets you import Change Order schedules into many widely used calendaring applications, including Microsoft Outlook and Lotus Notes.

When exporting schedules on some calendaring programs, choosing the Open option instead of Save causes the file to import incorrectly. To avoid this issue on Knowledge Management and Change Order schedules, select the Save option instead of Open. After you save the exported file, import it through the interface of the calendar program interface. You cannot export Change (blackout and maintenance) Windows, only Change Orders.

The data you export is based on the current view. If you want to export a custom range of dates, such as 32 days, the export should be done from the list view. Otherwise, the view is truncated to a month or week, and it only exports that amount.

Follow these steps:

1. Click the Change Calendar tab.
   The Change Calendar filter fields appear.

2. Complete the search fields to display a calendar or list view that includes the change orders of interest.

3. Click Export.
   The Schedule Export page appears.

The SchedExpMaximum variable in web.cfg controls the maximum events allowed for an export. Increasing the default (1000) could cause system instability. If you attempt to export more than the value specified in SchedExpMaximum, a message appears refusing your exporting request.

4. Enter the location where you want to save an iCalendar file.
   An iCalendar file containing all events in the current view is saved at the specified location.

Use the Change Calendar Tab

This tab displays only if you have access to the Change Calendar.

The Change Calendar tab provides access to the schedule to view change order impacts on your system. From the Change Calendar tab, you can:

- Search for change orders
- Filter and sort change orders and configuration items
- Create change orders
- View CIs associated with change orders
- View change windows
- View CIs associated with change windows

You can use the schedule (see page 2292) to view and manage change orders. Create change orders from the schedule and search for change orders and configuration items.

To search for items within the schedule, use the search filter. Complete one or more of the search entry fields and click Search. The list pane populates with all items that match your search criteria.

View and Configure Scheduling Views

This article contains the following topics:

Schedule Views

CA SDM provides the following scheduling views:

- **List**
  Displays a list page sorted by schedule start and end date.

- **Month**
  Displays a calendar for a full month.
  The view shows change orders in groups, with each entry collecting one or more change orders. You can see detailed information about the change orders in a group by hovering over the group with the mouse; by pressing Alt+Right Arrow when the focus is on the group; or by clicking on the group to display its contents in an n-day view.

- **Week**
  Displays a full week in a single column, starting with the day configured as the first weekday.
  The view shows changes individually and includes detailed information about each change order scheduled during the week.

- **Day**
  Displays change orders for a single day.
  The view shows changes individually and includes detailed information about each change order scheduled during the day.

- ***n* Days**
  Displays change orders for the number of days specified by the dropdown selector.
  The view shows changes individually and includes detailed information about each change order scheduled during the days selected.

Navigating the Schedule Views

You can use the arrow and tab keys to navigate the scheduling views. The following keyboard shortcuts are available:

- **Tab**
  Navigates to a later date. Use this from the last cell in the schedule to navigate to the Search button.

- **Shift+Tab**
  Navigates to a previous date. Use this from the first cell in the schedule to navigate to the Next Month button.

- **Shift+Arrow**
  Navigates around the calendar from date to date in the direction of the arrow.

- **Right Arrow**
  Displays the context menu for the currently focused date or event. If there is no context menu, it navigates to the next higher date (similar to Shift+Right Arrow).

- **Alt+Right Arrow**
  Displays a hover information popup for the currently focused date or event. If there is no hover information, it navigates to the next higher date (similar to Shift+Right Arrow).

- **Down Arrow**
  Navigates to the next event in the current cell. If there are no events in the current cell, or if the focus is already on the last event, it navigates to the date in the next cell down (similar to Shift+Down Arrow).

- **Up Arrow**
  Navigates to the previous event in the current cell. If focus is not on an event, it navigates to the date in the next cell up (similar to Shift+Up Arrow).

Calender View Hotkeys

Each schedule view supports hotkey access to its buttons. The following are the supported hotkeys:

- **Alt+0**
  Switch to list view.
- **Alt+1**
  Switch to daily view.
- **Alt+7**
  Switch to weekly view.
- **Alt+3**
  Switch to monthly view.
- **Alt+9**
  Switch to *n*-day view.
- **Alt+<**
  Move to previous time period in current view.
- **Alt+>**
  Move to next time period in current view.

Scheduling View Configuration

You configure the monthly and weekly scheduling views by specifying pdm_macro statements in the <head> section of the HTMPL forms defining the schedule. We recommend using the Source View of Web Screen Painter to edit these forms.

Any form that displays a schedule must contain the following:

- A schedConfig macro
- At least one schedAttr macro
- At least one schedGroup macro

The configuration macros are in a separate source file referenced by a pdm_include statement in the main source file. This file lets you configure your schedule without modifying the main source file.

For example, the configuration macros for the Change Calendar form list_chgsched.htmpl are in a file named list_chgsched_config.htmpl. For the Knowledge Lifecycle Schedule, you can modify the list_kdsched_config.htmpl using the same macros.

You can find list_chgsched_config.htmpl and list_kdsched_config.htmpl in the following directory:

$NX_ROOT\bopcfg\www\htmpl\web\analyst\

schedConfig Macro -- Configure Schedule

The schedConfig macro specifies that a form contains a schedule and provides basic configuration information. The following values are valid macro arguments:

- **autosearch=1|0**
  Specifies whether the schedule form reloads data from the server when the user selects a view outside the currently selected date range. Setting the value to 1 (default) causes the form to search automatically when the user selects a view with one or more days outside the date selection range of the search filter. Setting the value to 0 requires the user to press the Search button to initiate a search.

- **defaultView=0|1|7|30|99**
  Specifies the default view for the search filter as 0 (list), 1 (day), 7 (week), 30 (month), or 99 (n-day).
  The specification for defaultView affects only the initial display of the search filter. After the schedule displays, CA SDM automatically keeps the filter view selection aligned with the current view.
  Default: 30

- **firstday=0|1|2|3|4|5|6|7**
  Specifies the first weekday on the monthly view as a number between 0 (Sunday) and six (Saturday).
  Default: 0

- **export=xxx|0**
  Specifies the code name of the template used for exporting in iCalendar format. Setting the value to 0 indicates the export feature and button are disabled.
  Default: ChangeSchedule

- **legend=1|2|0**
  Specifies the location of the schedule legend showing the name and formatting of the groups on the schedule. You can set the value to 1 to position the legend above the schedule, or 2 to position the legend below the schedule. Set the value to 0 to disable the legend.
  Default: 2

- **maxGroups=0/*n***
  Specifies the maximum number of groups to be displayed in a single cell of the calendar month view.
  If there are more than maxGroups scheduled for a single day, CA SDM displays only the first maxGroups-1, and replaces the last with a "..nn more changes" hyperlink that the user can mouseover or click to see the full list. Set the value to 0 to disable this feature and allow an unlimited number of events in a calendar cell.
  Default: 4

- **nday=(n,n,...)**
  Specifies selections for the drop-down list for the n-day view.
  The specification is a list of day counts that are to be included in the drop-down list, or 0 to indicate that the n-day drop-down list is omitted from the schedule. The first value specified is the default for the drop-down list.
  Default: (3,7,14,28)

- **round=(*hr,min*)|0**
  Specifies whether schedule start and end dates are rounded when collecting change orders or knowledge documents into groups. Specify round=0 to disable rounding.
  By default, schedule start and end date groups objects. All CA SDM dates include a time, and without rounding, objects scheduled as little as a minute apart would be in separate groups. Rounding determines the group after adjusting the start date to an earlier hour or minute and the end date to a later hour or minute.
  The value of round specifies either an hour or a minute (but not both). Times are rounded to the nearest multiple of the value specified, for example:
  round=(0,15) rounds to the nearest quarter hour
  round=(0,30) rounds to the nearest half hour
  round=1 rounds to the nearest hour
  round=12 rounds to the nearest half day (12:00 AM or PM)
  round=24 rounds to the nearest day
  Default: (0,15)

- **timefmt=24hr|([am],[pm])**
  Specifies the format of times on the calendar views of the schedule.
  The default value of 24hr specifies that times are displays in 24 hour format (0:01 - 23:59). The alternative value of (am,pm) specifies a suffix for either morning or afternoon times, or both.

All schedConfig arguments are optional.

schedAttr Macro -- Specify a Stored Attribute

The schedAttr macro specifies an attribute stored for each item selected for the list. Stored attributes are available for hover information on the monthly view, for the detailed or summary information in views other than the monthly view, and in the setSchedEvents() JavaScript function. The following values are valid macro arguments:

- **attr=xxxx**
  (Required) Specifies an attribute from the object on the schedule, such as a change order or Knowledge Document. Dotted attributes are permitted. The keyword attribute name CI*nn* can be used on the Change Calendar to specify that first *nn* CIs associated with the change order are included with the information stored.

  This argument is the only required argument for the schedAttr macro.

- **attrRef=.COMMON_NAME|xxxx**
  Stores the attribute of the referenced table stored for an SREL attribute (ignored for non-SREL attributes). The attribute name specified must be prefixed with a dot.
  Default: .COMMON_NAME

- **label=**
  Displays a label for the attribute on the n-day view.
  Default: the Majic DISPLAY_NAME of the attribute

- **ident=1|0**
  Specifies whether the attribute is an identifier for the object (such as a reference number of a change order). Identifier attributes are displayed without a label in front of the group name in hover information and the n-day view.
  Default: 0

- **detail=1|0**
  Specifies whether the attribute is included in the detail information shown on views other than the monthly view. Detail information is the information shown when the Summary Only check box on the view is not selected.
  Default: 1

- **hoverInfo=1|0**
  Specifies whether the attribute is included in the hover information pop-up displayed on the monthly view when the mouse pointer hovers over a group, or the user presses Alt+Right Arrow when focus is on the group.
  Default: 0

- **summary=1|0**
  Specifies whether the attribute is included in the detail information shown on views other than the monthly view. Detail information is the information shown when the Summary Only check box on the view is not selected.
  Default: 0

CA SDM displays attributes in summary, detail, or hover information in the same order as their schedAttr macros.

schedGroup Macro -- Specify an Event Group

The schedGroup macro specifies the name and color coding of a group of items. The monthly view aggregates all items in a group into a single event. Views other than the monthly show individual items in the format for the group to which they belong. The following optional values are valid macro arguments:

- **grpname=xxx**
  (Required) Specifes the name of the group. The macro automatically assigns a number to the group and assigns the number to a JavaScript variable with a name of the form schedGroup_xxx, where xxx is the name of the group. This variable can be used in the setSchedEvents() JavaScript function to create an event belonging to the group.

  This argument is the only required argument for the schedGroup macro.

- **label=xxx**
  Specifies a label for the group. If specified, the label is displayed in all views.

- **legend=xxx|0**
  Displays a description of the group for the legend that appears at the bottom of the schedule. Groups appear in the legend if at least one example of the group exists in the current view. Specifying 0 causes the group always to be excluded from the legend.
  Default: 0

- **color=black|*color***
  Specifies the color of text in items of this group. You can specify color in CSS format, either a valid web color or a hexadecimal value preceded by a pound sign.
  Example: Enter either "#FF0000" or "red" for red.
  Default: black

- **bgcolor=white|*color***
  Specifies the background color of items of this group. You can specify bgcolor in CSS format, either a valid web color or a hexadecimal value preceded by a pound sign.
  Example: Enter either "#FF000" or "red" for red.
  Default: white.

- **style=normal|bold|italic**
  Specifies the style of text of this group in the normal, bold, or italic style.
  Default: normal

Configure Blackout and Maintenance Windows on the Change Calendar

You edit PDM_MACRO statements in list_chgsched_config.htmpl to modify colors, labels, legends, and icons for change windows.

If you use schedGroup macros to change the formatting of windows on the Change Calendar, you must also update *schedule.css* if you want the formatting to be consistent with the Change Scheduler.

To configure change windows

1. Open the *list_chgsched_config.htmpl* form in a text editor or WSP.
   You can locate this file in the following directory:

   ```
   $NX_ROOT\bopcfg\www\htmpl\web\analyst\
   ```

2. On the schedGroup macro, modify the following PDM_MACRO statements:
   For maintenance windows:

   ```
   <PDM_MACRO NAME=schedGroup grpname=maintWindow
       bgcolor=lightgreen
       label="Maintenance"
       legend="Maintenance Window"
       icon= "confirmation_12.png">
   ```

   For blackout windows:

```
<PDM_MACRO NAME=schedGroup grpname=blackoutWindow style=italic color=white
    bgcolor=black
    label="Blackout"
    legend="Blackout Window"
    icon= "warning_12.png">
```

- **bgcolor**
  Specifies the background color of the window.

- **label**
  Specifies the window label as Blackout or Maintenance.

- **legend**
  Specifies the text of the legend as it appears on the Change Calendar.

- **icon**
  Specifies an optional URL to a 12x12 pixel web graphic.
  This icon displays with a change order or group on the Change Calendar if the change order lies completely within a maintenance window or overlaps a blackout window.

3. Save the form.
   The change windows are configured.

The setSchedEvents() JavaScript Function

The setSchedEvents() JavaScript function creates events in the schedule. Modify this function when you want to view any new group objects. The predefined group objects appear by default.

CA SDM calls setSchedEvents() once for each object (change order or knowledge document) selected by the schedule search filter. The function creates events for the object by calling a second function, schedEvent(), and passing the group ID, start date, and end date of the event.

The function can create any number of events (including zero) for an object. The default setSchedEvents() function for the Change Calendar (list_chgsched.htmpl) creates one event for each change order and groups change orders by change type. This function is coded as follows:

```
1.    function setSchedEvents( chg )
2.    {
3.    var grpnum;
4.    switch( chg["chgtype"] - 0 ) {
5.        case 100: grpnum = schedGroup_std;  break;
6.        case 300: grpnum = schedGroup_emer; break;
7.        default:  grpnum = schedGroup_norm; break;
8.    }
9.    chg.schedEvent( grpnum, chg["sched_start_date"], chg["sched_end_date"] );
10.    }
```

The case parameter specifies the change type ID.

The function has a single argument of a JavaScript object containing the attributes specified by schedAttr macros. The switch statement in lines 4-8 examines the chgtype attribute of the change order, and assigns the appropriate group number from one of the schedGroup_xxxx variables defined by previous schedGroup macros. On line 9, it calls the schedEvent() function to create an event in the schedule, passing the group number previously assigned and the schedule start and end dates. The dates are available in the argument object because they were specified in earlier schedAttr macros.

How to Schedule Change Windows

Contents

Schedule Change Order

You can schedule change windows and view them in the Change Calendar. *Maintenance windows* establish time periods when CI changes should occur, and *blackout windows* establish time periods when CI changes should *not* occur. Change windows help you schedule changes to minimize their effect on critical business processes. CA SDM can implement change windows at the global or system level.

To schedule change windows, do the following:

1. View the Change Calendar to see where you want change windows.

2. Create the appropriate change windows for your organization.

   - **Maintenance Window**
     Indicates a scheduled time period during which a CI or a set of CIs can be changed. Because changes can involve downtime, these windows can be used to minimize disruptions to critical business processes. In general, scheduled changes should occur inside a maintenance window.

   - **Blackout Window**
     Indicates a scheduled time period during which CI changes should not occur. This blackout can indicate a reduced support period (for example, a holiday), a corporate event, or a critical business time, such as fiscal year-end. In general, scheduled changes should only occur outside blackout windows.

   - **Global Change Windows**
     Indicates a blackout or maintenance window that occur for your entire organization. For example, you want to create a global (see page 2308) blackout window named Holiday that starts in November and ends in January in the American - East timezone. This blackout window does *not* allow non-emergency changes between these dates. Global change windows do not associate with specific CIs because they apply to all CIs.

3. (Optional) Specify the recurrence patterns of the change windows.

4. Open the Change Calendar.
   The legend displays icons and colors to identify change windows in the schedule.

5. Create change orders associated with CIs.

6. Update the Change Calendar by using the Change Scheduler.

Define Change Windows

You can define change windows to avoid collisions on the Change Calendar. For example, you want to create a global (see page 2308) blackout window named Holiday that starts in November and ends in January in the Amercan - East timezone. This blackout window does *not* allow nonemergency changes between these dates.

Follow these steps:

1. On the Administration tab, select Service Desk, Change Orders, Change Windows.
   The Change Windows List appears.

2. Click Create New.
   The Create New Change Window page appears.

3. Complete the required fields for the change window.

4. Specify one of the following recurrence patterns:

   - **None**
     Specifies no recurrence pattern.

   - **Daily**
     Specify either the number of days between recurrences, or that the window should recur every day.

   - **Weekly**
     Specifies the number of weeks between recurrences, and the weekdays when the window recurs. Windows longer than 24 hours can only recur on a single weekday.

   - **Monthly**
     Specifies the number of months between occurrences, and the day of the recurrence. The day can be specified either absolutely (for example, the 7th of the month) or positionally (for example, the second Monday of the month).

   - **Yearly**
     Specifies the number of years between occurrences, and the day of the recurrence. The day can be specified either absolutely (for example, March 7th) or positionally (for example, the second Monday of March).

   - **End by**
     Specifies the end of the recurrence.

5. Save and close the window.
   The change window appears in the Change Window List.

Associate a CI with a Maintenance Window

To control when a CI undergoes maintenance, you can associate that CI to a maintenance window.

Follow these steps:

1. Navigate to the Change Window Detail page.
2. Click the Associated CIs tab.
   The Associated CIs list appears.
3. Click Update Configuration Items.
   The CI Search page appears.
4. Specify information for the required CIs.
5. Click Search
   The Available CIs page appears.
6. Move any required CIs in the Available CIs list to the Associated CIs list.
7. Click OK.
   The Change Window Detail page appears.
8. Click Save.
   The CI is associated with a maintenance window.

The change window, the CIs and the selected window associations are saved.

Create a Blackout Window Example

The following example creates a blackout window to indicate that your organization does not schedule change orders for a specific time period. You want this blackout window to last 48 hours and recur every Friday at 6:00 PM in your time zone.

Follow these steps:

1. On the Administration tab, click Service Desk, Change Orders, Change Windows.
   The Change Windows List appears.
2. Click Create New.
   The Create New Change Window page appears.
3. Complete the appropriate fields as follows:
   a. Enter **Friday_Blackout** as the window name.
   b. Select the type Blackout.

c. Select the Active status.

d. Select the upcoming Friday and 6:00 PM from the Date Helper as the Start Date.

e. Select the upcoming Sunday and 6:00 PM from the Date Helper as the End Date.

f. Select your time zone.

g. (Optional) Enter a description for the blackout window.

h. On the Recurrence Pattern tab, select Weekly.

- Set the recurrence to every **1** week.
- Select the date to end the recurrence.

4. Save and close the blackout window.

Create a Global Maintenance Window

Create a global maintenance window for your organization. For example, you do *not* want to define maintenance windows by server or CI and want to complete global changes during weekends.

Follow these steps:

1. Navigate to the Change Windows List page.
2. Click Create New.
3. The Create New Change Window page appears.
4. Enter or modify the necessary fields for the maintenance window.
5. Set Type to Maintenance.
6. Verify that the Global checkbox is checked.

A global maintenance window cannot be associated with CIs.

7. Enter Start Date, End Date, and Timezone.
8. Click Save.
   The global maintenance window is saved.

Ticket Management

Contents

A ticket can be an incident, problem, change order, issue or request

Use the Quick Profile

You can view detailed information about the contacts and organizations that make up your enterprise. Depending on your role, you can access the Quick Profile in the following ways:

- For the roles that use the Quick Profile frequently, click the Quick Profiles tab.
- For the roles that use the Quick Profile less often, select the View, Quick Profile command on the menu bar of a Scoreboard tab.
- For the roles that create new tickets using the Quick Profile, click the Quick Profile button on ticket detail pages.

You can use the Quick Profile as follows:

- Shows contact and organization information, environment, and history in the left pane.
- Display the windows for different types of contact history depending on your latest selection in the right pane.
- View the Scratchpad, which allows you to enter description information to the record you are creating in the bottom pane.

Quick Profile Scratchpad

You can use the Scratchpad Area at the bottom of the Quick Profile screen to merge information about the current user into new incidents, requests, issues, change orders, and activity logs. You can merge the text and contact information into a new record. You can also use existing templates to create records.

Note: The type of tickets that you can create from the Scratchpad Area depends on the Preferred Document setting for the Access type of the selected contact. Your administrator determines this setting. This setting also determines the type of tickets that the "Quick" button labels use in the Scratchpad Area.

The Quick Profile Scratchpad lets you perform the following tasks:

- Check the spelling of the text in the scratchpad by clicking Spelling.
- Search the knowledge base using the keywords that are entered in the scratchpad by clicking Search Knowledge.
- Clear all text from the scratchpad by clicking Clear Scratchpad.
- Create a ticket using the data from the scratchpad and immediate close the ticket by clicking Quick Close.
- Create a ticket quickly using the selected template by clicking Quick. No detail page displays, but a message indicating the results of the quick create process is displayed.
- Create a ticket by opening the detail page for the ticket type that is selected in the Type field. The text that is entered in the Scratchpad Area displays in the Description field of the new ticket, and the current contact is the Affected End User of the new ticket.

Add Activities to a Ticket

You can record all the actions that you are taking to resolve the ticket on the Activities tab. Activities can include actions such as research, calling a customer, and transferring responsibility to a different analyst. Some activities, such as "Initial" or "Field Update" are posted automatically when you create the ticket or update a field. Others, such as returning a call, changing the status, or transferring the ticket are posted when you select items from the Activities menu or from the Activities page itself.

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.
3. Open the desired ticket from the list that appears.
4. On the menu bar, click Activities, and then select one of the following options:
   - **Update Status** to update the status of the ticket.
   - **Callback** to record the time that is spent on the call.
   - **Research** to record the time spent conducting the research.
   - **Log Comment** to record your comments.
   - **Solution** to enter a description of the solution.
   - **Transfer** to reassign a problem to another technician.
   - **Escalate** to escalate the priority of a problem.
   - **Manual Notify** to send a manual notification to the user.

5. Edit the fields as appropriate. The following fields require explanation:

   - **Internal?**
     Select this check box if the activity must only be visible to internal users.

   - **Time Stamp**
     Specifies the date and time the activity began. This field shows the system date and time the activity record was opened. This field cannot be edited.

   - **Date of Activity**
     The date and time the activity was performed. Defaults to the date and time the activity record was opened, but can be changed.

   - **Time Spent**
     Specifies the amount of time that is spent on the activity. Enter this value in hours, minutes, and seconds (hh:mm:ss).

   - **Related Ticket Activity Type**
     Specifies the type of activity that is generated for a related ticket, for example, Update Status

   - **Change**
     Select an existing change order to which you want to attach the ticket.

   - **Impact**
     Indicates the effect that the record has on tasks being performed. Your system administrator can modify the default impact codes, so they can vary from one installation to another.

6. Click Save.
   The activity is recorded on the Activities tab on the ticket details page.

Provide a Reason for Escalating the Ticket

If your priority calculation settings let you change Urgency and Impact values, you provide a reason for escalating the ticket. If priority calculation is not enabled, you can edit the priority field.

Follow these steps:

1. Open a ticket, such as an Incident or a Problem.
   The Ticket Detail page appears.

2. Modify the Urgency or Impact of the ticket.

3. Click Save.
   The Escalate Detail page appears and displays the current, read-only values for Priority, Urgency, and Impact.

4. Enter a reason for why you want to change the Urgency or Impact values.

5. Click Accept.
   The ticket is modified and the activity log updates with your changes.

Send a Manual Notification to a Temporary Email Address

You can send a manual notification to a temporary email address. For example, one that is not associated with a contact record. This operation is available only if the Administrator has installed the notification_allow_temp_address Update Options (Options Manager, Notifications).

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.
3. Open the desired ticket from the list that appears.
4. On the menu bar, click Activities, Manual Notify.
   The Manual Notification page appears.
5. Complete the following field, and click Add Email.
   - **Email address**
     Specifies an SMTP address for an email recipient. You can specify temporary email addresses (for example, addresses not associated with a contact record). Separate multiple addresses with a semi-colon. This field appears only if the Administrator installed the notification_allow_temp_address Update Options (Options Manager, Notifications).

   The address is added to the Recipients list.
6. Complete the remaining fields as appropriate.

   Note: You can also add a personalized response such as a generic or administrator signature to the notification. The response is added at the end of the message text. For more information about personalized responses, see Personalized Responses (see page 2316).
7. Click Notify.
   The manual notification is sent and the activity is recorded on the Activities tab of the ticket Detail page.

Attach to Existing Change Order

You can attach an incident, problem, or request, to a related change order. Change orders are requested changes that vary from the original scope of a specific project or task.

Follow these steps:

1. On the Service Desk tab, select the incident, problem, or request to which you want to attach the change order.
   The ticket detail page appears.

2. Select Activities, Attach to Existing Change Order on the menu bar.
   The Attach Change Order to Incident page appears.

3. Click Change.
   The Change Order Search page opens.

4. Enter the search criteria that you want to use and click Search.
   A list of change orders matching the search criteria appears.

5. Select the desired change order from the list.
   The Attach Change Order to Incident page displays the selected change order number in the Change field.

   Note: If you know the Change Order number, you can type it in the Change field.

6. (Optional) Enter the comments in the Remarks field.

7. Click Attach.
   The ticket is attached to the change order, and the activity is recorded on the Activities tab on the ticket detail page.

Detach Change Order

You can end the association between an incident and an attached change order.

Follow these steps:

1. On the Service Desk tab, select the desired incident, problem, or request from which you want to detach the change order.
   The ticket detail page appears.

2. Select Activities, Detach Change Order on the menu bar.
   The Detach Change Order from Incident page appears.

3. Click Detach.
   The ticket is detached from the change order, and the activity is recorded on the Activities tab on the ticket detail page.

_Attach a Service Type Event

Contents

- Delay or Resume a Service Type Event (see page 2314)

Attach a Service Type Event

Service types determine the level of support that is given for a ticket. You can associate service type events with tickets. An event that is associated with a service type is attached to records defined with that service type.

Follow these steps:

1. On the Service Desk tab, select Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.
3. Select the desired ticket from the list that appears.
4. Choose the Service Type tab, and click Attach Service Type Event.
   OR
   Choose Actions, Attach Service Type Event.
   The Attach Service Type Event page appears.
5. Click Service Type Event.
   The Event Search page appears.
6. Complete one or more of the search fields, and click Search.
   The Event List displays the events that match your search criteria.
7. Select the desired event.
   The Attach Service Type Event page appears.
8. Click OK.
   The Delay Time field appears. The delay time indicates the interval of time after which the event occurs.
9. Specify the delay time as hh:mm:ss (hours, minutes, seconds).
   For example, if the event is attached to the incident at 2:20, and the Delay Time is 01:00:00 (one hour), the event occurs at 3:20.
10. Click OK.
    The ticket detail page appears with the event listed on the Service Type tab.

Delay or Resume a Service Type Event

You can delay and resume service type events.

Follow these steps:

1. Select the desired ticket from the list page on the Service Desk tab.
   The ticket detail page appears.
2. Select the Service Type tab.
   A list of any service type events that have been added to the ticket appears.

3. Click Delay or Resume.
   The Reason page appears.

4. Enter the reason, and click OK.
   The ticket detail page displays the Status of the event.

Create an Issue Template

You can define a ticket, such as an incident, problem, issue, change order, or request, to serve as a model for future tickets. You can then save it as a template. Tickets that are created with that template have certain fields auto-populated with your specified values.

Follow these steps:

- You can use a new ticket to create a template to be used when creating future tickets. Complete the following fields:

  1. a. On the Service Desk tab, click the File menu and select the ticket type for the template. For example, to create an incident template, click File, New Incident.

     b. Complete the ticket template fields (see page) as appropriate for the template in the page that opens.

     c. Select the Template tab at the bottom of the page.

     d. Click Save.

- You can use an existing ticket to create a template.Complete the following fields:

  1. a. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.

     b. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.

     c. Select the desired ticket from the list that appears.

     > **Note:** Some roles can only access certain ticket types through the Search menu on the Service Desk menu bar.

     d. Click Edit.

     e. (Optional) Edit the ticket template fields (see page) as appropriate.

     f. Select the Template tab at the bottom of the page.

     g. Click Save

Ticket Template Fields

Complete the following fields:

Template Name
This name appears in the list of available templates.

Template Class
(Optional) You can assign a class to the template.

Quick Template Type
You can use quick templates to define new requests on the Quick Profile Scratchpad. Select one of the following options:

- None
- Quick
- Review Before Save

Template Active
Specifies whether the template is active or inactive in the database.

Description
Describe the template settings and intended usage. This field can be used as a filter when searching for a template. Wildcard searches are supported.

Personalized Response

Personalized Responses are frequently used when you respond to customers. You can create and attach these predefined responses to all ticket types when updating activities for the record. For example, you can append personalized response information to an updated status or a logged comment.

Create a Personalized Response

Create a personalized response so that you can add them in your response to customers.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. From the Scoreboard, choose File, New Personalized Response.
   The Create New Personalized Response page displays.

2. Fill in the fields as follows:

- **Name** -- Unique identifier and key for the response. This field can be up to 50 alphanumeric characters long.
- **Response Owner** -- Name of the contact that owns the personalized response. If this field is left blank, the response is available to all analysts. Enter the contact name directly into this field, or click the search icon to search for the desired contact name.
- **Record Status** -- Indicates whether the response is Active or Inactive.
- **Response** -- The personalized response text that is delivered to the customers. This field can be up to 1000 characters long.
  You can use variables in this field, for example:
  - Ticket ref_num: @{call_req_id.ref_num}
  - Assignee: @{call_req_id.assignee.combo_name}
  - Customer: @{call_req_id.customer.combo_name}
  - Description: @{call_req_id.description}
- **Display the Response For** -- Select the type of records for which you would like this response available. By default, Requests, Change Orders, and Issues are selected. For example, if you select the Requests option, you can append this response to a Request record.

The personalized response is created.

Add Personalized Response to a Ticket

Add a personalized response when you are sending a communication to a customer about a ticket.

Note: The tickets for which personalized responses are available depend on the type of tickets that are selected when the personalized response was created. For more information, refer to CreatePersonalizedResponse (see page).

To add a personalized response to a ticket:

1. On the Service Desk tab, select Incidents, Problems, Requests, Change Orders, or Issues.

   The ticket detail page appears.

2. Open the ticket for editing.

3. From the Activities menu, select the activity for which you want to add a personalized response.
   The Create New Activity form opens. You see the Personalized Response drop-down at the end of the form.

4. Select the response that you want to add to the ticket and save the form.
   The description is automatically updated with the personalized response. You also see this response in the Log, Activities tab of the ticket.

Edit Service Targets

Service targets determine whether Service Level Agreements (SLA) have been met within the required time frame. If a service type has a set of service targets, you can view the status and deadlines for completing each target on the ticket. If necessary, you can update or override service target values such as Workshift.

Follow these steps:

1. On the Service Desk tab, select Incidents, Problems, Requests, Change Orders, or Issues.
   The ticket detail page appears.

2. Click the Service Type tab.
   Additional Service Type information appears at the bottom of the ticket.

   Note: Service targets appear on tickets that meet the conditions that the Administrator sets up. Priority calculation can be a factor in how target information calculates and displays.

3. In the Target column, click the target.
   The Service Target Detail page appears.

4. Click Edit.
   The Update Service Target page appears.

5. Complete the following fields as appropriate:

   - **Name**
     Identifies the service target.

   - **Target Duration**
     Specifies the amount of allotted time to perform the service target. You can only override this value by editing the ticket.

   - **Workshift**
     Displays the schedule to use for service target time calculations.

   - **Condition**
     Specifies the name of the condition or site-defined condition. The condition evaluates the ticket data to determine whether the service target is met.

   - **Required Outcome**
     Displays the required result of the condition or site-defined condition Macro.

- **Cost**
  Specifies the penalty that incurs for missing the target. This information also displays on the ticket.

- **Target Date/Time**
  Specifies the deadline for completing the target. If the ticket is in a Hold status or the target has been met, this field is blank.

- **Actual Date/Time**
  Specifies the date and time that the condition was satisfied or the user clicked Set Actual.

- **Time Left**
  Specifies the amount of remaining time for the service target. A negative value indicates the amount of time that exceeded the target time frame.

- **Allow Set Actual**
  Lets the users set the date and time of a service target.

- **Allow Reset Actual**
  Lets the users reset the service target.

- **Last Modified Date/Time**
  Displays the date that this ticket was last modified.

- **Service Type**
  Displays the Service Type that is attached to this service target.

- **Service Target Template**
  Specifies the name of the service target template to link to the service type.

- **Last Modified By**
  Displays the name of the last person who edited the ticket.

- **Lock Target Date/Time From Hold Recalculations**
  Prevents automatic target date and time updates when the ticket goes on hold or when the ticket is delayed.

6. Click Save.
   The system saves and updates the service target.

View Ticket Counters and Timers for Service Targets

If an analyst assigned a set of service targets to a ticket, you can view the status and deadlines for completing each target.

Follow these steps:

1. On the Service Desk tab, display a list of Incidents, Problems, Requests, Change Orders, or Issues.
   The ticket detail page appears.

2. Click the Service Type tab.
   Additional Service Type information appears at the bottom of the ticket.

3. In the Target column, click the Service Target for additional information.
   The Ticket Counters and Timers section appears near the bottom of the Assigned Service Target Detail page. The Assigned Service Target Detail page displays the following fields:

   - **Name**
     Displays the name of the service target.

   - **Target Duration**
     Displays the amount of allotted time to perform the service target. You can only override this value by editing the ticket.

   - **Workshift**
     Displays the schedule used for time calculations for the service target.

   - **Condition**
     Displays the condition or site-defined condition macro that evaluates the ticket data to determine whether the work can complete within the target time frame.

   - **Required Outcome**
     Displays the required result of the condition or site-defined condition Macro.

   - **Cost**
     Displays the penalty that incurs for missing the target. This information also displays on the ticket.

   - **Target Date/Time**
     Displays the deadline for completing the target. If the ticket is in a Hold status or the service target has been met, this field is blank.

   - **Actual Date/Time**
     Specifies the date and time that the condition was satisfied or the user clicked Set Actual.

   - **Time Left**
     Displays the amount of remaining time for the service target. A negative value indicates the amount of time that exceeded the target time frame.

   - **Allow Set Actual**
     Displays whether you can set the actual time. Yes indicates that you can set the Actual Date/Time of a Service Target. No indicates that you cannot override the Actual Date /Time.

   - **Allow Reset Actual**
     Displays whether you can restart the time. Yes indicates that you can reset the Actual Date /Time of a Service Target. No indicates that you cannot reset the Actual Date/Time.

   - **Last Modified Date/Time**
     Displays the date that this ticket was last modified.

   - **Last Modified By**
     Displays the name of the last person who edited the ticket.

   - **Service Type**
     Displays the name of the service type that attached this service target.

- **Service Target Template**
  Displays the name of the service target template that was linked to the service type that was used to create this Service Target.

- **Lock Target Date/Time From Hold Recalculations**
  Locks the Target Date/Time from being automatically updated when the ticket goes on hold or is delayed.

- **Last Start Date/Time**
  Displays the last time the service target timer was started.

- **Ticket Status**
  Displays the value of the Status field of the ticket.

- **Hold Status**
  Displays whether the ticket status has placed the ticket on hold.

- **Last Hold Date/Time**
  Displays the last time that the ticket was placed on hold.

- **Hold Count**
  Displays the number of times the ticket was placed on hold.

- **Last Resolved Date/Time**
  Displays the last time that the ticket transitioned to a resolved status.

- **Resolved Count**
  Displays the number of times that the ticket changed to resolved status.

- **Last Closed Date/Time**
  Displays the last time the ticket was changed to a closed status.

- **Closed Count**
  Displays the number of times the ticket was changed to a closed status.

- **Ticket Open Date/Time**
  Displays the date and time the ticket was opened.

- **Ticket Resolved Date/Time**
  Displays the date and time the ticket was resolved.

- **Ticket Closed Date/Time**
  Displays the date and time the ticket was closed.

View Service Target Status

On an open ticket, you can view the status for each service target. Status information such as Time Left and Violation Cost help you prioritize your work.

Follow these steps:

1. On the Service Desk tab, display a list of Incidents, Problems, Requests, Change Orders, or Issues.
   The respective ticket list displays with the following Service Target information:

   - **Service Target**
     Displays the time that the next service target is due.

   - **Projected Violation**
     Displays the incurred cost when the service type time limit is violated.

2. Select the ticket that you want from the list page.
   The ticket detail page appears.

3. Select the Service Type tab.

   Note: Service targets appear on tickets that meet the conditions that the administrator sets up. Priority calculation can be a factor in how target information calculates and displays.

   If the ticket meets predefined target conditions, the Service Targets List the following information about service targets:

   - **Action**
     Sets or resets the Actual Date/Time to the current date and time.

   - **Target**
     Specifies the current service target for the ticket.

   - **Target Date/Time**
     Specifies date and time when this service target is due. If the ticket is in a Hold status, this value is blank.

   - **Actual Date/Time**
     Specifies the time when the target condition was met. If no value appears, the target condition has not been met.

   - **Time Left**
     Specifies the amount of remaining time for the service target when the ticket is on hold. If the service target has been met, the Time Left field shows the unused time. A negative value indicates the amount of time that elapsed since the missed target date.

   - **Violation Cost**
     Displays the penalty that incurs for missing the target. This information also displays on the ticket.

Save Search Filters

This article contains the following topics:

Basic Search

You can set filter values on the search page of an object to list the corresponding details, or leave the fields blank to display all the details.

Note: If you are using multi-tenancy, a tenant drop-down list appears in the search filter. If you select <empty> from the drop-down list, the search is public.

Follow these steps:

1. Navigate to **Service Desk**, **Search**, and select any object.
   The search page related to the object is displayed.

2. (Optional) Define the required fields for your search criteria. Click **Save As** to save the filters as your personalized search.

3. Click **Search** to display the search results.

4. Click any link to view the details of that specific result in the list.

   The object details are displayed.

Search Using Personalized Filters

As an Analyst, you can save your search conditions. These saved searches are displayed on the analysts' scoreboard. You need not define the search fields for such objects need not be defined every time a search is performed. Saving the search filters enables users to update the search criteria values and save it for future use. Other analysts can also customize their scoreboards and add these saved searches.

Note: You can save a filter only for those roles for which the scoreboard appears.

By default, you can save a filter for the following objects:

- Incident

- Problems
- Requests
- Change Orders
- Issues
- Announcements
- Configuration Items
- Contacts
- Change Workflow Tasks
- Issue Workflow Tasks

By default, personalized search options are enabled. For disabling the personalized search options, see the *Enable or Disable Personalized Search Options* section below.

Follow these steps:

1. Click a saved search from **My Saved Search** in the scoreboard.
   The search results appear based on the saved search criteria.
2. (Optional) Click **Show Filter** and update the required fields for your search criteria.
3. Do any *one* of the following tasks:
   a. Click **Save** to save the updated filters.
   b. Click **Save As** to save the search with another name.
   c. Click **Search**.
      The page displays search results based on the updated search criteria.
4. Click any link to view the details of that specific result in the list.

   The object details are displayed.

Enable or Disable Personalized Search Options

As an administrator, execute the following command to disable the search options:

```
pdm_options_mgr -c -s DISABLE_SAVED_SEARCHES -v 1 -a pdm_option.inst
```

To ensure that the search options update takes effect while running the pdm_configure command, execute the following command with the **-t** option.

```
pdm_options_mgr -c -s DISABLE_SAVED_SEARCHES -v 1 -a pdm_option.inst -t
```

Add Activities to a Ticket

You can record all the actions that you are taking to resolve the ticket on the Activities tab. Activities can include actions such as research, calling a customer, and transferring responsibility to a different analyst. Some activities, such as "Initial" or "Field Update" are posted automatically when you create the ticket or update a field. Others, such as returning a call, changing the status, or transferring the ticket are posted when you select items from the Activities menu or from the Activities page itself.

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.
3. Open the desired ticket from the list that appears.
4. On the menu bar, click Activities, and then select one of the following options:
   - **Update Status** to update the status of the ticket.
   - **Callback** to record the time that is spent on the call.
   - **Research** to record the time spent conducting the research.
   - **Log Comment** to record your comments.
   - **Solution** to enter a description of the solution.
   - **Transfer** to reassign a problem to another technician.
   - **Escalate** to escalate the priority of a problem.
   - **Manual Notify** to send a manual notification to the user.
5. Edit the fields as appropriate. The following fields require explanation:
   - **Internal?**
     Select this check box if the activity must only be visible to internal users.
   - **Time Stamp**
     Specifies the date and time the activity began. This field shows the system date and time the activity record was opened. This field cannot be edited.
   - **Date of Activity**
     The date and time the activity was performed. Defaults to the date and time the activity record was opened, but can be changed.
   - **Time Spent**
     Specifies the amount of time that is spent on the activity. Enter this value in hours, minutes, and seconds (hh:mm:ss).

- **Related Ticket Activity Type**
  Specifies the type of activity that is generated for a related ticket, for example, Update Status

- **Change**
  Select an existing change order to which you want to attach the ticket.

- **Impact**
  Indicates the effect that the record has on tasks being performed. Your system administrator can modify the default impact codes, so they can vary from one installation to another.

6. Click Save.
   The activity is recorded on the Activities tab on the ticket details page.

Provide a Reason for Escalating the Ticket

If your priority calculation settings let you change Urgency and Impact values, you provide a reason for escalating the ticket. If priority calculation is not enabled, you can edit the priority field.

Follow these steps:

1. Open a ticket, such as an Incident or a Problem.
   The Ticket Detail page appears.

2. Modify the Urgency or Impact of the ticket.

3. Click Save.
   The Escalate Detail page appears and displays the current, read-only values for Priority, Urgency, and Impact.

4. Enter a reason for why you want to change the Urgency or Impact values.

5. Click Accept.
   The ticket is modified and the activity log updates with your changes.

Send a Manual Notification to a Temporary Email Address

You can send a manual notification to a temporary email address. For example, one that is not associated with a contact record.

Note: This operation is available only if the Administrator has installed the notification_allow_temp_address Update Options (Options Manager, Notifications).

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.

2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.

3. Open the desired ticket from the list that appears.

4. On the menu bar, click Activities, Manual Notify.
   The Manual Notification page appears.

5. Complete the following field, and click Add Email.

   - **Email address**
     Specifies an SMTP address for an email recipient. You can specify temporary email addresses (for example, addresses not associated with a contact record). Separate multiple addresses with a semi-colon.

   Note: This field appears only if the Administrator installed the notification_allow_temp_address Update Options (Options Manager, Notifications).
   The address is added to the Recipients list.

6. Complete the remaining fields as appropriate.

   Note: You can also add a personalized response such as a generic or administrator signature to the notification. The response is added at the end of the message text. For more information about personalized responses, see Personalized Responses (see page 2325).

7. Click Notify.
   The manual notification is sent and the activity is recorded on the Activities tab of the ticket Detail page.

Attach or Detach Change Orders

Attach to Existing Change Order

You can attach an incident, problem, or request, to a related change order. Change orders are requested changes that vary from the original scope of a specific project or task.

Follow these steps:

1. On the Service Desk tab, select the incident, problem, or request to which you want to attach the change order.
   The ticket detail page appears.

2. Select Activities, Attach to Existing Change Order on the menu bar.
   The Attach Change Order to Incident page appears.

3. Click Change.
   The Change Order Search page opens.

4. Enter the search criteria that you want to use and click Search.
   A list of change orders matching the search criteria appears.

5. Select the desired change order from the list.
   The Attach Change Order to Incident page displays the selected change order number in the Change field.

> **Note:** If you know the Change Order number, you can type it in the Change field.

6. (Optional) Enter the comments in the Remarks field.

7. Click Attach.
   The ticket is attached to the change order, and the activity is recorded on the Activities tab on the ticket detail page.

Detach Change Order

You can end the association between an incident and an attached change order.

Follow these steps:

1. On the Service Desk tab, select the desired incident, problem, or request from which you want to detach the change order.
   The ticket detail page appears.

2. Select Activities, Detach Change Order on the menu bar.
   The Detach Change Order from Incident page appears.

3. Click Detach.
   The ticket is detached from the change order, and the activity is recorded on the Activities tab on the ticket detail page.

Attach a Service Type Event

Service types determine the level of support that is given for a ticket. You can associate service type events with tickets. An event that is associated with a service type is attached to records defined with that service type.

Follow these steps:

1. On the Service Desk tab, select Incidents, Problems, Requests, Change Orders, or Issues.

2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.

3. Select the desired ticket from the list that appears.

4. Choose the Service Type tab, and click Attach Service Type Event.
   OR
   Choose Actions, Attach Service Type Event.
   The Attach Service Type Event page appears.

5. Click Service Type Event.
   The Event Search page appears.

6. Complete one or more of the search fields, and click Search.
   The Event List displays the events that match your search criteria.

7. Select the desired event.
   The Attach Service Type Event page appears.

8. Click OK.
   The Delay Time field appears. The delay time indicates the interval of time after which the event occurs.

9. Specify the delay time as hh:mm:ss (hours, minutes, seconds).
   For example, if the event is attached to the incident at 2:20, and the Delay Time is 01:00:00 (one hour), the event occurs at 3:20.

10. Click OK.
    The ticket detail page appears with the event listed on the Service Type tab.

Delay or Resume a Service Type Event

You can delay and resume service type events.

Follow these steps:

1. Select the desired ticket from the list page on the Service Desk tab.
   The ticket detail page appears.

2. Select the Service Type tab.
   A list of any service type events that have been added to the ticket appears.

3. Click Delay or Resume.
   The Reason page appears.

4. Enter the reason, and click OK.
   The ticket detail page displays the Status of the event.

Create a Parent-Child Relationship

Records that are entered in the CA SDM system can be related to other records that are entered into the system. For example, a problem could result in two more problems when you attempt to resolve the original problem. The original record is referred to as the *parent*, and the additional records are referred to as *children*.

You can record such relationships in the CA SDM system for future references. The Parent/Child tab on the ticket detail page lists the parent and children tickets of a ticket.

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.

2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.

3. Open the desired ticket from the list that appears.

4. Select the Parent/Child tab and click Update Children.
   The search page opens.

5. Complete one or more of the search fields for related ticket records, and click Search.
   A list of tickets matching the search criteria are displayed.

6. Select the related tickets from the list on the left, and click  .
   The selected tickets are added to the list on the right.

7. When all related tickets are in the list on the right, click OK.
   The detail page displays with the selected tickets listed on the Parent/Child tab.

Close All Children

You can close all the children tickets before closing the parent ticket.

Follow these steps:

1. Select the appropriate ticket type from the Scoreboard. For example, select Requests.

2. Open the parent ticket.

3. Click the Action menu and select Close All Children.

Create a Ticket Template

You can define a ticket, such as an incident, problem, issue, change order, or request, to serve as a model for future tickets. You can then save it as a template. Tickets that are created with that template have certain fields auto-populated with your specified values.

Create a Template from a New Ticket

You can use a new ticket to create a template to be used when creating future tickets.

Follow these steps:

1. On the Service Desk tab, click the File menu and select the ticket type for the template. For example, to create an incident template, click File, New Incident.

2. Complete the fields as appropriate for the template in the page that opens.

3. Select the Template tab at the bottom of the page.

4. Complete the following fields:

   Template Name
   This name appears in the list of available templates.

Template Class
(Optional) You can assign a class to the template.

Quick Template Type
You can use quick templates to define new requests on the Quick Profile Scratchpad. Select one of the following options:

- None
- Quick
- Review Before Save

Template Active
Specifies whether the template is active or inactive in the database.

Description
Describe the template settings and intended usage. This field can be used as a filter when searching for a template. Wildcard searches are supported.

5. Click Save.

Create a Template from an Existing Ticket

You can use an existing ticket to create a template.

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.
3. Select the desired ticket from the list that appears.

> **Note:** Some roles can only access certain ticket types through the Search menu on the Service Desk menu bar.

4. Click Edit.
5. (Optional) Edit the fields as appropriate.
6. Select the Template tab at the bottom of the page.
7. Complete the following fields:

Template Name
This name appears in the list of available templates.

Template Class
(Optional) You can assign a class to the template.

Quick Template Type
You can use quick templates to define new requests on the Quick Profile Scratchpad. Select one of the following options:

- None
- Quick
- Review Before Save

Template Active
Specifies whether the template is active or inactive in the database.

Description
Describe the template settings and intended usage. This field can be used as a filter when searching for a template. Wildcard searches are supported.

8. Click Save.

Create Tickets

You can create a ticket such as an incident, problem, request, issue, or change order, using various methods. This article explains these methods.

Important! Depending on your role, you do not have access to all the functionality described in this section. For example, some predefined roles can edit records but cannot create new ones.

Create a Ticket from the File Menu

You can either create a ticket from scratch or use an existing template.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Service Desk tab, click the File menu and select the ticket type that you want to create. For example, to create a request from scratch, click File, New Request. To create a request from a template, Click File, New Request from Template.

2. Fill in the fields as appropriate for the ticket. See the field definitions at the end of this page. Use the controls available on the tabs at the bottom of this page to process the ticket as appropriate.

3. Click one of the following buttons:

   Save -- Saves the incident and closes the page.

   Auto Assign -- Triggers an auto assignment task, and updates the activity log.

   Note: This button appears only when the ticket specifies a category or area that has auto-assignment enabled.
   Create Change Order -- Opens the Create New Change Order page. You can create a change order ticket that is associated with this incident.**Note:** This button appears only when you create incidents, problems, and requests.

   Create Problem -- Opens the Create New Problem page so you can create a problem ticket associated with this incident.**Note:** This button appears only when you create incidents and requests.

   Create Incident – Opens the Create New Incident page so you can create an associated incident ticket.**Note:** This button appears only when you create change orders and requests.

   Reset -- Resets all fields to the last saved values.

   Find Similar -- Opens the Find Similar page to search for similar problems.**Quick Profile --** Displays the contact information for the specified user in the **Affected End User** field. You can also view their environment details and their entire ticket history.

   Use Template -- Displays a list of available templates for the selected ticket type. You can select the template that you want to use for creating this ticket.

Create a Ticket Using Quick Profile

You can use the Quick Profile to identify a contact to be the affected end user of your new ticket. Quick Profile allows you to search for a contact, and view the history of the issues, requests, change orders, incidents, and problems that are assigned to that contact. When you have identified a contact, you can create the incident ticket directly from the Quick Profile.

Follow these steps:

1. Select View, Quick Profile on the menu bar of the Scoreboard.
   The Quick Profile Contact Search window opens.

2. (Optional) Complete one or more of the filter fields to list only the contacts of interest.

3. Click Search.
   Note: All search fields that allow text entry support use of the % wildcard character.
   The Quick Profile Contact List page lists the contacts that match your search criteria.

4. Select the user who is the affected end user of the new ticket.
   The contact pane displays contact information and the ticket history for the contact.

5. In the Scratchpad pane, do the following actions:
    a. Enter a description for the new record in the Scratchpad text field.
    b. Select the ticket type from the Type drop-down list.
    c. (Optional) Enter a Template name for the new record. You can enter a value directly or click the search icon to search for available templates.
6. Click New.
   A new window opens and displays the information that you entered in the Scratchpad.
7. Complete the empty fields as appropriate.
   See the field definitions at the end of this page.
8. Use the controls available on the tabs at the bottom of this page to process the ticket as appropriate.

Add Attachments to Tickets

You can attach a document or a link to a URL to a ticket. The document or URL provides more explanation or justification for the report.

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.
3. Open the desired ticket from the list that appears.
4. Select the Attachments tab, and then click one of the following options:
    - Attach Document
    - Attach URL
5. Follow the on-screen instructions to attach a file or URL to the incident.
   The URL or the document is added to the record and is listed on the Attachments tab of the Incident Detail page.

View Tickets

You can view summary information for tickets after you create them.

If you are using multi-tenancy, a tenant drop-down list appears in the search filter. If you select <empty> in this drop-down list, the search is public.

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.
3. Select the folder for the tickets that you want to see.
4. (Optional) Click Show Filter and complete one or more of the fields to specify search criteria that restricts the list to the tickets of interest.
5. Click Search.
   The search result displays the tickets that match the criteria.
6. Click the ticket # link to view the incident of interest.
   The detail page appears.

Use Knowledge to Resolve a Ticket

You can search the CA SDM Knowledge Base to help resolve a ticket, such as an incident, problem, request, issue, or change order.

Follow these steps:

1. On the Service Desk tab, browse to the ticket type such as, Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.
3. Open the desired ticket from the list that appears.
4. Select the **Knowledge Management** tab.
5. Enter text in the search field to describe the problem, or copy text from the **Summary** or **Description** fields of the ticket.
6. From the drop-down list, select where you want to search.
7. Click **Search**.
   A list of documents matching the search criteria displays.
8. Look for the document that provides the solution to your ticket.
9. Right-click the document and select **Accept as Solution**.
   The knowledge document information is copied into the **Summary** and **Description** fields.

Submit a Knowledge Document

When you log a solution activity for a ticket, you can submit the solution to the knowledge base administrator as a candidate for publication.

Follow these steps:

1. Open a ticket, such as an Incident.
   The ticket detail page appears.

2. On the Knowledge tab, click Submit Knowledge.
   The Create New Document page displays.

For more information on creating knowledge documents, refer to Create Knowledge Documents (see page 2732).

After you submit a solution to the knowledge base, it becomes a candidate for publication in the knowledge base. A Knowledge Management administrator reviews the information and publishes it if it is deemed appropriate and accurate. After it is published, the information becomes available to other users.

View Events

The Event List contains a record of the events that are associated with the ticket. Your administrator maintains events, or procedures the system perform after a certain amount of time has elapsed. For example, an event might send a message to an analyst if a Priority 1 ticket is not resolved within an hour.

Follow these steps:

1. On the Service Desk tab, select Incidents, Problems, Requests, Change Orders, or Issues.

2. Navigate to Assigned or Unassigned, and select the priority for the desired ticket.

3. Select the desired ticket from the list that appears.

4. Click the Event Log tab at the bottom of the details page.
   A list of events for this incident appears.

View the Event History

You can view the event history for a ticket to see what actions have been performed to resolve the ticket.

Follow these steps:

1. On the Service Desk tab, select Incidents, Problems, Requests, Change Orders, or Issues.

2. Navigate to Assigned or Unassigned, and select the priority level for the desired ticket.

3. Select the desired ticket from the list that appears.

4. Select View, Event History on the detail page menu bar.
   The Event History window displays the following fields:

- **Condition**
  Indicates the condition checked for by the event. CA SDM provides macros that check for standard conditions such as priorities and object status (open or closed).

- **Event**
  Indicates the name of event that is associated with this row in the Event History list.

- **Status**
  Indicates whether the event is active or inactive.

- **Check Time**
  Indicates the time that the event was checked, based on time parameters that are specified in the event configuration.

- **Time Loaded**
  Indicates the time that the event was loaded, based on time parameters that are specified in the event configuration.

View the Event Delay History

You can view the event delay history for a ticket to see descriptions of the service type event delays. Service type event delays let you suspend a service type event to prevent a service level violation.

Follow these steps:

1. On the Service Desk tab, select Incidents, Problems, Requests, Change Orders, or Issues.
2. Navigate to Assigned or Unassigned, and select the priority level for the desired ticket.
3. Select the desired ticket from the list that appears.
4. Select View, Event Delay History on the detail page menu bar.
   The Event Delay History window displays the following fields:

   - **Start Time**
     Indicates the date and time the delay began.

   - **Stop Time**
     Indicates the date and time the delay ended.

   - **Actual Delay**
     Indicates the actual duration of delay.

   - **Effective Delay**
     Indicates the effective duration of delay.

   - **Service Type**
     Defines the support level that is assigned to the ticket (for example, four-hour service requirement).

Event Logs

The Event Log displays significant actions that are performed by the user, such as on tickets. For example, you submit a Knowledge Document and link it to an Incident. The Incident logs a failed status transition or detected Change Conflict. In this example, the Contact detail can display the following types of information:

- The log displays the time that the user logged in to CA SDM and when they closed the session.
- The user accepted the Terms of Usage.
- The user created a Knowledge Document.
- The user created a ticket, such as an Incident, Problem, Request, or Change Order.
- The user used a Knowledge Document to avoid creating a ticket.

Asset Management

This section contains the following articles:

Audit History

An *audit history* is a chronological list of changes that are made to an object record over time. Auditing records all changes that are made to each field in an object record. CA APM lets you use an audit history to view a list of changes that are made to a record.

You can use an audit history to see the changes that are made to the value of a particular field. You can also see who changed the value. If a field contains an incorrect entry or value, use the audit history to verify the last correct value and update the object record.

The following objects enable auditing by default and without any additional configuration:

- Models (including Model Pricing)
- Assets

- Companies
- Contacts
- Organizations
- Locations
- Sites
- Legal Documents (including Terms and Conditions)
- Legal Assets (including Terms and Conditions)
- Costs
- Payments
- Relationships
- Asset Configurations (Models and Assets)
- Software Internal Allocations (Locations, Companies, Contacts, and Assets)

View an Audit History of Object Changes

You can view an audit history for an object record to see the changes that are made to the record. The audit history maintains and displays the historical information of the changes that are made to an object.

Example: Review the Audit History to Change the Cost Center

In this example, a line manager discovers that the incorrect department is being charged for a laptop. The line manager investigates the situation and determines that the laptop is assigned to the incorrect cost center. To understand how this error occurred, the line manager configures and filters the audit history search criteria and results for the laptop to include the cost center. The line manager reviews the audit history for a specific time period to determine when the cost center value changed and who changed the value. The line manager contacts the asset manager to have the cost center changed to the correct value.

Follow these steps:

1. Click the tab and optional subtab for the object for which you want to view an audit history.
2. Search to find the list of available objects.
3. Click the object in the search results for which you want to view an audit history.
4. Click View Audit History.

   All changes that are made to the object record appear.
5. (Optional) To view the audit history for a relationship, complete the following steps:

a. Select the relationship (for example, Image Partitions).

b. Click the Edit Record icon, and click View Audit History.

6. (Optional) Complete any of the following steps in the Search Criteria to filter the audit history search results:

   a. Select a specific field in the Target Field drop-down list and click Go.
   The Search Results are limited to the field that you select. In addition, the standard auditing fields identify the user who changed the field and the type and date of change.

   b. Select the Highlight Changes check box and click Go.
   The Search Results highlight changes in adjacent rows. You can use this check box, in combination with a specific field in the Target Field drop-down list, to identify field-level changes that need correction.

7. Export the audit history to a CSV file or to return to the object details, click the hyperlink.

View an Audit History of Events

CA APM lets you view an audit history of all events that are created for an object. For example, you define a date event on the Terminate Date field for a legal document and a notification for the event is sent to the appropriate person on 3/1/2010. The audit history maintains and displays the event history for an object.

Follow these steps:

1. Click the tab and optional subtab for the object for which you want to view an audit history.

2. Search to find the list of available objects.

3. Click the object in the search results for which you want to view an audit history.

4. Click View Audit History.
   All changes that are made to the object record appear.

5. In the audit history results, click the icon in the Event History column.
   All events and their associated status (see page 2340) that is created for the audit record appear.

Event Status

When you view an audit history of events, you can see the associated status for each event.

Event Status	Description
Unprocessed	CA APM has created the event. However, the event has not been processed to map the workflow process attributes for notifications in CA Process Automation.
Started	The mapping for the workflow process attributes in CA Process Automation is complete. The associated notification process for the event has started.

Event Status	Description
In Progress	The CA Process Automation notification process for the event is processing.
Completed	The CA Process Automation notification process for the event is completed.
Failed	The CA Process Automation notification process for the event has failed.
Aborted	The CA Process Automation notification process for the event has stopped.

Contract Management

After you negotiate contracts with your vendors, the supporting documentation is frequently archived and the terms are forgotten. Making contract information easily accessible lets you properly administer the terms of an agreement. CA APM lets you manage legal documents and standardize on terms and conditions for reporting and analysis. You can see the relationships between agreements and costs associated with vendor contracts to understand the financial impact. Finally, CA APM lets you attach electronic files or URL pages containing supporting documentation to objects, such as contract profiles, to quickly access the original document.

Contract management in CA APM involves working with the following objects:

- Legal documents (see page 2341)
- Terms and conditions (see page 2347)
- Attachments (see page 2349)

Legal Documents

This article contains the following topics:

A *legal document* describes a legal relationship or agreement between two or more parties. For example, contracts, notification letters, master agreements, lease agreements, volume purchase agreements, additions to agreements, letters of intent to purchase, and so forth, are all considered legal documents.

Legal document records are based on legal templates, which your CA APM administrator defines. When you define a legal document, you start by selecting the appropriate template. Templates provide fields that apply to specific types of legal documents. Regardless of the legal template you use, you can use legal documents to track the following information:

- Record information about parties to the legal document, both primary and other parties.
- Create relationships to associate related records (for example, to associate an amendment to its original agreement).
- Store attachments with your legal document record (for example, a scanned image of a document).
- Record associated cost information.

You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

Manage Legal Documents

You can define, update, or delete a legal document. For example, you can define a legal document for a contract or negotiation letter, or you can change the termination date for an equipment lease. You can delete a contract or lease agreement that has expired. You cannot delete a legal document that is associated with an asset.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click Legal Document.
2. Perform one of the following actions.
3. Define a legal document.
    a. Click New Legal Document.
    b. Enter the legal document information.
    c. Click Save.

Note: You can also define a legal document by copying an existing legal document, supplying a new name, changing the information, and saving the new legal document.

4. Update a legal document.
    a. Search to find the list of available legal documents.
    b. Click the legal document that you want to update.
    c. Enter the new information for the legal document.
    d. Click Save.

    Note: You can also view the details for an object that is related to your legal document, if the related object has a Browse icon. When you click the Browse icon, you leave the legal document page and you navigate to the related object page. To keep the legal document page in view and preserve the legal document information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.

5. Delete a legal document.
    a. Search to find the list of available legal documents.
    b. Click the legal document that you want to delete.
    c. Click Delete and confirm that you want to delete the legal document.

Associate a Governing Legal Document with a Legal Document

A governing legal document is the document on which a legal document is based. CA APM lets you associate a governing legal document with the legal documents on which it is based. This association is useful when tracking the source of the legal terms and conditions of a legal document.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Legal Document.
2. Search to find the list of available legal documents.
3. Click the legal document to which you want to associate a governing legal document.
4. On the left, expand Relationships and click Governing Legal Document.
5. Click Select New and select a different legal document, other than the legal document previously selected.

6. Click Save.
   The governing document is associated with the legal document.

Track Amendments to a Legal Document

CA APM lets you create and track amendments that have been made to a legal document. Save the amendments as a separate legal document and associate the amendments with the parent legal document.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Legal Document.
2. Search to find the list of available legal documents.
3. Click the legal document for which you want to enter amendment details.
4. On the left, expand Relationships and click Legal Amendment.
5. Click Select New and select a different legal document, other than the legal document previously selected.
6. Click Save.
   The amendment details are saved.

Associate an Asset with a Legal Document

CA APM lets you associate assets and legal documents to identify the assets that a legal document covers. Initiate this association from either the legal document or asset. You can associate multiple assets to a single legal document and multiple legal documents to a single asset.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Legal Document.
2. Search to find the list of available legal documents.
3. Click the legal document that you want to associate with an asset.
4. On the left, expand Relationships and click Legal Asset.

5. Click Select New in the Legal Asset section, search for and select an asset.
   The asset name appears.

6. Click Save.
   The asset is associated with the legal document.

Add and Remove Asset Legal Document Terms and Conditions

Terms and conditions are specific areas of agreement that are defined in legal documents. For example, legal documents can have terms and conditions for a multi-product discount, a new pricing model, copyright protection, and so forth. After you associate an asset with a legal document, CA APM lets you add or remove terms and conditions for the asset legal document from the Asset or the Legal Document page.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Legal Document.

2. Search to find the list of available legal documents.

3. Click the legal document for which you want to add or remove terms and conditions.

4. On the left, expand Relationships and click Legal Asset.

5. Click the Edit Record icon for the asset for which you want to add or remove terms and conditions.

6. Click View Assigned T's & C's.

7. Select one of the following options:

   - Click Select New for the date-specific or non-date-specific T's and C's to add to the asset legal document.

   - Click the Mark for Deletion icon for the terms and conditions that you want to remove from the asset legal document.

8. Click Save.
   The terms and conditions are added or removed.

   For more information about defining date-specific and non-date-specific terms and conditions for legal documents, see Define Legal Document Terms and Conditions (see page 1535).

Associate a Legal Party with a Legal Document

CA APM lets you associate the people and entities involved in creating a legal document to the document record. For example, you can associate the lawyers and the law firm as legal parties for the legal document.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Legal Document.
2. Search to find the list of legal documents.
3. Click the legal document for which you want to associate a legal party.
4. On the left, expand Relationships and click Legal Party.
5. Click Select New to search for and select a company.
6. Click Save.
   The company is defined as the legal party.

Make an Obsolete Legal Document Inactive

As a best practice, change the status of an obsolete legal document to inactive rather than deleting the legal document. We recommend this approach because when you delete a legal document record, the historical information for the legal document is permanently removed from the repository. In this way, you retain the legal document information for future reporting and reference.

Follow these steps:

1. Click Legal Document.
2. Search to find the list of available legal documents.
3. Click the legal document that you want to make inactive.
4. Select the Inactive check box.
5. Click Save.
   The legal document status is changed to inactive.

Assign and Track the Status of a Legal Document

CA APM lets you assign and track the status of a legal document. For example, if the document has been signed, assign the status as executed. You can track the changes in the status of a legal document over time. The status identifies the stage of completion or implementation of the legal document.

Follow these steps:

1. Click Legal Document.
2. Search to find the list of available legal documents.
3. Click the legal document for which you want to track the status.
   The legal document details appear. The status details are available in the Status section.
4. Click New in the Status section.
5. Specify the new status for the legal document.
6. Select the Current check box to indicate that the selected status is the current status of the legal document.
7. Click Save.
   The status is updated and the previous status is added to a chronological status list for the legal document. As a best practice, change the current status each time the status of a legal document changes. Only one status can be entered as the current status of a legal document. All dates are automatically updated.

Terms and Conditions

This article contains the following topics:

Terms and conditions are areas of agreement specified in legal documents. CA APM lets you track terms and conditions for the following reasons:

- To enforce order or comply with an existing legal document.
- To negotiate future legal documents.

Administrators and users with appropriate privileges create and maintain a master list of terms and conditions. When you work with legal documents, you use terms and conditions from this list. You can assign terms and conditions when you define legal document records or asset records.

When you define a legal document record, you start by selecting a legal template. The legal template contains the terms and conditions that typically apply to the legal document type. You can update the terms and conditions provided by the legal template to help ensure that the legal document record contains only the terms and conditions that apply.

A master terms and conditions list must exist in your repository before you can assign terms and conditions to your legal templates. You can assign a term or condition to one or more legal templates and legal document records.

Terms and conditions can be date-specific or non-date-specific. Date-specific terms and conditions include information about the start and end dates. For example, if one of your terms and conditions is Installation Date, you can have start and end date information included about the Installation Date.

You determine which terms and conditions are date-specific when you create new terms and conditions in Directory, List Management.
For more information about defining date-specific and non-date-specific terms and conditions for legal documents, see Define Legal Document Terms and Conditions (see page 1535).

We recommend that you do not include the following terms and conditions in your master list:

- Effective and termination dates, as they are recorded directly on legal document records.
- Cost-related terms and conditions, as they are recorded directly on cost records.
- Software licensing terms, as they are recorded on license records.

Note: When you define an asset, you can associate the asset to the legal document records that govern the asset. The terms and conditions that apply to the legal documents also apply to the asset. If a particular asset requires terms and conditions that the legal documents do not provide, you can change the terms as you associate the asset and legal document. The legal documents covering a particular asset must contain the terms and conditions that apply only to the asset.

Add and Remove Legal Document Terms and Conditions

Terms and conditions are specific areas of agreement that are defined in legal documents. For example, legal documents can have terms and conditions for a multi-product discount, a new pricing model, or a copyright protection. CA APM lets you add the terms and conditions that are required in a legal document and remove any that are inherited from the legal template but are not required in the legal document.

Note: After you associate an asset with a legal document, you can add or remove terms and conditions for the legal document from the Asset or Legal Document page.

Follow these steps:

1. Click Legal Document.
2. Search to find the list of available legal documents.
3. Click the legal document for which you want to add or remove terms and conditions.
4. On the left, click T's and C's.
5. Select one of the following options:
   - Click Select New for the date-specific or non-date-specific T's and C's to add to the legal document.

- Click the Mark for Deletion icon for the terms and conditions that you want to remove from the legal document.

6. Click Save.
   The terms and conditions are added or removed for the legal document.

For more information about defining date-specific and non-date-specific terms and conditions for legal documents, see Define Legal Document Terms and Conditions (see page 1535).

Manage an Attachment

Attachments are electronic files or URL pages containing supporting documentation that you associate with an object. For example, you can add an attachment of a scanned contract to the legal document record that represents the contract.

You can use the following types of attachments:

- **Web URL**. Provides direct access to the page specified in the URL. When you add this type of attachment, include the prefix http:// for the link to work correctly.
- **File**. Provides direct access to a file. The file opens using the default program for the file type. At the time that you create this attachment type, the file is copied from your file system to the file system on a CA APM server.

You can add attachments to the following objects:

- Model
- Asset
- Legal Document
- Contact
- Company
- Organization
- Location

You can add, update, and delete an attachment for an object. The following examples illustrate how you can manage an attachment:

- You can attach a scanned copy of an invoice to record all assets that are listed on the invoice.
- You can edit the URL to a scanned copy of an invoice if the location has changed.

When you delete an attachment, you delete only the reference to the attachment in the object record. If the deleted attachment is a file, the file remains in the file system on the CA APM server.

Follow these steps:

1. Click the tab and optional subtab for the object for which you want to manage an attachment.

2. Search to find the list of available objects.
3. Click the object for which you want to manage an attachment.
4. On the left, click Attachments.
5. **Add an Attachment.** Follow these steps:
    a. Click New.
    b. Complete the required information.
    c. In the File Path field, select a file from your local server, or enter a URL for the new attachment. For a URL, include the following prefix:

    ```
    http://
    ```

    If you are adding a file attachment, your selected file is copied to a CA APM server. This copy activity can take a few moments to complete. Wait for the file to finish copying before you click Save.

    Important! The file size is limited by the product environmental settings. For more information, contact your administrator or CA Support.

    Note: If you select a file that exists on the server, you are prompted to overwrite the existing file. Click Yes to overwrite the file, click No to use the existing file on the server, or click Cancel to clear the file selection.

6. **Update an Attachment.** Follow these steps:
    a. Click the Edit Record icon for the attachment.
    b. Change the information for the attachment.

    Note: For a file attachment, you can update the name and description for the attachment record. However, to update the file for a file attachment, you delete the existing attachment record and add a new attachment with a new file.

7. **Delete an Attachment.** Click the Mark for Deletion icon next to the attachment.
8. Click Save.
   The attachment is added, updated, or deleted.

Financial Management

Understanding the financial impact of your asset base lets you decide what costs are relevant to your business. CA APM helps you track, manage, and categorize all asset-related expenditures, including historical, current, and projected costs, so that you can analyze their financial impact.

Financial management in CA APM involves working with the following objects:

- Models (see page 2351)
- Assets (see page 2355)
- Asset Configurations (see page 2367)
- Costs and Payments (see page 2371)
- Events and Notifications (see page 2376)
- Notes (see page 2402)

Models

This article contains the following topics:

The repository contains two types of records that describe the basic characteristics of IT products:

- A *model* describes a product type that you have purchased or might purchase.
- An *asset*, which is based on a model, describes a product that you own or plan to acquire. You can create many assets that are based on a single model, and the new asset inherits the model attributes. For example, if you own 100 laptops of a particular model, you would have one model record describing the laptop and 100 asset records describing the individual laptops.

A model can be any of the following examples:

- A *computer model* such as Dell Optiplex GX270 and Dell Precision 410.
- A *hardware component* such as 104+ keyboard, 256 MB-RAM, Monitors, and Intel Pentium processor.

You manage *hardware models* to describe the following models:

- Configurations that the manufacturer offers.
- Substitutions or additions that you typically make to the configurations when you purchase them.

Each model configuration is composed of links between the models and their component model records (such as a monitor and a keyboard).

You can have some products that you want to group together to manage as models, such as the following examples:

- Standard, relatively inexpensive computer components in a configuration. For example, you can record a particular type of network card as a model. This model lets you determine which systems are using that type of network card without tracking details about individual network cards of that type. Other similar components include SCSI hard drives, memory, graphics cards, and CD or DVD devices.
- Products that your company purchases from different vendors at different times. This additional information lets you track pricing information for those products and select the best price.

Define models first in the repository for each asset that you want to manage. After you define a model, the model acts like a template for the physical assets that are created. The assets inherit the properties or attributes from the model, such as the name, asset family, and manufacturer. By using this template, a single model can represent many assets and the model information is common to many assets. However, each asset record contains information specific to that asset.

Manage Models

Managing models includes defining, updating, and deleting models for an asset. For example, you define Dell Precision Workstation 410 as a model to describe the workstation.

Follow these steps:

1. Click Model.
2. Perform one of the following actions.
3. **Define a model.**
    a. Click New Model.
    b. Enter the model information.

    Note: You can also define a model by copying an existing model, supplying a new name, changing the model information, and saving the new model.

4. **Update a model.**
    a. Search for the list of available models.
    b. Click the model that you want to update.
    c. Enter the new information for the model.

Note: You can also view the details for an object that is related to your model, if the related object has a Browse icon. When you click the Browse icon, you leave the model page and you navigate to the related object page. To keep the model page in view and preserve the model information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.

5. **Delete a model.**
   a. Search for the list of available models.
   b. Click the model that you want to delete.
   c. Click Delete and confirm that you want to delete the model.
6. Click Save.

Define an Asset from a Model

You define an asset, which is based on a model, to describe a product that you own or plan to acquire. For example, you have defined Dell Precision Workstation 410 as a model. Your enterprise has purchased 100 individual computers, and you define 100 asset records that are based on the model to describe the individual computers.

Note: You cannot define an asset from a model that does not have an asset family.

Follow these steps:

1. Click Model, New Model.
2. Enter the model information with a valid asset family.
3. Click Save.
   The model is defined.
4. Click the Create Asset hyperlink.
5. Enter the asset-specific information.
6. Click Save.

Make an Obsolete Model Inactive

As a best practice, change the status of an obsolete model to inactive rather than deleting the model. For example, after replacing all Dell Precision Workstation 410 computers with laptops, you can change the status of the associated model to inactive.

We recommend this approach because deleting a model record permanently removes the historical information from the repository. Changing the status to inactive lets you retain the model information for future reporting and reference.

Note: Changing the status to inactive has no impact on the assets that are based on the model. If you want the assets to be inactive, search for the assets that are based on the model and manually indicate that they are inactive.

Follow these steps:

1. Click Model and search for the list of available models.
2. Click the model that you want to make inactive and select the Inactive check box.
3. Click Save.

Change a Model Asset Family

You can change the asset family of selected models. For example, you realize that a set of related computer models were imported into the product using the hardware asset family. You search for these models and select them. Then you can change the asset family for all selected models simultaneously.

Note: When you change the asset family for a model, the asset family is also changed for the associated assets.

Follow these steps:

1. Click Model.
2. Click Change Model Asset Family under Mass Change Utilities on the left.
3. Select the original asset family and the new asset family.

   Note: If the original asset family has extended fields that the new asset family does not have, a warning message and a check box appear. To proceed with changing the model asset family, select the check box Check to change model to new asset family. The extended fields are lost. To avoid the data loss, define the extended fields for the new asset family before you change the model asset family.

4. Click Go.
   All models that have the original asset family are listed in the Search results.

5. Select either the individual models that you want to change or all models.

6. Select a class for the models using one of the following actions:

   - Select the Assign a Single Class to All Models check box and select a class if you want to apply the same class to all selected models.

   - Select the class for each individual selected model.

7. Click Change Model Asset Family.
   Your request is submitted.

8. Click View Mass Change Utilities Progress to see the status of your job and verify completion.

Add Components in a Model Configuration

You associate a hardware model to its component models to define a model configuration. A generic model is a model that is not acquired as an asset, for example, keyboards and network cards. Generic models comprise a model configuration. This configuration is available to the inherited assets from the model.

Follow these steps:

1. Click Model and search for the list of available models.

2. Click the model for which you want to add components.

3. Expand Configurations on the left and click Model Configuration.

4. Click Select New, search for and select a model.

5. Click the Edit Record icon next to the model name to define the association between the hardware model and model components.

6. Click Save.

Assets

This article contains the following topics:

An *asset* is an IT product that you own or plan to acquire. Assets represent physical products with unique identifiers such as a serial number, a configuration, or a contact. You define assets that are based on a model and the information specific to the asset is added to the asset record. Define an asset record when you want to track cost, legal, and other ownership purposes of an asset.

You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

Note: The search results only include assets that CA APM manages. If your repository contains assets that the product does not manage, those assets do not appear in the asset search results.

You can assign one lifecycle status to an asset to indicate its availability. If your administrator configured the asset search to include the Lifecycle Status field, you can retrieve information about assets based on the status.

Best Practices for Tracking Assets

When you manage assets, we recommend the following best practices:

- Enter useful information for cost, productivity, and decision making.
- If you cannot think of an immediate need, reconsider tracking the information.
- Keep the information accurate and up-to-date. If the information becomes outdated and obsolete, you do not know what information to trust. As a result, you can make incorrect purchasing and business decisions.
- Track expensive products and key components (such as system units, mainframes, large devices, printers, and monitors) as assets. Do not maintain information about IT assets that are not important when making purchasing and business decisions.
- Track a product as an asset only if you want to know the detailed information (such as the cost, serial number, bar code number, location) about each instance of that product. For example, if you want to know the location of each monitor of a particular model being used, or the cost of each monitor of a model.
- If you are using a discovery product to track the usage of hardware or software products, consider the following information:

- The discovery product, instead of CA APM, tracks the product types.
- The product types that the discovery product and CA APM must track support a comparison of usage and ownership information.

Asset Families

You can classify assets and models that are based on an asset family. An *asset family* is a way to organize and classify assets to track specialized information about products, services, or equipment that you use. The asset family determines the information that you see on the page when you enter an asset.

The product provides a set of predefined asset families, such as computer, hardware, other, projects, service, and software. Your administrator can create user-defined asset families based on the internal structure of your organization. When you define an asset, select either a predefined asset family or a user-defined asset family.

For each asset family, you can create a hierarchy to track an asset to a precise location. Assets inherit the asset family from the model records on which they are based.

Asset Classification

Asset classification helps reduce the number of records that are returned in searches and reports. When you define a model and asset, you can classify the objects by asset family. You can further classify models and assets in the following ways:

- **Class**. Broadly categorizes the product, such as a printer.
- **Subclass**. Provides additional refinement, such as inkjet or laser printer.

Assets inherit class and subclass assignments from the models on which they are based. Consider the following information when classifying assets:

- If you change the class and subclass for a model, the change is not automatically made to saved assets based on the model. The changes are not retroactive.
- You can change the class or subclass that an asset inherits from the model.

Manage Assets

You can add information about each asset to the repository so that you can manage assets throughout their lifecycle. Assets are defined based on models, and inherit data from the selected model. For example, you have defined Dell Precision Workstation 410 as a model. Your enterprise has purchased 100 individual computers, and you define 100 asset records that are based on the model to describe the individual computers.

Follow these steps:

1. Click Asset and perform one of the following actions.
   - **To define an asset, complete the following steps:**
     a. Click New Asset.

b. Enter the asset information.

c. Associate the asset with other objects such as contacts, organizations, and companies.
Associating assets with other objects enables data access to roles or users when you implement multi-tenancy.

Note: You can also define an asset by copying an existing asset, supplying a new name, changing the asset information, and saving the new asset.

- **To copy an asset, complete the following steps:**

  a. Search for the list of available assets.

  b. Click the asset that you want to copy.

  c. Click Copy.

  The Asset Copy wizard appears.

  d. Follow the on-screen instructions to define unique assets and to specify the data that you want to copy to the new assets.

  e. Click Finish when you have completed the wizard.

  f. Click Close and then click Save.

- **To update an asset, complete the following steps:**

  a. Search for the list of available assets.

  b. Click the asset that you want to update.

  c. Enter the new information for the asset.

Note: You can also view and edit an object that is related to your asset, if the related object has a Browse icon. When you click the Browse icon, you leave the asset page and you navigate to the related object page. To keep the asset page in view and preserve the asset information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished.

- **To delete an asset, complete the following steps:**

  a. Search for the list of available assets.

  b. Click the asset that you want to delete.

  c. Click Delete and confirm that you want to delete the asset.

Note: If the CI check box is selected (on the Asset Details page) for the asset you want to delete, you cannot delete the asset. The selected CI check box indicates that CA Service Desk Manager manages the asset. Delete the asset from CA Service Desk Manager.

Important! We do not recommend that you delete an asset because the audit history for the asset is permanently removed. For example, legal, cost, relationship, and other information that is related to the asset is also deleted. Instead, update the asset status to indicate that the asset has been disposed of, or is *obsolete*. Using this approach, you retain the information about the asset in your repository for future reporting and reference purposes.

2. Click Save.

Add an Asset that CMDB Manages

You can add assets to your repository that CMDB manages. CMDB is integrated with CA Service Desk Manager. After you add an asset that CMDB manages, you can then open CA Service Desk Manager from CA APM and view and manage the asset.

Note: You can also create a configuration item (CI) in CMDB and then view it as an asset in CA APM. For more information about creating a configuration item, see Configuration Items (see page 2470).

Important! You cannot delete an asset in CA APM that CMDB manages. You can only delete assets in CA APM that CA APM manages.

Follow these steps:

1. Click Asset, New Asset.
2. Enter the asset information.
3. Select the CI check box to have CMDB and CA Service Desk Manager manage the asset.

   Important! After you save an asset with the CI check box selected, you cannot update the asset to clear the CI check box.

4. Associate the asset with other objects such as contacts, organizations, and companies. This approach enables specific data access to roles or users when you implement multi-tenancy.
5. Click Save.

6. (Optional) View the new asset in CA Service Desk Manager by clicking the CMDB hyperlink at the top of the page.

7. Log in to CA Service Desk Manager.
   A CA Service Desk Manager window opens and the details of the selected asset appear.

Associate a Legal Document with an Asset

You associate assets and legal documents to identify the assets that a legal document covers. For example, you associate a volume purchase agreement with 100 laptops. Initiate this association from either the legal document or asset. You can associate multiple assets to a single legal document and multiple legal documents to a single asset.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Asset.

2. Search to find the list of available assets.

3. Click the asset that you want to associate with a legal document.

4. Expand Relationships (on the left) and click Legal Documents.

5. Click Select New in the Legal Document section, search for and select a legal document.

6. Click Save.

Add and Remove Asset Legal Document Terms and Conditions

Terms and conditions are specific areas of agreement that are defined in legal documents. For example, legal documents can have terms and conditions for a multiproduct discount, a new pricing model, or copyright protection. After you associate a legal document with an asset, add or remove terms and conditions for the asset legal document from the Asset or Legal Document page.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Asset.

2. Search for the list of available assets.

3. Click the asset for which you want to add or remove legal document terms and conditions.

4. Expand Relationships (on the left) and click Legal Documents.
5. Click the Edit Record icon for the legal document for which you want to add or remove terms and conditions.
6. Click View Assigned T's & C's.
7. Select one of the following options:
   - Click Select New for the date-specific or non-date-specific terms and conditions to add to the asset legal document.
   - Click the Mark for Deletion icon for the terms and conditions that you want to remove from the asset legal document.
8. Click Save.

Change an Asset Model

You can change the model for selected assets. For example, you identified 15 assets that were entered into the product with an incorrect server model. You search for the assets and select them. You then can change the server model for all selected assets simultaneously.

Follow these steps:

1. Click Asset.
2. Click Change Asset Model under Mass Change Utilities on the left.
3. Select the original model and the new model and click Go.
   All assets that have the original model are listed in the Search results. If you do not select an original model, all assets that do not have models are listed.

   Note: If the original model asset family has extended fields that the new model asset family does not have, a warning message appears. If you proceed with changing the asset model, the extended fields are lost. To avoid the data loss, define the extended fields for the new model asset family before you change the asset model.

4. (Optional) Select Assign Model Class to All Assets if you want all the listed assets to use the new model class.

   Note: This check box is available only if the new model has a class.

5. Select the individual assets that you want to change or select all assets.

6. Click Change Model.
   Your request is submitted.

7. Click View Mass Change Utilities Progress to see the status of your job.

View an Asset in CA Service Desk Manager

When you integrate the product with CA Service Desk Manager, you can select an asset in CA APM and view the asset information in CA Service Desk Manager.

Follow these steps:

1. Click Asset.

2. Search for the list of available assets.

3. Click the asset that you want to view in CA Service Desk Manager.

4. Click the CMDB hyperlink at the top of the page.

   Note: You can see the CMDB hyperlink only if the product is integrated with CA Service Desk Manager and if your user role includes asset configuration privileges.

5. Log in to CA Service Desk Manager.
   A CA Service Desk Manager window opens and the details of the selected asset appear.

   Note: Asset information that you enter in the product is not immediately available in CA Service Desk Manager. By default, a 10-minute delay exists from the time an asset is updated and the time you can view the asset in CA Service Desk Manager.

View Discovered and Owned Information for an Asset

You can view the discovered information for the owned assets that are linked with discovered assets during hardware reconciliation. Discovered information for an asset includes system configuration, operating system, system devices, file systems, and other information. You can also view the owned information for the assets that you define in the product. Owned information for an asset includes asset properties (for example, operating system and product version), legal information, installed software, components, and other information.

Follow these steps:

1. Click Asset.

2. Search for the list of available assets.

3. Click the asset for which you want to view the information and perform one of the following steps:

   - Click Discovered Information.

     Note: The Discovered Information hyperlink appears only for assets that are reconciled.

   - Click Owned Information.

     Note: If the product is integrated with CA Service Desk Manager, CA Client Automation, and CA SAM, you can see the asset information from those products.

   An asset viewer window opens and displays the information. The links on the window let you access more details.

4. Click each link to view the specific information.

5. Close the window when you are finished viewing the information.

Hardware Assets

CA APM lets you track the hardware asset information that your company is entitled to use. For each hardware asset, you can track the following information:

- Maintain a record of cost and legal information.
- Maintain a record of components in asset configuration and the configurations where the asset is a component.
- Maintain the availability status of the asset.
- Track the software details that are allocated to the asset.

Add Components in an Asset Configuration

An asset can inherit the components from a model. Unicenter APM lets you add components to an asset configuration, for example, an external hard drive or a DVD writer.

Follow these steps:

1. Click Asset.
2. Search for the list of available assets.
3. Click the asset for which you want to add components.
4. Expand Configurations on the left and click Asset Configuration.

5. Click Select New in the Asset Configuration section, search for and select an asset.

6. Click Save.

Update the Asset Status

CA APM lets you change the lifecycle status of an asset. For example, you can update the status when the asset changes from received to available.

To update the asset status

1. Click Asset.

2. Search to find the list of available assets.

3. Click the asset for which you want to update the status.

4. Change the Lifecycle Status and Lifecycle Status Date fields to the appropriate status and date for the asset.

5. Click Save.
   The status for the asset is updated.

Track Image Partitions

CA APM lets you enter image partition details for an existing asset and track them. For example, you can specify that the hard disk on a computer has two partitions and enter the size in GB for each partition. Create an image partition as a separate asset and associate it with the parent asset.

Note: You can view an audit history for this relationship.

To track image partition details

1. Click Asset.

2. Search to find the list of available assets.

3. Click the asset for which you want to enter image partition details.

4. On the left, expand Relationships and click Image Partitions.

5. Click Select New and select a different asset, other than the asset previously selected.

6. Click Save.
   The image partition details are saved and can be tracked.

Asset Groups

An *asset group* is a collection of assets that you acquire together and that are based on the same model. You define an asset group in one asset record. The value in the Quantity field on the Asset Details page indicates the number of assets in the group. The product tracks the asset information for the entire group, rather than for the individual assets. All members of an asset group share asset information.

Asset groups are useful in the following situations:

- The assets are covered under the same purchase or license agreement. You do not need to track cost, payment, licensing, and legal information separately for each asset.
- The assets share some common information, but some of the individual assets in the group have different information. In this situation, you first define the assets as a group and enter the common information one time. Then, you divide the asset group into individual assets (subgroup the asset group) and enter any information that is unique to the individual assets.

You do not have to use asset groups when you are billed for assets on a single invoice. You can record payments for assets that are tracked separately, regardless of whether they were billed on the same invoice.

Asset Subgrouping

CA APM lets you divide (subgroup) an asset group into individual assets using the product. When you subgroup assets, the data for the asset group is copied to the new individual assets, *except* for the following information:

- Serial Number
- Alt Asset ID
- Host Name
- DNS Name
- MAC Address

You can change any existing data or add unique information to the new individual assets. You track the new assets separately from that point forward.

Example: Subgroup Software Licenses

In this example, you purchase 100 licenses of Microsoft Visual Studio under a single purchasing agreement. You record the licenses as an asset group with a quantity of 100. Later, you allocate ten licenses to members of your development staff. You then subgroup the ten allocated licenses into individual assets and enter their allocation information. The 90 licenses that are not allocated remain in the asset group.

Define an Asset Group

CA APM lets you add information to the repository about a group of assets that share common information. You can then manage these assets as a group throughout their lifecycle. You can divide (subgroup) the asset group into individual assets later so that you can specify and track unique information for the individual assets.

Follow these steps:

1. Click Asset, New Asset.
2. Enter the asset information.
3. In the Quantity field, enter the total number of assets in the group. You enter a value greater than one for an asset group.
4. Associate the asset group with other objects such as contacts, organizations, and companies. This approach enables specific data access to roles or users when you implement multi-tenancy.
5. Click Save.

Subgroup an Asset Group

CA APM lets you divide an asset group into individual assets when you want to manage assets in the group separately. When you subgroup an asset group, the product removes assets from the group (decreases the group quantity) and creates either one new asset or multiple new assets (depending on your criteria). The product copies the information for the group to the new assets, except Serial Number, Alt Asset ID, Host Name, DNS Name, and MAC Address.

Follow these steps:

1. Click Asset.
2. Search to find the list of available assets.
3. Click the asset that you want to subgroup.
   The Asset Details page for the selected asset appears.
4. Click Subgroup.

   Note: The Subgroup button is enabled only for an asset with a quantity greater than one.

   The Subgroup Asset wizard appears.
5. Select a subgrouping option and click Next. The following fields require explanation:

- **Create a new asset**
  Divides the original asset group into two assets. You specify the quantity for the new asset. The remaining quantity is left with the original asset.
  For example, you have an asset group with a quantity of 50. You want to divide the group into two assets with a quantity of 35 for the new asset and 15 for the original asset. You use this subgrouping option and specify 35 for the new asset quantity.

- **Create individual assets each with a quantity of one**
  Divides the entire quantity of the original asset group into multiple assets. Each asset has a quantity of one.
  For example, you have an asset group with a quantity of 25. You want to divide the group into 25 individual assets. You use this option.

6. Follow the wizard to define unique asset names and to specify the data that you want to copy to the new assets.

   Note: If you do not define unique asset names, the new assets retain the name of the original asset group.

7. Click Finish when you have completed the wizard.

8. Click Save.

Asset Registration

Use the *asset registration process* to report on a single asset and identify the instances of the asset within all asset functional areas through asset registration fields. These fields help ensure that assets within an asset functional area are not duplicated.

The following fields on the Asset Details page represent the asset registration fields:

- Asset Name
- Serial Number
- Asset Tag (represented on the page as Alt Asset ID)
- Host Name
- DNS Name
- MAC Address

Asset Configurations

This article contains the following topics:

An *asset configuration* is a description of an asset (for example, a desktop computer) and its individual components (for example, personal productivity software, monitor, modem, and so forth). CA APM lets you track the configuration information for both an asset and model. In addition, you can associate an asset or model record to their component asset and model records to initiate a relationship between them.

This information helps you maintain historical information about the changes to a configuration for an asset over the course of its life. You can define configuration records for any model or asset in the repository.

Asset configuration records can be of the following types:

Model configuration. Describes the configurations that manufacturers currently offer and any substitutions or additions that your company typically makes to those configurations when you purchase them. Use this type of configuration record to describe configurations for hardware models.

- **Asset configuration**. Describes the configurations of existing hardware assets. Use this type of configuration record when the asset configurations are different from the standard model configurations to indicate the changes between the model and asset configurations. You can also use this configuration type to describe changes to existing configurations.

You can change these configuration types at any time and manage the changes.

Add Components in a Model Configuration

You associate a hardware model to its component models to define a model configuration. A generic model is a model that is not acquired as an asset, for example, keyboards and network cards. Generic models comprise a model configuration. This configuration is available to the inherited assets from the model.

Follow these steps:

1. Click Model and search for the list of available models.
2. Click the model for which you want to add components.
3. Expand Configurations on the left and click Model Configuration.
4. Click Select New, search for and select a model.
5. Click the Edit Record icon next to the model name to define the association between the hardware model and model components.
6. Click Save.

Define Generic Model Configuration Details

CA APM lets you define configuration details for a generic model on which an asset can be based.

Follow these steps:

1. Click Model.
2. Search for the list of available models.
3. Click the model for which you want to define a generic configuration.
4. Expand Configurations on the left and click Model Configuration.
5. Click Select New to search for and select a model.
6. Click Save.

Define Generic Asset Configuration Details

CA APM lets you define configuration details for a generic asset.

Follow these steps:

1. Click Asset.
2. Search for the list of available assets.
3. Click the asset for which you want to define a generic configuration.
4. Expand Configurations on the left and click Model Configuration.
5. Click Select New to search for and select a model.
6. Click Save.

Define Specific Asset Configuration Details

CA APM lets you define a specific asset configuration.

Follow these steps:

1. Click Asset.
2. Search for the list of available assets.
3. Click the asset for which you want to define a specific configuration.
4. Expand Configurations on the left and click Asset Configuration.
5. Click Select New to search for and select an asset.

6. Click Save.

Add Components in an Asset Configuration

An asset can inherit the components from a model. Unicenter APM lets you add components to an asset configuration, for example, an external hard drive or a DVD writer.

Follow these steps:

1. Click Asset.
2. Search for the list of available assets.
3. Click the asset for which you want to add components.
4. Expand Configurations on the left and click Asset Configuration.
5. Click Select New in the Asset Configuration section, search for and select an asset.
6. Click Save.

Update or Delete a Configuration Record

CA APM lets you update or delete a configuration record.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click Model or Asset.
2. Search for the model or asset for which you want to update or delete the configuration record.
3. Click the model or asset in the search results list.
4. Expand Configurations on the left and click the appropriate configuration option. For example, click Asset Configuration or Model Configuration.
5. Perform the steps for one of the following actions.
6. Update the configuration record.
    a. Click the Edit Record icon next to the configuration record.
    b. Select the new information for the configuration record.
    c. Click Save.

7. Delete the configuration record.
    a. Click the Mark for Deletion icon next to the configuration record.
    b. Click Save.

View the Configuration When an Asset is a Component

CA APM lets you view the configuration when an asset is a component.

Follow these steps:

1. Click Asset.
2. Search for the asset for which you want to view the configuration.
3. Click the asset in the search results list.
4. Expand Configurations on the left and click Asset Configuration.
   The list of assets in the specific configuration appears.

Costs and Payments

This article contains the following topics:

CA APM lets you track financial information that is associated with assets and legal documents. Tracking costs and payments helps reduce the risk of overpaying or underpaying vendors and suppliers. This information is also useful when deciding about future equipment purchases and deployment.

In addition to tracking cost-related information for assets and legal documents, use cost records with payments to create *payment schedules.* The schedules can help you make timely payments and reduce the risk of overpayment. The information that you provide on the Cost page is used to calculate the payment schedules. If you define the cost as a recurring cost, the schedule includes multiple payment records. For example, if you enter a cost that recurs monthly for one year, the product automatically creates 12 payment records. If the cost is a one-time cost (not a recurring cost), the schedule includes only a single payment record.

Cost records store information about costs and billing, payees, recurring charges, and one time charges. Payment records maintain information about individual payments that are related to a specific cost. A payment record also calculates and displays the total scheduled payment amount, total paid amount, and the balance due for a given cost. A payment record can represent a single payment of the full cost or multiple partial payments.

Define the Parts and Pricing for a Model

You can define the parts and pricing details for a model to identify the individual component costs that comprise the total cost for a model. For example, you have a model named Dell Precision Workstation 410. You can define the parts and pricing for the internal drives, video connectors, USB connectors, SCSI port connectors, and power supply.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Model.
2. Search to find the list of available models.
3. Click the model for which you want to define the parts and pricing.
4. In the Parts and Pricing area of the page, click New and enter the parts and pricing details.
5. Click Save.

Define the Cost for an Asset or Legal Document

Defining asset costs helps you track and manage the financial information that is related to a specific asset or legal document. You can add multiple cost records for an asset or legal document. You can also add cost information to multiple assets or legal documents and update multiple payment records.

Follow these steps:

1. Click Asset or Legal Document.
2. Search to find the list of available items.
3. Click the asset or legal document that you want to update.
4. On the left, click Costs.
5. Click New and enter the cost information.
   The following fields require explanation:

   - **Unit Amount**
     Specifies the cost per unit.
   - **Total Amount**
     Displays the total cost for the total quantity of the selected asset. This amount is calculated automatically by multiplying the Unit Amount on the Costs page by the Quantity on the Asset Details page.

- **Recurring Period**
  Specifies the number of Recurring Period Units (days, months, or years) after which the cost recurs. For example, if you enter 1 for the Recurring Period and select Month for the Recurring Period Units, the cost recurs every month.

  Note: If you specify a value other than zero, select the Recurring Period Units and Termination Date.

- **Recurring Period Units**
  Specifies the unit (days, months, or years) for the Recurring Period.

- **Termination Date**
  Specifies the last date for the recurring schedule.

6. Click Save.

   Note: If you specify recurring period information for an asset cost, a payment schedule with multiple payments is automatically created. If you do not specify recurring period information, the payment schedule includes only one payment.

7. (Optional) View the payment schedule for the cost that you defined using the following steps:

   a. Click the Edit Record icon for the cost record.

   b. Click Show Payments on the right.

      Note: You can record payments that you made for this cost.

Add Cost Records to Multiple Assets

CA APM lets you add a cost record to multiple assets at a time. For example, you procured 20 new laptops and want to enter cost records for these laptops.

You can choose to update individual asset cost record or make changes to all the records at a time. For example, all the laptops that you procured have the same Unit Amount. You enter the Unit Amount and apply the value to all the asset cost records.

Follow these steps:

1. Click the Asset tab.

2. Click Add Asset Cost under Mass Change utilities on the left.

3. Search for the list of the available assets.

> **Note**: You can only add new cost records to the assets. To update existing cost records, you must open the respective asset cost record and must update it.

4. To make cost record changes to multiple assets at the same time, complete the following steps:
    a. Under Search Results, select the assets that have common cost record fields.
    b. Click Fill All Values in a Column.
    c. Click New.
    d. In the Select Column drop-down list, select the cost record field name that you want to fill for the assets.
    e. In the Value text box, enter the data that you want to update.
    f. Click the Check button.
    The selected field column is updated with the value you entered.
5. Under Search Results, enter the appropriate values in the cost record fields.
6. Click Submit.
    The cost records are added to the assets.

Delete a Cost Record

You can delete the cost record of an asset or legal document. The payment records that are associated with the deleted cost record are also deleted.

> **Important!** When you delete a cost record, you can no longer view the audit history for the record.

Follow these steps:

1. Click Asset or Legal Document.
2. Search for and select the asset or legal document for which you want to delete the cost record.
3. On the left, click Costs.
4. Click the Mark for Deletion icon for the records you want to delete.

Note: To reverse the Mark for Deletion selection, click the Undo Record Deletion icon.

5. Click Save.

Payment Schedules and Recalculation

The Payment Schedule is a list of the payments due, based on the cost information you provide on a cost record. CA APM automatically generates the payment schedule in the form of a table when you define and save a cost record. The schedule generated depends on whether the cost is a one-time cost or a recurring cost.

For a one-time cost, the schedule assumes that you will pay the entire amount on the date you incurred the cost. One payment record is scheduled.

For a recurring charge, the schedule assumes that you will make payments of equal amounts for each recurring period. One payment record for each recurring period is scheduled.

Each row in the payment schedule represents a payment that you expect to make. If a payment is done, you can manually enter the date and amount paid details in the respective columns.

By default, every schedule is system-maintained as CA APM creates schedules when you create and save cost records. However, when you manually change information in a payment schedule, it becomes user-maintained.

System-Maintained Payment Schedules

A system-maintained payment schedule is a schedule that CA APM creates and automatically calculates the payments and dynamically updates whenever the cost record is modified. CA APM recalculates payment schedule based on the criteria you provide.

For example, you expect costs to escalate 3% a year and specify an escalation percentage. CA APM creates a payment schedule on this data. Later, if you change the escalation percentage to 3.5%, CA APM automatically recalculates the schedule. This helps you adjust cost information affecting the payment schedule to meet your requirements.

Payments are calculated automatically when you change the following values of the cost record:

- Unit Amount
- Recurring Period
- Recurring Period Units
- Escalation Percent
- Begin Date
- Termination Date
- Asset Quantity

User-Maintained Payment Schedule

The system-maintained payment schedule becomes user-maintained when you manually change the information on the payment schedule.

For example, to change the escalation percentage, you perform one of the following tasks:

- Recalculate each payment manually and update the amount due in each row.
- Specify the cost information and Save. CA APM automatically recalculates and updates the payments.

Events and Notifications

This article contains the following topics:

An *event* represents an activity related to a field (default or extended) for an object. When you define an event, you specify the criteria that must be met before the event occurs. For example, you want to know when the data in a particular field changes. You can define an event that detects the data change. An event works in combination with a *notification*, which the workflow provider (for example, CA Process Automation) creates to alert your team members that an important event has occurred for a specific field or object. By using events and notifications, you alert people about upcoming events and help ensure that the appropriate tasks are performed in the correct order at the right time.

A notification is triggered when an event that you define occurs. For example, you define a date event on the Termination Date field for a legal document to notify the contract manager 15 days before a legal contract expires. The contract manager uses the 15 days to review and possibly negotiate a better contract. When the date arrives (that is, 15 days before the contract expires), the event occurs and the notification process is triggered through the workflow provider. The workflow provider constructs, issues, and manages the notification based on the configuration that you provided in the workflow provider and in CA APM.

The default notification method in CA APM supports email notifications using a workflow provider. You can send an email notification to any user or distribution list that is defined in your internal email system, even if the user is not a CA APM user. In addition, you can send an email to any external email address, if permitted by your email system.

You can also configure the notification process in the workflow provider to trigger any type of process. For example, you can set up the notification process to perform certain actions in another application when an event occurs in CA APM. For information about setting up different notification processes, see your workflow provider documentation.

You can define the following types of events to track and manage important changes to fields or objects:

- Date events. Monitor a date field for an object and have the workflow provider notify you that an important date is approaching or has passed.
- Change events. Monitor a field for an object and have the workflow provider notify you that the field value has changed.
- Watch events. Monitor a field for an object and have the workflow provider notify you about a potential obstruction to completing a task.

Escalation of Notifications

When an event occurs, the workflow provider sends an email notification to the recipients that you specified when you defined the event. CA APM lets you send email notifications to different levels of recipients.

- *Initial recipients* are the primary recipients of the notification. They are the first users to receive the notification and to respond and acknowledge the notification. The notification contains information about the event that you specified when you defined the event. The recipient receives a reminder email before the acknowledgment due date arrives. If the recipient still does not acknowledge the notification by the due date, the notification is escalated if you selected a workflow process with escalation.
- *Escalation recipients* are secondary recipients of the notification. If the initial recipients do not acknowledge the notification within a specified time frame, the product escalates the notification to the escalation recipients if you selected a workflow process with escalation. Escalations help ensure that someone is notified about an important date or event when the initial recipient is not available to acknowledge the notification. The product includes the following workflow processes and escalations:

- Notification and One Escalation - Sends a notification to the initial recipient and sends a reminder email. If the recipient acknowledges the notification, the process marks the event as completed. If the recipient does not acknowledge in the specified time frame, the process escalates the notification to the escalation recipient. If the escalation recipient responds, the process marks the event as completed. If the escalation recipient does not respond, the process marks the event as failed.

- Notification without ACK - Sends a notification to the initial recipient and marks the event as completed. The recipient does not need to respond and the process does not escalate the notification.

- Notification without Escalation - Sends a notification to the initial recipient and sends a reminder email. If the recipient does not respond, the process marks the event as failed. If the recipient responds in the specified time frame, the process marks the event as completed.

The notification levels let you notify one or more users about an event and provide separate instructions to each user. You define the recipients and the notification escalation levels when you specify the workflow provider process parameters (see page 2393) for an event.

Acknowledgements

An email notification is acknowledged when the recipient opens the email, clicks the link to CA Process Automation, logs in to CA Process Automation, and acknowledges receipt of the notification. You acknowledge an email notification in the workflow provider.

The email that is sent to the initial recipient contains the message that you specified when you defined the event. If a user does not acknowledge receipt of the email, the notification is escalated to the next responsible recipient if the selected workflow process includes escalations. When a notification is acknowledged, the product does not perform any future escalations for the same event notification.

Email Notification Process Selection

When a date, change, or watch event occurs, the email notification process is started in the workflow provider (for example, CA Process Automation). You define and set up the email notification process in the workflow provider and in CA APM (for example, you define the email recipients, levels of escalation, and notification text). CA APM lets you define different types of notification processes in the workflow provider. For example, you can have an email notification process (provided with the product) and another user-defined process that initiates actions in an external application, such as an asset management dashboard. You select the notification process that you want to use with a specific event when you define the event.

Note: For more information about defining notification processes in the workflow provider, see your workflow provider documentation.

The type of email notification process that is started after an event occurs depends on the process that you selected when you defined the event. The following email notification processes are provided with the product and apply to the CA Process Automation workflow provider:

- Notification and One Escalation - Notifies the initial recipient and sends a reminder email. If the recipient acknowledges the notification, the process marks the event as completed. If the recipient does not acknowledge in the specified time frame, the process escalates the notification to the escalation recipient. If the escalation recipient responds, the process marks the event as completed. If the escalation recipient does not respond, the process marks the event as failed.

- Notification without ACK - Notifies the initial recipient and marks the event as completed. The recipient does not need to acknowledge the notification.

- Notification without Escalation - Notifies the initial recipient and sends a reminder email. If the recipient does not acknowledge the notification within the specified time frame, the process marks the event as failed. If the recipient acknowledges within the specified time frame, the process marks the event as completed.

You can define additional notification processes in the workflow provider that perform other actions (in addition to email notifications) when events occur. You can then select one of your own defined processes when you define an event.

How to Manage Events and Notifications

Events work in combination with notifications, which the workflow provider (for example, CA Process Automation) creates, to communicate information to your team members about important events and activity. To manage events and notifications, complete the following steps:

1. Administrators grant permissions to users to manage events.

   For more information about the permissions to manage events, see Grant Permissions to Manage Events (see page 1523).

2. Open an existing local or global configuration and define any of the following events:

   - Date event (see page 2379)
   - Change event (see page 2384)
   - Watch event (see page 2388)

3. When defining an event, map all required workflow provider notification parameters to a CA APM object attribute (see page 2393).

4. The workflow provider initiates the email notification process.

5. View an audit history of events.

6. (Optional) The notification recipient acknowledges the notification (see page 2378).

Date Events

Use a *date event* to monitor a date field for an object and have the workflow provider (for example, CA Process Automation) notify you that an important date is approaching or has passed. Date events are based on the value that is stored in a specific date field (default and extended fields), and the

notification from the workflow provider provides an advanced warning to alert someone to complete a follow-up task. The date on which a user is notified about the upcoming or passed event is based on the field value for the object and the information that you specify when you define the event, including the Days After value.

CA APM lets you define one or more date events for a single field.

Note: As a rule, events are not triggered (and notifications are not sent) for field changes that happened before the event was defined. An exception to this rule occurs for date events. If the notification date occurs *after* the event was defined, an event is triggered (and a notification is sent) even if the field change happened *before* the event was defined.

Example: Define a Date Event to Terminate a Legal Document

In this example, a contract negotiator must review contracts thirty days before they expire. You define a date event on the Terminate Date field for a legal document. For example, when the contract manager adds a legal document for which the termination date is 3/31/2010, a notification is sent to the appropriate person on 3/1/2010.

Define a Date Event

CA APM lets you define a date event to monitor a date field and have the workflow provider (for example, CA Process Automation) notify you that an important date is approaching or has passed. For example, you can define a date event on the Terminate Date field for a legal document. You can define one or more date events for a single field.

Note: If your administrator has granted you the correct permissions, you can complete this task.

Follow these steps:

1. Click the tab and optional subtab for the event definition that you want to configure. On the left, click CONFIGURE: ON.

   The configuration of the event is enabled. In the Configuration Information area of the page, select an existing global or local configuration.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

   Next to the field, click the Event Configuration icon.

The Events page for the selected field appears.

2. Click New.

3. Specify the information for the date event.
   The following fields require explanation:

   - **Event Type**
     Select the type of event as a date event. After you select the event type and save the event, you cannot change the event type. If you select the incorrect event type when defining an event, delete the event and define it again using the correct event type.

   - **Days After**
     Specify a positive or negative number to indicate how many days before or after a field change occurs to create a date event.

     - A positive number indicates how many days after the original value has passed to create a date event.

     - A negative number indicates how many days before the original value approaches to create a date event.

   - **Inactive**
     Select this check box to indicate that the date event is inactive. When you make a date event inactive, no new notifications are created for the event. However, pending notifications are processed.

   - **Event Provider**
     Select the workflow provider to notify users that the date event has occurred (for example, CA IT Process Automation Manager). When you select a provider, all available workflow processes for the selected provider appear in the Workflow Process field.

   - **Workflow Process**
     Identifies the workflow process for the workflow provider. When you select a workflow process, all available process parameters for the workflow provider appear.

     - Notification and One Escalation - Notifies the initial recipient and sends a reminder email. If the recipient acknowledges the notification, the process marks the event as completed. If the recipient does not acknowledge in the specified time frame, the process escalates the notification to the escalation recipient. If the escalation recipient responds, the process marks the event as completed. If the escalation recipient does not respond, the process marks the event as failed.

     - Notification without ACK - Notifies the initial recipient and marks the event as completed. The recipient does not need to acknowledge the notification.

     - Notification without Escalation - Notifies the initial recipient and sends a reminder email. If the recipient does not acknowledge the notification within the specified time period, the process marks the event as failed. If the recipient acknowledges within the specified time period, the process marks the event as completed.

     - (Optional) Additional Process Types - Uses processes you defined in the workflow provider.

- **Notification Parameters**
  Specify each process parameter for the workflow provider by doing one of the following in each field:
  - Enter an actual (hard-coded) value.
  - Click Map Fields to map the parameter to a CA APM object attribute (see page 2393).
  - Enter an actual (hard-coded) value and, in the same field, click Map Fields to map the parameter.

  Note: Refer to the field tooltips for specific information about the format and content of each parameter field.

4. Click Save.
5. Click CONFIGURE: OFF.
   The configuration of the date event is complete.

Update a Date Event

CA APM lets you update the information for an existing date event. For example, you can change the event name and description, and you can make the event inactive.

Note: If your administrator has granted you the correct permissions, you can complete this task.

Follow these steps:

1. Click the tab and optional subtab for the event definition that you want to configure. On the left, click CONFIGURE: ON.

   The configuration of the event is enabled.

   In the Configuration Information area of the page, select an existing global or local configuration.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

   Next to the field, click the Event Configuration icon.

   The Events page for the selected field appears.

2. Click the Edit Record icon next to the date event that you want to update.

3. Enter the new information for the date event.

   Note: After you define and save an event, you cannot change the Event Type, Event Cause, Value Changed From, and Value Changed To. If you enter the incorrect information, delete the event and define it again using the correct information.

4. Click the Complete Record Edit icon.

5. Click Save.

6. Click CONFIGURE: OFF.
   The configuration of the date event is complete.

Delete a Date Event

CA APM lets you delete a date event that you do not need. For example, when you do not want to be notified about a change to the Terminate Date field for a legal document, you can delete the associated date event. If your administrator has granted you the correct permissions, you can complete this task.

Note: Any pending notifications from the workflow provider (for example, CA Process Automation) about the event are sent before the event is deleted. When you delete an event, all historical information about the event is deleted. We recommend that instead of deleting the event, you make the event inactive. That way, if you need the event in the future, you do not have to redefine it.

Follow these steps:

1. Click the tab and optional subtab for the event definition that you want to configure.

   On the left, click CONFIGURE: ON. The configuration of the event is enabled.

   In the Configuration Information area of the page, select an existing global or local configuration.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

Next to the field, click the Event Configuration icon. The Events page for the selected field appears.

2. Click the Mark for Deletion icon next to the date event that you want to delete.

3. Click Save.

4. Click CONFIGURE: OFF.
   The configuration of the date event is complete.

Change Events

Use a *change event* to monitor a field for an object and have the workflow provider (for example, CA Process Automation) notify you that the field value has changed. Change events are based on the value that is stored in a specific field (default and extended fields), and the notification from the workflow provider provides a warning to alert someone when the value of a field is set or changes.

CA APM lets you define one or more change events for a single field.

Example: Define a Change Event to Find Equipment for a New Employee

In this example, asset technicians provide the appropriate equipment when an employee is hired or transferred to a different department. You define a change event that issues a notification to a member of the asset technician team when the Department field value for the contact is set or changes. This notification alerts the technician to find equipment for the new or transferred employee.

Define a Change Event

CA APM lets you define a change event to monitor a field and have the workflow provider (for example, CA Process Automation) notify you that the field value has changed. For example, you can define a change event on the Department field for a contact. You can define one or more change events for a single field.

Note: If your administrator has granted you the correct permissions, you can complete this task.

Follow these steps:

1. Click the tab and optional subtab for the event definition that you want to configure.

   On the left, click CONFIGURE: ON. The configuration of the event is enabled.

   In the Configuration Information area of the page, select an existing global or local configuration.

Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

Next to the field, click the Event Configuration icon.

The Events page for the selected field appears.

2. Click New.

3. Specify the information for the change event.
The following fields require explanation:

   - **Event Type**
     Select the type of event as a change event. After you select the event type and save the event, you cannot change the event type. If you select the incorrect event type when defining an event, delete the event and define it again using the correct event type.

   - **Event Cause**
     Select the type of action that must happen to the field for the change event to occur. Supported event causes include when a field is changed, a record is added, and a record is deleted.

   - **Value Changed From**
     Select the initial state of the field value for the change event to occur. Supported field value changes include the following options:

     - **Any value**. Any field value sets the initial state.
     - **Blank**. A blank field value sets the initial state.
     - **Old value**. A specific value sets the initial state.

   - **Value**
     Available when you select *Old value* in the Value Changed From field. Enter a specific value to set the initial state.

   - **Value Changed To**
     Select the final state of the field value for the change event to occur. Supported field value changes include the following options:

     - **Any value**. Any field value, except a blank value, sets the final state.
     - **Blank**. A blank field value sets the final state.
     - **New value**. A specific value sets the final state.

   - **Value**
     Available when you select *New value* in the Value Changed To field. Enter a specific value to set the final state.

- **Inactive**
  Select this check box to indicate that the change event is inactive. When you make a change event inactive, no new notifications are created for the event. However, pending notifications are processed.

- **Event Provider**
  Select the workflow provider to notify users that the change event has occurred (for example, CA IT Process Automation Manager). When you select a provider, all available workflow processes for the selected provider appear in the Workflow Process field.

- **Workflow Process**
  Identifies the workflow process for the workflow provider. When you select a workflow process, all available process parameters for the workflow provider appear.

  - Notification and One Escalation - Notifies the initial recipient and sends a reminder email. If the recipient acknowledges the notification, the process marks the event as completed. If the recipient does not acknowledge in the specified time frame, the process escalates the notification to the escalation recipient. If the escalation recipient responds, the process marks the event as completed. If the escalation recipient does not respond, the process marks the event as failed.

  - Notification without ACK - Notifies the initial recipient and marks the event as completed. The recipient does not need to acknowledge the notification.

  - Notification without Escalation - Notifies the initial recipient and sends a reminder email. If the recipient does not acknowledge the notification within the specified time period, the process marks the event as failed. If the recipient acknowledges within the specified time period, the process marks the event as completed.

  - (Optional) Additional Process Types - Uses processes you defined in the workflow provider.

- **Notification Parameters**
  Specify each process parameter for the workflow provider by doing one of the following in each field:

  - Enter an actual (hard-coded) value.

  - Click Map Fields to map the parameter to a CA APM object attribute (see page 2393).

  - Enter an actual (hard-coded) value and, in the same field, click Map Fields to map the parameter.

  Note: Refer to the field tooltips for specific information about the format and content of each parameter field.

4. Click Save.

5. Click CONFIGURE: OFF.
   The configuration of the event is complete.

Update a Change Event

CA APM lets you update the information for an existing change event. For example, you can change the event name and description, and you can make the event inactive.

Note: If your administrator has granted you the correct permissions, you can complete this task.

Follow these steps:

1. Click the tab and optional subtab for the event definition that you want to configure. On the left, click CONFIGURE: ON.
   The configuration of the event is enabled.

2. In the Configuration Information area of the page, select an existing global or local configuration. Next to the field, click the Event Configuration icon.

   The Events page for the selected field appears.

   Note: Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration

3. Click the Edit Record icon next to the change event that you want to update.

4. Enter the new information for the change event.

   Note: After you define and save an event, you cannot change the Event Type, Event Cause, Value Changed From, and Value Changed To. If you enter the incorrect information, delete the event and define it again using the correct information.

5. Click the Complete Record Edit icon.

6. Click Save.

7. Click CONFIGURE: OFF.
   The configuration of the change event is complete.

Delete a Change Event

CA APM lets you delete a change event that you do not need. For example, when you do not want to be notified about a change to the Department field for a contact, you can delete the associated change event. If your administrator has granted you the correct permissions, you can complete this task.

Note: Any pending notifications from the workflow provider (for example, CA Process Automation) about the event are sent before the event is deleted. When you delete an event, all historical information about the event is deleted. We recommend that instead of deleting the event, you make the event inactive. That way, if you need the event in the future, you do not have to redefine it.

Follow these steps:

1. Click the tab and optional subtab for the event definition that you want to configure. On the left, click CONFIGURE: ON.

   The configuration of the event is enabled. In the Configuration Information area of the page, select an existing global or local configuration.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

   Next to the field, click the Event Configuration icon.

   The Events page for the selected field appears.

2. Click the Mark for Deletion icon next to the change event that you want to delete.

3. Click Save.

4. Click CONFIGURE: OFF.
   The configuration of the change event is complete.

Watch Events

Use a *watch event* to monitor a field for an object and have the workflow provider (for example, CA Process Automation) notify you about a potential obstruction to completing a task. Watch events are based on inactivity on a particular field (default and extended fields) within a specified time period, and the notification from the workflow provider provides an advanced warning to alert someone about a potential obstruction. If the field value changes within the time period, the workflow provider does not send a notification.

CA APM lets you define one or more watch events for a single field.

Example: Define a Watch Event to Configure and Deploy New Laptops

In this example, you require that asset technicians configure and deploy all new laptops to employees within five days of receiving the laptop. To meet this requirement, you define a watch event that creates an event when an asset is assigned a status (Lifecycle Status field) of received. If the status remains received for more than five days, a notification is sent to an asset technician.

Define a Watch Event

CA APM lets you define a watch event to monitor a field and have the workflow provider (for example, CA Process Automation) notify you about inactivity on a particular field. For example, you can define a watch event on the Lifecycle Status field for an asset. You can define one or more watch events for a single field.

Note: If your administrator has granted you the correct permissions, you can complete this task.

Follow these steps:

1. Click the tab and optional subtab for the event definition that you want to configure. On the left, click CONFIGURE: ON.

   The configuration of the event is enabled. In the Configuration Information area of the page, select an existing global or local configuration.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

   Next to the field, click the Event Configuration icon.

   The Events page for the selected field appears.

2. Click New.

3. Specify the information for the watch event.

Important! The Value Changed From and Value fields work together to start the timer for the watch event. The timer continues for the duration that you specify in the Days After field. The Value Changed To and Value fields work together to indicate the value that you want to achieve and stop the timer. If the value that you want to achieve does not occur in the specified time period after the timer starts, the watch event occurs and indicates that the defined workflow did not happen.

The following fields require explanation:

- **Event Type**
  Select the type of event as a watch event. After you select the event type and save the event, you cannot change the event type. If you select the incorrect event type when defining an event, delete the event and define it again using the correct event type.

- **Event Cause**
  Select the type of action that must happen to the field for the watch event to occur. A supported event cause is when a field is changed.

- **Days After**
  Specify a positive number to indicate how many days to wait after the Value Changed From field value to start the watch timer.

  Note: If the Value Change To field value does not occur, the watch timer expires after the number of days that you specify. After the watch timer expires, the watch event is created. However, the watch timer will stop when the Value Change To field value changes to the specified value and no watch event is created.

- **Value Changed From**
  Select the initial field value to start the timer to create the watch event. Supported field value changes include the following options:

  - **Any value**. Any field value starts the timer for the watch event.
  - **Blank**. A blank field value starts the timer for the watch event.
  - **Old value**. A specific initial value starts the timer for the watch event.

- **Value**
  Available when you select *Old value* in the Value Changed From field. Enter a specific value to start the timer for the watch event.

- **Value Changed To**
  Select the final state of the field value that stops the timer for the watch event and prevents the watch event from occurring. Supported field value changes include the following options:

  - **Any value**. Any field value stops the timer for the watch event and prevents the watch event from occurring.

- **Blank**. A blank field value stops the timer for the watch event and prevents the watch event from occurring.

- **New value**. A specific field value stops the timer for the watch event and prevents the watch event from occurring.

- **Value**
  Available when you select *New value* in the Value Changed To field. Enter a specific value to stop the timer for the watch event and prevent the watch event from occurring.

- **Inactive**
  Select this check box to indicate that the watch event is inactive. When you make a watch event inactive, no new notifications are created for the event. However, pending notifications are processed.

- **Event Provider**
  Select the workflow provider to notify users that the watch event has occurred (for example, CA IT Process Automation Manager). When you select a provider, all available workflow processes for the selected provider appear in the Workflow Process field.

- **Workflow Process**
  Identifies the workflow process for the workflow provider. When you select a workflow process, all available process parameters for the workflow provider appear.

  - Notification and One Escalation - Notifies the initial recipient and sends a reminder email. If the recipient acknowledges the notification, the process marks the event as completed. If the recipient does not acknowledge in the specified time frame, the process escalates the notification to the escalation recipient. If the escalation recipient responds, the process marks the event as completed. If the escalation recipient does not respond, the process marks the event as failed.

  - Notification without ACK - Notifies the initial recipient and marks the event as completed. The recipient does not need to acknowledge the notification.

  - Notification without Escalation - Notifies the initial recipient and sends a reminder email. If the recipient does not acknowledge the notification within the specified time period, the process marks the event as failed. If the recipient acknowledges within the specified time period, the process marks the event as completed.

  - (Optional) Additional Process Types - Uses processes you defined in the workflow provider.

- **Notification Parameters**
  Specify each process parameter for the workflow provider by doing one of the following in each field:

  - Enter an actual (hard-coded) value.

  - Click Map Fields to map the parameter to a CA APM object attribute (see page 2393).

  - Enter an actual (hard-coded) value and, in the same field, click Map Fields to map the parameter.

Note: Refer to the field tooltips for specific information about the format and content of each parameter field.

4. Click Save.

5. Click CONFIGURE: OFF.
   The configuration of the watch event is complete.

Update a Watch Event

CA APM lets you update the information for an existing watch event. For example, you can change the event name and description, and you can make the event inactive.

Note: If your administrator has granted you the correct permissions, you can complete this task.

Follow these steps:

1. Click the tab and optional subtab for the event definition that you want to configure. On the left, click CONFIGURE: ON.

   The configuration of the event is enabled. In the Configuration Information area of the page, select an existing global or local configuration.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

   Next to the field, click the Event Configuration icon.

   The Events page for the selected field appears.

2. Click the Edit Record icon next to the watch event that you want to update.

3. Enter the new information for the watch event.

   Note: After you define and save an event, you cannot change the Event Type, Event Cause, Value Changed From, and Value Changed To. If you enter the incorrect information, delete the event and define it again using the correct information.

4. Click the Complete Record Edit icon.

5. Click Save.

6. Click CONFIGURE: OFF.
   The configuration of the watch event is complete.

Delete a Watch Event

CA APM lets you delete a watch event that you do not need. For example, when you do not want to be notified about a change to the Lifecycle Status field for an asset, you can delete the associated watch event. If your administrator has granted you the correct permissions, you can complete this task.

Note: Any pending notifications from the workflow provider (for example, CA Process Automation) about the event are sent before the event is deleted. When you delete an event, all historical information about the event is deleted. We recommend that instead of deleting the event, you make the event inactive. That way, if you need the event in the future, you do not have to redefine

Follow these steps:

1. Click the tab and optional subtab for the event definition that you want to configure. On the left, click CONFIGURE: ON.

   The configuration of the event is enabled. In the Configuration Information area of the page, select an existing global or local configuration.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

   Next to the field, click the Event Configuration icon.

   The Events page for the selected field appears.

2. Click the Mark for Deletion icon next to the watch event that you want to delete.

3. Click Save.

4. Click CONFIGURE: OFF.
   The configuration of the watch event is complete.

Workflow Provider Process Parameters

You perform some of the setup and configuration of the email notification process in the workflow provider. However, you also specify the process parameters for the workflow provider when you define an event in CA APM. The process parameters include items such as user IDs, email addresses, email subject, content of email, and other items. The workflow provider uses this information to construct, issue, and manage the email notification.

Note: For information about workflow provider process parameters that you must specify in CA Process Automation, see Integrate with CA Process Automation Integration for a Notification Process Manually (see page 3489). For information about setting up a notification process, see your workflow provider documentation.

You can provide actual (hard-coded) values when you specify the process parameters. If you use an actual value for an email address (or another parameter), you must verify that the address (or other data) is valid.

You can also map the process parameters to CA APM object attributes. If you map a process parameter to a CA APM object attribute, the workflow provider accesses CA APM to find the current value of the mapped attribute and uses that value to construct and manage the notification. For example, you map the process parameter Initial Email Addresses to the CA APM attribute Contact Email Address when you define an event. When that event occurs, the workflow provider determines the current value of the CA APM Contact Email Address and uses that value for the Email ID.

Important! To map CA Process Automation process parameters to CA APM objects successfully, you must understand the CA APM data objects and the CA Process Automation parameters. You need to determine which CA APM object is an appropriate match for each CA Process Automation parameter.

Notification and One Escalation Process Parameters

The process parameters that appear when you define an event depend on the workflow provider process type that you select. The Notification and One Escalation process is an email notification process that is included with the product. This process sends an email notification to the initial recipient when an event occurs and, if the initial recipient does not respond, escalates the email to the first escalation level recipients. When you select this process as the workflow process for an event, a list of parameters appears.

Important! CA APM and CA Process Automation do not validate the information that you enter for the parameters. You must verify that your input is valid and that you entered the data in the correct format.

The following fields require explanation:

- **Initial User IDs**
  CA Process Automation user ID (CA APM or non-CA APM user) for acknowledging the initial notification. You can specify more than one user ID, separated with colons. Do not enter spaces between entries.
  Example: This example contains a user ID (John) that is a text entry value and the mapped field {legaldoc.owner.userid}. The two items are separated with a colon. The mapped field {legaldoc.owner.userid} represents the user ID of the user in the Owner field of the Legal Document. To obtain the mapped field {legaldoc.owner.userid}, click the Map Fields button, select the Owner link in the Add Fields dialog, and select User ID from the list of attributes.

```
John:{legaldoc.owner.userid}
```

- **Initial Groups**
  CA Process Automation group name for acknowledging the initial notification. You can specify more than one group name, separated with colons. Do not enter spaces between entries.
  Example: This example contains a CA Process Automation group name (ITAM) that is a text entry value.

```
ITAM
```

- **Initial Email Addresses**
  Email address (or distribution list) of the initial recipient of the email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.
  Example: This example contains an email address (john.doe@company.com) that is a text entry value and the mapped field {legaldoc.owner.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.owner.emailid} represents the email address of the user in the Owner field of the Legal Document. To obtain the mapped field {legaldoc.owner.emailid}, click the Map Fields button, select the Owner link in the Add Fields dialog, and select Email Address from the list of attributes.

```
john.doe@company.com;{legaldoc.owner.emailid}
```

- **Initial Email Copy Addresses**
  Email address (or distribution list) of the initial copy recipient of the email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.
  Example: This example contains an email address (jane.doe@company.com) that is a text entry value and the mapped field {legaldoc.requestor.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.requestor.emailid} represents the email address of the user in the Requestor field of the Legal Document. To obtain the mapped field {legaldoc.requestor.emailid}, click the Map Fields button, select the Requestor link in the Add Fields dialog, and select Email Address from the list of attributes.

```
jane.doe@company.com;{legaldoc.requestor.emailid}
```

- **Initial Email Subject**
  Subject of the email message for the initial recipient. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (Acknowledgement required for) and the mapped field {legaldoc.documentidentifier}.

```
Acknowledgment required for {legaldoc.documentidentifier}
```

- **Initial Email Message**
  Message of the email for the initial recipient. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (The Legal Document Document Identifier), the mapped field {legaldoc.documentidentifier}, and more text entry content.

```
The Legal Document Document Identifier {legaldoc.documentidentifier} requires your acknowledgment using the link in
the Subject of this email.
```

- **Acknowledgment Title**
  Title that appears on the acknowledgment task that the user accesses in CA Process Automation to acknowledge receipt of the notification. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (The Legal Document Document Identifier) only.

```
The Legal Document Document Identifier
```

- **Acknowledgment Description**
  Description that appears on the acknowledgment task that the user accesses in CA Process Automation to acknowledge receipt of the notification. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (The Legal Document Document Identifier) and the mapped field {legaldoc.documentidentifier}.

```
The Legal Document Document Identifier {legaldoc.documentidentifier}
```

- **Escalation User IDs**
  CA Process Automation user ID (CA APM or non-CA APM user) for acknowledging the escalation notification. You can specify more than one user ID, separated with colons. Do not enter spaces between entries.
  Example: This example contains a user ID (Mary) that is a text entry value and the mapped field {legaldoc.owner.supervisor.userid}. The two items are separated with a colon. The mapped field {legaldoc.owner.supervisor.userid} represents the user ID of the supervisor of the user in the Owner field of the Legal Document. To obtain the mapped field {legaldoc.owner.supervisor.userid}, click the Map Fields button, select the Owner link in the Add Fields dialog, select the Supervisor link, and select User ID from the list of attributes.

```
Mary:{legaldoc.owner.supervisor.userid}
```

- **Escalation Groups**
  CA Process Automation group name for acknowledging the escalation notification. You can specify more than one group name, separated with colons. Do not enter spaces between entries.
  Example: This example contains a CA Process Automation group name (ITAM) that is a text entry value.

```
ITAM
```

- **Escalation Email Addresses**
  Email address (or distribution list) of the recipient of the escalation email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.
  Example: This example contains an email address (mary.doe@company.com) that is a text entry value and the mapped field {legaldoc.owner.supervisor.emailid}. The two items are separated with a semicolon. To obtain the mapped field {legaldoc.owner.supervisor.emailid}, click the Map Fields button, select the Owner link in the Add Fields dialog, select the Supervisor link, and select Email Address from the list of attributes.

```
mary.doe@company.com;{legaldoc.owner.supervisor.emailid}
```

- **Escalation Email Copy Addresses**
  Email address (or distribution list) of the copy recipients of the escalation email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.
  Example: This example contains an email address (jane.doe@company.com) that is a text entry value and the mapped field {legaldoc.requestor.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.requestor.emailid} represents the email address of the user in the Requestor field of the Legal Document. To obtain the mapped field {legaldoc. requestor.emailid}, click the Map Fields button, select the Requestor link in the Add Fields dialog, and select Email Address from the list of attributes.

```
jane.doe@company.com;{legaldoc.requestor.emailid}
```

- **Escalation Email Subject**
  Subject of the escalation email. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (Escalation for), the mapped field {legaldoc. documentidentifier}, and additional text entry content.

```
Escalation for {legaldoc.documentidentifier}. Acknowledgment required
```

- **Escalation Email Message**
  Message of the escalation email. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (The Legal Document Document Identifier), the mapped field {legaldoc.documentidentifier}, and more text entry content.

```
The Legal Document Document Identifier {legaldoc.documentidentifier} requires your acknowledgment using the link in
the Subject of this email.
```

- **Reminder Email Subject**
  Subject of the reminder email message for initial and escalation recipients. The product sends a reminder when half of the Acknowledgment Time-out period has passed. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (Reminder for), the mapped field {legaldoc. documentidentifier}, and additional text entry content.

```
Reminder for {legaldoc.documentidentifier}. Acknowledgment required.
```

- **Reminder Email Message**
  Message of the reminder email for initial and escalation recipients. The product sends a reminder when half of the Acknowledgment Time-out period has passed. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (Reminder: The Legal Document Document Identifier), the mapped field {legaldoc.documentidentifier}, and more text entry content.

```
Reminder: The Legal Document Document Identifier {legaldoc.documentidentifier} requires your acknowledgment using the
link in the Subject of this email.
```

- **Acknowledgment Time-out (Days:Hours:Minutes)**
  The amount of time that is allowed for acknowledgment after the email notification is sent before the escalation process begins. This time-out applies to initial and escalation notifications. Days, hours, and minutes can be any numeric value. The format must be *days*:*hours*:*minutes* (separated with colons).
  Example: This example specifies a time-out period of exactly four days.

```
4:00:00
```

Notification without ACK Process Parameters

The process parameters that appear when you define an event depend on the workflow provider process type that you select. The Notification without ACK process is an email notification process that is included with the product. This process sends an email notification to the specified recipient when an event occurs. The recipient does not need to acknowledge the notification, and the product does not escalate the notification. When you select this process as the workflow process for an event, a list of parameters appears.

Important! CA APM and CA Process Automation do not validate the information that you enter for the parameters. You must verify that your input is valid and that you entered the data in the correct format.

The following fields require explanation:

- **Email Address**
  Email address (or distribution list) of the recipient of the email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.
  Example: This example contains an email address (john.doe@company.com) that is a text entry value and the mapped field {legaldoc.owner.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.owner.emailid} represents the email address of the user in the Owner field of the Legal Document. To obtain the mapped field {legaldoc.owner.emailid}, click the Map Fields button, select the Owner link in the Add Fields dialog, and select Email Address from the list of attributes.

```
john.doe@company.com;{legaldoc.owner.emailid}
```

- **Email Copy Address**
  Email address (or distribution list) of the copy recipient of the email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.
  Example: This example contains an email address (jane.doe@company.com) that is a text entry value and the mapped field {legaldoc.requestor.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.requestor.emailid} represents the email address of the user in the Requestor field of the Legal Document. To obtain the mapped field {legaldoc. requestor.emailid}, click the Map Fields button, select the Requestor link in the Add Fields dialog, and select Email Address from the list of attributes.

```
jane.doe@company.com;{legaldoc.requestor.emailid}
```

- **Email Subject**
  Subject of the email message for the recipient. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (Acknowledgment required for) and the mapped field {legaldoc.documentidentifier}.

```
Acknowledgment required for {legaldoc.documentidentifier}
```

- **Email Message**
  Message of the email for the recipient. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (The Legal Document Document Identifier), the mapped field {legaldoc.documentidentifier}, and more text entry content.

```
The Legal Document Document Identifier {legaldoc.documentidentifier} requires your acknowledgment using the link in
the Subject of this email.
```

Notification without Escalation Process Parameters

The process parameters that appear when you define an event depend on the workflow provider process type that you select. The Notification without Escalation process is an email notification process that is included with the product. This process sends an email notification to the specified recipient when an event occurs. If the recipient does not respond in the specified time period, the process does not escalate the notification. However, the process marks the associated event as failed. When you select this process as the workflow process for an event, a list of parameters appears.

Important! CA APM and CA Process Automation do not validate the information that you enter for the parameters. You must verify that your input is valid and that you entered the data in the correct format.

The following fields require explanation:

- **User IDs**
  CA Process Automation user ID (CA APM or non-CA APM user) for acknowledging the notification. You can specify more than one user ID, separated with colons. Do not enter spaces between entries.
  Example: This example contains a user ID (John) that is a text entry value and the mapped field {legaldoc.owner.userid}. The two items are separated with a colon. The mapped field {legaldoc.owner.userid} represents the user ID of the user in the Owner field of the Legal Document. To obtain the mapped field {legaldoc.owner.userid}, click the Map Fields button, select the Owner link in the Add Fields dialog, and select User ID from the list of attributes.

```
John:{legaldoc.owner.userid}
```

- **Groups**
  CA Process Automation group name for acknowledging the notification. You can specify more than one group name, separated with colons. Do not enter spaces between entries.
  Example: This example contains a CA Process Automation group name (ITAM) that is a text entry value.

```
ITAM
```

- **Email Addresses**
  Email address (or distribution list) of the recipient of the email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.
  Example: This example contains an email address (john.doe@company.com) that is a text entry value and the mapped field {legaldoc.owner.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.owner.emailid} represents the email address of the user in the Owner field of the Legal Document. To obtain the mapped field {legaldoc.owner.emailid}, click the Map Fields button, select the Owner link in the Add Fields dialog, and select Email Address from the list of attributes.

```
john.doe@company.com;{legaldoc.owner.emailid}
```

- **Email Copy Addresses**
  Email address (or distribution list) of the copy recipient of the email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.
  Example: This example contains an email address (jane.doe@company.com) that is a text entry value and the mapped field {legaldoc.requestor.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.requestor.emailid} represents the email address of the user in the Requestor field of the Legal Document. To obtain the mapped field {legaldoc.requestor.emailid}, click the Map Fields button, select the Requestor link in the Add Fields dialog, and select Email Address from the list of attributes.

```
jane.doe@company.com;{legaldoc.requestor.emailid}
```

- **Email Subject**
  Subject of the email message for the recipient. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (Acknowledgment required for) and the mapped field {legaldoc.documentidentifier}.

```
Acknowledgment required for {legaldoc.documentidentifier}
```

- **Email Message**
  Message of the email for the recipient. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (The Legal Document Document Identifier), the mapped field {legaldoc.documentidentifier}, and more text entry content.

```
The Legal Document Document Identifier {legaldoc.documentidentifier} requires your acknowledgment using the link in
the Subject of this email.
```

- **Acknowledgment Title**
  Title that appears on the acknowledgment task that the user accesses in CA Process Automation to acknowledge receipt of the notification. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (The Legal Document Document Identifier) only.

```
The Legal Document Document Identifier
```

- **Acknowledgment Description**
  Description that appears on the acknowledgment task that the user accesses in CA Process Automation to acknowledge receipt of the notification. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (The Legal Document Document Identifier) and the mapped field {legaldoc.documentidentifier}.

```
The Legal Document Document Identifier {legaldoc.documentidentifier}
```

- **Acknowledgment Time-out (Days:Hours:Minutes)**
  The amount of time that is allowed for acknowledgment after the email notification is sent. Days, hours, and minutes can be any numeric value. The format must be *days*:*hours*:*minutes* (separated with colons).
  Example: This example specifies a time-out period of exactly four days.

```
4:00:00
```

- **Reminder Email Subject**
  Subject of the reminder email message. The product sends a reminder when half of the Acknowledgment Time-out period has passed. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (Reminder for), the mapped field {legaldoc.documentidentifier}, and additional text entry content.

```
Reminder for {legaldoc.documentidentifier}. Acknowledgment required.
```

- **Reminder Email Message**
  Message of the reminder email. The product sends a reminder when half of the Acknowledgment Time-out period has passed. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.
  Example: This example contains text entry content (Reminder: The Legal Document Document Identifier), the mapped field {legaldoc.documentidentifier}, and more text entry content.

```
Reminder: The Legal Document Document Identifier {legaldoc.documentidentifier} requires your acknowledgment using the
link in the Subject of this email.
```

Make an Event Inactive

CA APM lets you make an event inactive so that the workflow provider (for example, CA Process Automation) does not send future notifications for the event. The history about important dates and events is retained.

Note: If your administrator has granted you the correct permissions, you can complete this task.

To make an event inactive

1. Click the tab and optional subtab for the event definition that you want to configure. On the left, click CONFIGURE: ON.

   The configuration of the event is enabled. In the Configuration Information area of the page, select an existing global or local configuration.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

   Next to the field, click the Event Configuration icon.

   The Events page for the selected field appears.

2. Click the Edit Record icon next to the event that you want to make inactive.
3. Select the Inactive check box.
4. Click the Complete Record Edit icon.
5. Click Save.
6. Click CONFIGURE: OFF.
   The configuration of the event is complete.

Notes

This article contains the following topics:

Notes are free-form explanatory text that you associate with any object, and supplement the information for an object. Notes are categorized by a *type* that you specify when you attach a note to an object. Use this information to search for objects that have a particular type of note assigned to them. For example, if another company acquires one of your primary suppliers, you can attach a company acquisition note to the company record for that supplier.

Default note types are provided for the following objects. Your administrator can define additional types.

- Models

- Assets
- Legal Documents
- Contacts
- Companies
- Organizations
- Locations
- Sites

Attach a Note

CA APM lets you attach a note to supplement the information for an object. For example, if another company acquires one of your primary suppliers, you can attach a company acquisition note to the company record for that supplier.

Follow these steps:

1. Click the object for which you want to attach a note. For example, click Model, Asset, Legal Document, Contact, Company, Organization, or Location.
2. Search for the list of available objects.
3. Click the object record for which you want to attach a note.
4. Click Notes on the left.
5. Click New and enter the note.
6. Click Save.

Update or Delete a Note

CA APM lets you update or delete a note that is attached to an object record.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click the object for which you want to update a note. For example, click Model, Asset, Legal Document, Contact, Company, Organization, or Location.
2. Search for the list of available objects.

3. Click the object record for which you want to update or delete a note.
4. Click Notes on the left.
5. Perform one of the following actions.
6. Update a note.
    a. Click the Edit Record icon for the note you want to update.
    b. Update the note information.
    c. Click Save.
7. Delete a note.
    a. Click the Mark for Deletion icon next to the note you want to delete.
    b. Click Save.

Hardware Asset Management

This section contains the following articles:

Hardware Reconciliation

This article contains the following topics:

The hardware reconciliation process matches *discovered assets* to corresponding *owned assets* from different logical repositories so that you can manage the assets based on your business practices. Use this process to identify the discrepancies between your owned and discovered assets. Hardware reconciliation identifies unauthorized, missing, under-utilized, and over-utilized assets, which helps you to optimize your hardware asset base.

- Owned assets provide IT asset information from a financial and ownership perspective. The product supports the entire lifecycle of an owned asset from procurement, acquisition, allocation, use, and disposal, including legal and cost information. Owned assets have purchase records, including a purchase order number, invoice number, associated costs (lease, payment schedule, maintenance), associated contracts (terms and conditions), and vendor information. The owned-asset data is entered and imported using the CA APM user interface, Administration tab, Data Importer.

- Discovered assets provide information about the assets that an enterprise is using or has deployed. External discovery products and the discovery component of CA Client Automation scan the assets on a network and store them as discovered assets in the CA MDB. Discovered assets contain evidence about the following information:

  - The asset is deployed and can be found on your network.

  - The asset is being used and has metrics.

  - The asset contains up-to-date configuration information for inventory.

The CA APM hardware reconciliation process matches the discovered asset data and the owned asset data that are stored in the CA MDB. The hardware reconciliation process may detect assets that cannot be reconciled with any of your owned assets. You can decide to add the unreconciled assets to your repository so that you can track and manage all assets in your network.

Hardware reconciliation automates the synchronization of ownership and discovered data. Hardware reconciliation supports the discovery component of CA Client Automation and third-party discovery products. These components and products are supported through the combination of the CA Asset Converter and the asset collector component of CA Client Automation. When CA SAM is installed, discovery connectors load the discovery data into the CA SAM repository. The discovery data is then synchronized with CA APM.

Hardware Reconciliation Engine

The *Hardware Reconciliation Engine* is a continuously processing Windows service that is responsible for the following tasks during the reconciliation process:

- Synchronizes discovered assets with ownership assets using reconciliation rules.

- Reconciles owned and discovered assets based on asset matching criteria (see page 2419).

- Maps discovery data to ownership data based on normalization rules (see page 2407).

- Updates selected asset fields in the product based on changes to the corresponding discovered assets.

- Completes the actions that are defined in the reconciliation rule that is being executed.

How Reconciliation Engines Process Reconciliation Rules

The date and time at which a reconciliation rule was last executed determines when the rule will be processed again. Hardware Reconciliation Engines process reconciliation rules in the following sequence, which allows for multiple tenant support as well as multiple Hardware Engines:

1. Each Hardware Reconciliation Engine searches for reconciliation rules that are not being processed by another engine and selects the rule that has the oldest processing date and time.

2. A Hardware Reconciliation Engine locks the reconciliation rule so it cannot be accessed by another engine, executes the rule, updates the rule date-and-time value, and then unlocks the rule. The Hardware Reconciliation Engine searches for the next available reconciliation rule with the oldest date-and-time value and repeats the process.

3. The process continues with all engines continuously operating and searching for and executing the next available reconciliation rule with the oldest date-and-time value.

How to Reconcile

The reconciliation process compares data from discovery products with CA APM ownership data in the CA MDB. This process reconciles discovered and owned assets, tracks changes to critical fields, and tracks discrepancies as the result of missing or deleted assets. To reconcile, complete the following steps:

1. Establish data normalization rules (see page 2407) to map data values between discovery repositories and the product.

2. Define a reconciliation rule to specify how to limit the data being processed and how to process the records found.

3. (Optional) Define reconciliation update options to specify the owned-asset fields that you want the Hardware Reconciliation Engine to update automatically with changes found in the corresponding discovered assets.

4. Define asset matching criteria (see page 2419) to match owned and discovered assets for a reconciliation rule.

5. (Optional) Exclude an ownership asset from the reconciliation process.

6. (Optional) Exclude an asset family from the reconciliation process.

7. View the reconciliation results in the message queue.

8. (Optional) Add unreconciled assets to your repository so that you can track and manage all assets in your network.

Note: You can generate reports to view information about your reconciliation results and environment. For more information about generating reports, see Reconciliation Reports (see page 2428).

Data Normalization

This article contains the following topics:

Data normalization is a step in the reconciliation process where you establish a list of rules to standardize, organize, and consolidate data between the product and discovery repositories. Normalization reduces, eliminates, and consolidates redundant data that is imported into the product from multiple sources, such as purchase order products, human resource products, procurement products, the Data Importer, and so forth.

When you normalize data, you reduce the time and effort necessary to manage the data. You also reduce the possibility of the user selecting the incorrect information when defining assets, models, and other objects, and when generating reports. The product guides you through the normalization process, enabling you to perform it much more efficiently and accurately. The consolidated discovery data is then reconciled with your owned assets during the reconciliation process and can be reported on using the reconciliation reports.

You normalize three of the fields that can be used as asset matching criteria (see page 2419): company, operating system, and system model. These fields are normalized because they often have multiple values that represent one normalized value. For example, the discovery tool may find many variations for the name of one company. You normalize all the variations to one value for the company name and include the normalized company name in asset matching criteria. These fields are normalized so that you can include them in asset matching criteria.

The Hardware Reconciliation Engine normalizes the data that is imported into the product by referencing the following normalization rules, which you define:

- Company normalization rules (see page 2408)
- Operating System normalization rules (see page 2411)
- System Model normalization rules (see page 2413)

Example: Normalize Company Data

In this example, when you import company data into the product using CA Client Automation, multiple variations of Document Management Company are discovered in various formats, including the following values:

- Document Management Company
- Document Management Co
- Doc Management Company
- Doc Management Co

To help users select the correct company when defining an asset and model and when generating reconciliation reports, you define company normalization rules to map all variations to Document Management Company. During the reconciliation process, the normalization rules map the values as follows, before an asset is updated in the CA MDB:

Note: A collected company that is mapped to an authoritative company affects Hardware Reconciliation only if the collected company is a discovered company.

Collected (Nonauthoritative Value)	Normalized (Authoritative Value)
Document Management Co	Document Management Company
Doc Management Company	Document Management Company
Doc Management Co	Document Management Company

Company Normalization Rules

Company normalization rules are intended for key organizations with which you have a business relationship, for example, Microsoft, Adobe, Lenovo, and so forth.

- **Collected Company**
  A *collected company* is either a discovered company or a *product-defined company*. Product-defined companies are collected from user input and other products that share the CA MDB. Hardware reconciliation reconciles only *discovered* companies. Collected companies have a *nonauthoritative* status. You map nonauthoritative collected companies to normalized *authoritative* companies.

Important! Only *discovered* collected companies that are mapped to normalized companies are reconciled during Hardware Reconciliation.

- **Normalized Company**
  A normalized company is either a *CA-content company* or a product-defined company. CA-content companies are provided with CA APM and have an *authoritative status*. Authoritative

status allows a company to have a normalization rule. You define a normalization rule for an authoritative normalized company when you map one or more collected companies to the authoritative company.
Product-defined companies initially have a nonauthoritative status. You can change the status of a product-defined company from nonauthoritative to authoritative. You can then map a collected company to the authoritative product-defined company to define a normalization rule. Only company normalization rules for discovered collected companies affect Hardware Reconciliation.

- **Subordinate Company**
  When you map a collected nonauthoritative company to a normalized authoritative company, the nonauthoritative company becomes *subordinate* to the authoritative company in the normalization rule.

Define Company Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

You can define company normalization rules that are applied during the matching process whenever the reconciliation rule contains asset matching criteria (see page 2419). Any asset matching criterion that contains company information automatically applies the company normalization rules.

When you map a collected nonauthoritative company to a normalized authoritative company, the nonauthoritative company becomes *subordinate* to the authoritative company in the normalization rule. The subordinate company no longer appears in the Collected Company list or the Normalized Company list. If you delete the normalization rule that contains the subordinate company, the subordinate company returns to nonauthoritative status and appears in the Collected Company list and, if it was a product-defined company, also in the Normalized Company list.

Follow these steps:

1. Click Directory, List Management.
2. On the left, expand Normalization and select Company Normalization.
   The discovered collected company values and the normalized company values appear.
3. If the term you want to use as the normalized value does not appear in the Normalized Company list or the Collected Company list, click New Company to add the company, and then repeat the previous steps.
4. (Optional) Change a nonauthoritative company to an authoritative normalized company.
5. Map the Collected Company list discovered values to a Normalized Company value.
   The list of company normalization rules is defined and is referenced during the reconciliation process.

Update Company Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

You update a company normalization rule when you want to change how a discovered company is normalized. This update may affect the reconciliation process. To update a normalization rule for a company, you delete the rule and define a new rule.

The product monitors updates to normalization rules. If you change a normalization rule, the Hardware Reconciliation Engine processes the asset matching so that the assets are matched using the new rule. Any assets that are matched as a result of a previous Hardware Reconciliation Engine process are evaluated again to determine if their matching should change based on the new normalization rule.

When you delete a company normalization rule, the subordinate company returns to nonauthoritative status and appears in the Collected Company list. If the subordinate company was a product-defined company, it also appears in the Normalized Company list on the Normalization Rule page.

Follow these steps:

1. Click Directory, List Management, Company Rules.
2. Delete the normalization rule that you want to change.
3. Define the new company normalization rule.

Change a Nonauthoritative Company to an Authoritative Normalized Company

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

You can map collected companies to only authoritative companies in the Normalized Company list on the Company Normalization page. Product-defined companies in the Normalized Company list initially have a nonauthoritative status. You can change a product-defined company that is in the Normalized Company list to an authoritative normalized company, to which you can map collected companies.

Note: Only company normalization rules for discovered collected companies affect Hardware Reconciliation.

Follow these steps:

1. Click Directory, List Management.

2. On the left, expand Normalization and select the normalization type.
   The discovered collected values and the normalized values appear.

3. Clear the Show only Authoritative records check box in the Normalized Company section.

4. Click Go in the Normalized Company section.
   The collected product-defined companies that are nonauthoritative and not yet mapped to an authoritative company appear in the normalized list with an Override icon next to the company name.

5. Click the Override icon to the left of the nonauthoritative company that you want to change to an authoritative company, in the *normalized* list.
   The nonauthoritative company changes to an authoritative normalized company.

6. Map a collected company to the new authoritative normalized company before performing any other action in the Normalized Company section.

   Note: The company is not saved as an authoritative company until at least one collected company is mapped to the new authoritative company.

   The new authoritative normalized company and its normalization rule are saved.

Operating System Normalization Rules

Operating system normalization rules are intended for operating systems managing your computers, for example, Windows XP Professional, Windows Server 2008 Enterprise Edition, Windows Vista Enterprise Edition, and so forth.

- **Collected Operating System**
  A collected operating system is always a discovered operating system. Collected operating systems have a nonauthoritative status. You map nonauthoritative collected operating systems to normalized authoritative operating systems.

- **Normalized Operating System**
  A normalized operating system is always a *product-defined operating system*. Product-defined operating systems are collected from user input and other products that share the CA MDB. Product-defined operating systems always have an authoritative status. Authoritative status allows an operating system to have a normalization rule. You define a normalization rule for an authoritative normalized operating system when you map one or more collected operating systems to the authoritative operating system.

- **Subordinate Operating System**
  When you map a collected nonauthoritative operating system to a normalized authoritative operating system, the nonauthoritative operating system becomes subordinate to the authoritative operating system in the normalization rule.

Define Operating System Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

You can define operating system normalization rules that are applied during the matching process whenever the reconciliation rule contains asset matching criteria (see page 2419). Any asset matching criterion that contains operating system information automatically applies the operating system normalization rules.

When you map a collected nonauthoritative operating system to a normalized authoritative operating system, the nonauthoritative operating system becomes subordinate to the authoritative operating system in the normalization rule. The subordinate operating system no longer appears in the Collected Operating System list. If you delete the normalization rule that contains the subordinate operating system, the subordinate operating system returns to nonauthoritative status and appears in the Collected Operating System list.

Follow these steps:

1. Click Directory, List Management.

2. On the left, expand Normalization and select Operating System Normalization.
   The discovered Collected Operating System values and the Normalized Operating System values appear.

3. If the term you want to use as the normalized value does not appear in the Normalized Operating System list or the Collected Operating System list, click New Operating System to add the operating system, and then repeat the previous steps.

4. Map the Collected Operating System list discovered values to a Normalized Operating System value.
   The list of operating system normalization rules is defined and is referenced during the reconciliation process.

Update Operating System Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

You update an operating system normalization rule when you want to change how a discovered operating system is normalized. This update may affect the value of the operating system in a matching asset. To update a normalization rule for an operating system, you delete the rule and define a new rule.

The product monitors updates to normalization rules. If you change an operating system normalization rule and the reconciliation rule update option for operating system is enabled, the Hardware Reconciliation Engine changes the value of the operating system to the new normalized name in matching assets.

Important! If you change a normalization rule for an operating system that applies to public tenant data, the change may affect discovered assets for all tenants, depending on whether they use the specific operating system.

When you delete an operating system normalization rule, the subordinate operating system returns to nonauthoritative status and appears in the Collected Operating System list on the Normalization Rule page.

Follow these steps:

1. Click Directory, List Management, Operating System Rules.
2. Delete the normalization rule that you want to change.
3. Define the new operating system normalization rule.

System Model Normalization Rules

System model normalization rules are intended for hardware devices such as a computer, for example, Lenovo ThinkPad T400, Lenovo ThinkCentre M58, and so forth.

- **Collected System Model**
  A collected system model is always a discovered system model. Collected system models have a nonauthoritative status. You map nonauthoritative collected system models to normalized authoritative system models.

- **Normalized System Model**
  A normalized system model is always a *product-defined system model*. Product-defined system models are collected from user input and other products that share the CA MDB. Product-defined system models always have an authoritative status. Authoritative status allows a system model to have a normalization rule. You define a normalization rule for an authoritative normalized system model when you map one or more collected system models to the authoritative system model.

- **Subordinate System Model**
  When you map a collected nonauthoritative system model to a normalized authoritative system model, the nonauthoritative system model becomes subordinate to the authoritative system model in the normalization rule.

Define System Model Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

You can define system model normalization rules that are applied during the matching process whenever the reconciliation rule contains asset matching criteria (see page 2419). Any asset matching criterion that contains system model information automatically applies the system model normalization rules.

When you map a collected nonauthoritative system model to a normalized authoritative system model, the nonauthoritative system model becomes subordinate to the authoritative system model in the normalization rule. The subordinate system model no longer appears in the Collected System Model list. If you delete the normalization rule that contains the subordinate system model, the subordinate system model returns to nonauthoritative status and appears in the Collected System Model list.

Follow these steps:

1. Click Directory, List Management.
2. On the left, expand Normalization and select System Model Normalization.
   The discovered collected system model name and manufacturer name values and the normalized system model name and manufacturer name values appear.
3. If the term you want to use as the normalized value does not appear in the Normalized System Model list or the Collected System Model list, click New System Model to add the system model, and then repeat the previous steps.
4. Map the Collected System Model list discovered values to a Normalized System Model value.
   The list of system model normalization rules is defined and is referenced during the reconciliation process.

Update System Model Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

You update a system model normalization rule when you want to change how a discovered system model is normalized. This update may affect the reconciliation process. To update a normalization rule for a system model, you delete the rule and define a new rule.

The product monitors updates to normalization rules. If you change a normalization rule, the Hardware Reconciliation Engine processes assets so that the assets are matched using the new rule. Any assets that are matched as a result of a previous operation of the Hardware Reconciliation Engine are evaluated again to determine if their matching should change based on the new normalization rule.

When you delete a system model normalization rule, the subordinate system model returns to nonauthoritative status and appears in the Collected System Model list on the Normalization Rule page.

Follow these steps:

1. Click Directory, List Management, System Model Rules.
2. Delete the normalization rule that you want to change.
3. Define the new system model normalization rule.

View Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

You can search for and view the normalization rules to see the mapping between collected values and the normalized values. This information is used during the hardware reconciliation process.

Follow these steps:

1. Click Directory, List Management.
2. On the left, expand Normalization and select the normalization rule type that you want to view.
3. Search for the normalized value or the collected value for which you want to view the normalization mapping rules.
   For each normalization rule, the collected value and its corresponding normalized value appear in the Search Results section.

Delete a Normalization Rule

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

You delete a normalization rule when you no longer want asset matching criteria to apply the normalization rule during the reconciliation process or when you want to change a normalization rule. To change a normalization rule for a company, operating system, or system model, you delete the rule and define a new rule.

When you delete a company normalization rule, the subordinate company returns to nonauthoritative status and appears in the Collected Company list. If the subordinate company was a product-defined company, it also appears in the Normalized Company list on the normalization rule page. When you delete an operating system normalization rule, the subordinate operating system returns to nonauthoritative status and appears in the Collected Operating System list on the normalization rule page. When you delete a system model normalization rule, the subordinate system model returns to nonauthoritative status and appears in the Collected System Model list on the normalization rule page.

Follow these steps:

1. Click Directory, List Management.

2. On the left, expand Normalization and select the normalization rule type for the rule that you want to delete.

3. Search for the normalized value or the collected value for which you want to delete a normalization rule.
   For each normalization rule, the collected value and its corresponding normalized value appear in the Search Results section.

4. Select the rule that you want to delete.

5. Click Delete Rule.
   The normalization rule is deleted. Asset matching criteria do not apply the rule during the reconciliation process.

Updates to Normalization Rules

You update a system model or company normalization rule when you want to change how a discovered system model or company is normalized. This update may affect the reconciliation process. You update an operating system normalization rule when you want to change how a discovered operating system is normalized. This update may affect the value of the operating system in a matching asset. To update a normalization rule, you delete the rule and define a new rule.

The product monitors updates to normalization rules. If you change a system model or company normalization rule, the Hardware Reconciliation Engine performs the asset matching process so that the assets are matched using the new rule. Any assets that are matched as a result of a previous operation are evaluated again to determine if their matching should change based on the new normalization rule. If you change an operating system normalization rule, the Hardware Reconciliation Engine changes the value of the operating system to the new normalized name in matching assets if the reconciliation rule update option for operating system is enabled.

When you delete a company normalization rule, the subordinate company returns to nonauthoritative status and appears in the Collected Company list. If the subordinate company was a product-defined company, it also appears in the Normalized Company list on the Normalization Rule page. When you delete an operating system normalization rule, the subordinate operating system returns to nonauthoritative status and appears in the Collected Operating System list on the

Normalization Rule page. When you delete a system model normalization rule, the subordinate system model returns to nonauthoritative status and appears in the Collected System Model list on the Normalization Rule page.

Define a Reconciliation Rule

Note: Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

Use a reconciliation rule to define the processing options and actions that the Hardware Reconciliation Engine performs. You can define one reconciliation rule for each tenant.

Note: Each tenant can have only one reconciliation rule. Therefore, if you make a rule inactive, the inactive rule is the only reconciliation rule that is associated with the tenant. If you want to change the reconciliation rule for a tenant, you can update the current reconciliation rule or delete the current reconciliation rule and define a new rule. If you delete a rule, all asset matching links between discovered and owned assets that are associated with the rule are also deleted.

Follow these steps:

1. Click Administration, Reconciliation Management.
2. On the left, click New Reconciliation Rule.
3. If applicable, select the tenant that is associated with the reconciliation rule that you are defining.
4. Enter the reconciliation rule information and click Save.

   Note: Select the Inactive check box if you want to suspend reconciliation processing for an individual tenant. If you select the Inactive check box, the Hardware Reconciliation Engine does not process the rule (no asset matching or data updates occur for the rule). For example, you can make a rule inactive temporarily while you define normalization rules or troubleshoot asset matching errors. If you make an existing rule inactive and the discovered and owned assets were already matched, the matching links are saved.

5. (Optional) Select the Monitor Asset Updates check box to define the reconciliation update options that you want the Hardware Reconciliation Engine to update automatically.
6. (Optional) Select the Match Assets check box to define the asset matching criteria (see page 2419) that you want the Hardware Reconciliation Engine to apply.

Note: If you do not define matching criteria, the Hardware Reconciliation Engine uses the default asset matching criterion, which matches the owned serial number to the discovered serial number.

7. Click Save.
   The new reconciliation rule is defined.

Define Reconciliation Update Options

Note: Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

You can apply changes to selected, critical owned-asset fields when the Hardware Reconciliation Engine detects new values in the corresponding discovered-asset fields. The Hardware Reconciliation Engine monitors the critical fields that you select and updates the owned-asset fields when changes are detected in the corresponding discovered assets. You specify the owned-asset fields that you want to be automatically updated with changes that are found in the corresponding discovered assets.

Follow these steps:

1. Click Administration, Reconciliation Management.
2. On the left, click Reconciliation Rule Search.
3. Search to find the list of available reconciliation rules.
4. Click the reconciliation rule for which you want to define reconciliation update options.
5. Select the Monitor Asset Updates check box to have the Hardware Reconciliation Engine apply automatic updates.
6. Select the check boxes for the fields that you want to be automatically updated.

   Note: Select the Host Name check box to enable and select the Copy Host Name to Asset Name update option.

7. Click Save.
   The new reconciliation update options are defined.

Asset Matching Criteria

This article contains the following topics:

The Hardware Reconciliation Engine matches the owned and discovered assets based on the *asset matching criteria* that you define for a reconciliation rule. The criteria define the matching factors for owned and discovered assets based on a list of field values from both CA APM and the discovery products. The Hardware Reconciliation Engine identifies all assets being managed and provides the required data during the reconciliation process.

If you modify the asset matching criteria associated with a reconciliation rule, the Hardware Reconciliation Engine reprocesses reconciled assets using the new criteria the next time the engine processes the rule.

You can match the following asset field values:

Owned Asset Field	Discovered Asset Field
Alternate Host Name	Host Name
Alternate Host Name	Registry Asset Name
Alternate ID	BIOS Asset Tag
Asset Alias	BIOS Asset Tag
Asset Alias	Host Name
Asset Name	Host Name
Class	System Type
Host Name	Host Name
Host Name	Registry Asset Name
MAC Address	MAC Address
MAC Address and Host Name	MAC Address and Host Name
Manufacturer	System Vendor
Model Name	System Model
Previous Asset Tag	BIOS Asset Tag
Serial Number	Serial Number
Subclass	System Type

The product monitors the asset matching fields of owned and discovered assets. If you modify the value of an owned asset field that can be used for asset matching, the Hardware Reconciliation Engine reprocesses the modified owned asset using the new value, during the next reconciliation process.

Similarly, if the discovery component of CA Client Automation or a third-party discovery product modifies the value of a discovered asset field in the CA MDB that can be used for asset matching, the Hardware Reconciliation Engine reprocesses the modified discovered asset using the new value, during the next reconciliation process.

The product also monitors changes to normalization rules for companies and system models. These rules affect the asset matching of owned and discovered assets. If you change one of the normalization rules, the Hardware Reconciliation Engine runs the asset matching process so that assets are matched using the new rules. Any assets that are matched as a result of a previous run of the Hardware Reconciliation Engine are evaluated again to determine if their matching should change based on the new normalization rules.

Inactive Status Effect on Asset Matching

Hardware Reconciliation processes all active owned assets created by CA APM that are not excluded from reconciliation. An inactive asset, model, asset family, or company affects reconciliation links between owned and discovered assets as follows:

- Inactive owned asset
  - If an owned asset is inactive before the Hardware Reconciliation Engine matches the asset to a discovered asset, the owned asset is not matched.
  - If an owned asset is made inactive after asset matching, the Hardware Reconciliation Engine clears the matching link the next time the engine processes the reconciliation rule.
- Inactive Model
  - When a model is made inactive before the Hardware Reconciliation Engine matches a discovered asset to an owned asset that is based on that model, the owned asset is not matched.
  - When a model is made inactive after an owned asset that is based on that model is matched, the Hardware Reconciliation Engine clears the matching link for that asset and all others that are based on the inactive model the next time the engine processes the reconciliation rule.
- Inactive Asset Family
  - When an asset family, class, or subclass is made inactive before the Hardware Reconciliation Engine matches a discovered asset to an owned asset with that asset family, class, or subclass, the owned asset is not matched.
  - When an asset family, class, or subclass is made inactive after an owned asset with the asset family, class, or subclass is matched, the Hardware Reconciliation Engine clears the matching link for that asset and all others that belong to the inactive asset family, class, or subclass the next time the engine processes the reconciliation rule.
- Inactive Company
  - When a company is made inactive before the Hardware Reconciliation Engine matches a discovered asset to an owned asset with that company as the manufacturer, the owned asset is not matched.

- When a company is made inactive after an owned asset with that company as the manufacturer is matched, the Hardware Reconciliation Engine clears the matching link for that asset and all others that are associated with the inactive company the next time the engine processes the reconciliation rule.

Define Asset Matching Criteria

Note: Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

Based on the matching criteria that you define for a reconciliation rule, the product attempts to match the owned and discovered assets. The Hardware Reconciliation Engine performs the asset reconciliation when the ownership field value matches the discovered field value.

Follow these steps:

1. Click Administration, Reconciliation Management.
2. On the left, click Reconciliation Rule Search.
3. Search to find the list of available reconciliation rules.
4. Click the reconciliation rule for which you want to define an asset matching criterion.
5. Select the Match Assets check box to have the Hardware Reconciliation Engine apply asset matching criteria.
6. Select the owned and discovered fields that you want to match and click Add Criteria.
   A new asset matching criteria record is added to the Matching Criteria section and a new trimming record is added to the Trimming section.
7. Click the Edit Record icon next to the new criterion in the Matching Criteria section.
8. Select the matching criterion options.
9. (Optional) In the Trimming section, click the Edit Record icon and select trimming options for the asset matching criterion. For example, discovered computer names at one site have a three-character location code as a prefix, which is not in the owned asset computer name. You create a trimming record for the asset matching criterion that trims three characters from the left side of the discovered computer names.
10. (Optional) Continue to add matching criteria to the reconciliation rule.
11. Click Save.
    The new asset matching criteria are defined and the reconciliation rule is saved.

Note: After a reconciliation rule is saved, if you want to change the matched fields in an asset matching criterion to different fields, delete the criterion and create a new one.

Exclude an Ownership Asset from the Reconciliation Process

You can exclude individual owned assets from the reconciliation process. Some reasons for excluding assets from reconciliation include the following examples:

- An owned asset has no matching discovered asset and continues to be included in the list of unreconciled assets. For example, assets that are never attached to the network, like some laptops, or assets that are retired, but their ownership data is stored in CA APM.
- A company does not want to include a particular class of asset, for example, laptops, in reconciliation.

If an owned asset is excluded from the reconciliation process before the Hardware Reconciliation Engine matches the asset to a discovered asset, the owned asset is not available for matching. If an owned asset is excluded from the reconciliation process after asset matching, the Hardware Reconciliation Engine clears the matching link the next time the engine processes the reconciliation rule. The owned asset is not available for matching.

Note: If the asset family of an excluded asset is set to be included in the hardware reconciliation process, the asset continues to be excluded from the process. If an asset family is excluded from the hardware reconciliation process, all assets that belong to the excluded asset family are excluded.

Follow these steps:

1. Click Asset, Asset Search.
2. Search to find the list of available assets.
3. Click the asset that you want to exclude from the reconciliation process.
4. In the Basic Information section, select the Exclude Reconciliation check box.
5. Click Save.
   The ownership asset is not included in future reconciliations.

Exclude an Asset Family from the Reconciliation Process

You can exclude all owned assets in an asset family from the hardware reconciliation process. Some reasons for excluding asset families from reconciliation include the following examples:

- Assets in an asset family have no matching discovered assets and continue to be included in the list of unreconciled assets. For example, assets that are in the service asset family are not attached to the network, but their ownership data is stored in CA APM.
- The asset family is software. The product does not reconcile software.

- A company wants to make an asset family inactive. Hardware Reconciliation processes active owned assets created by CA APM.

If an asset family is excluded from the reconciliation process before the Hardware Reconciliation Engine matches owned assets in that asset family to discovered assets, the owned assets are not available for matching. If an asset family is excluded from the reconciliation process after owned assets in that asset family are matched, the Hardware Reconciliation Engine clears the matching links the next time the engine processes the reconciliation rule. The owned assets are not available for matching.

Follow these steps:

1. Click Directory, List Management.
2. On the left, expand Asset Lists and click Asset Family.
3. Click the Edit Record icon for the asset family that you want to exclude from the reconciliation process.
4. Complete one of the following options:
   - Clear the Reconcile Hardware check box.
   - Select the Is Software check box.
   - Select the Inactive check box.
5. Select the Complete Record Edit icon for the asset family object.
6. Click Save.
   Assets in the excluded asset family are not included in future reconciliations.

Exclude an Asset Family Class or Subclass from the Reconciliation Process

You can exclude all owned assets in an asset family class or subclass from the hardware reconciliation process. For example, you can exclude assets because your company wants to make an asset family class or subclass inactive. Hardware Reconciliation processes active owned assets created by CA APM.

If an asset family class or subclass is excluded from the reconciliation process before the Hardware Reconciliation Engine matches discovered assets to owned assets in that asset family class or subclass, the owned assets are not available for matching. If an asset family class or subclass is excluded from the reconciliation process after owned assets in that asset family class or subclass are matched, the Hardware Reconciliation Engine clears the matching links the next time the engine processes the reconciliation rule. The owned assets are not available for matching.

Follow these steps:

1. Click Directory, List Management.
2. On the left, expand Asset Lists and click Asset Family.
3. Click the Edit Record icon for the asset family with a class or subclass you want to exclude from the reconciliation process.

4. Click Class List.
5. Click the Edit Record icon for the class you want to exclude from the reconciliation process (or the class with a subclass you want to exclude).
6. Select the Inactive check box and click the Complete Record Edit icon for the asset family class if you want to exclude the entire class.

   Note: Skip this step if you want to exclude a subclass, but not the entire class, from the reconciliation process.

7. Click Subclass List if you want to exclude a subclass.
8. Click the Edit Record icon for the subclass you want to exclude from the reconciliation process.
9. Select the Inactive check box and click the Complete Record Edit icon for the asset family subclass.
10. Click Save.
    Assets in the excluded asset family class or subclass are not included in future reconciliations.

View the Reconciliation Results

Note: Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.\

When the Hardware Reconciliation Engine processes actions for a reconciliation rule, the engine writes records to the message queue in the database. You can search the message queue for reconciliation log messages. The message queue retains log messages for a configurable number of days.

Note: You can control the level of detail written to the message queue by changing the Hardware Reconciliation Engine logging level. You can also control the number of days that messages are retained in the message queue. For more information about logging level and message queue retention settings, see Hardware Reconciliation Engine Configuration Settings.

Follow these steps:

1. Click Administration, Reconciliation Management.

2. On the left, click Reconciliation Message Search.
   The message queue displays reconciliation log messages in the Search Results section.

3. (Optional) Search to find a message in the message queue.

Note: You can export the message queue to a comma-separated values (CSV) file for use in a spreadsheet application. You can also generate reports to view information about your environment relative to reconciliation. For more information about generating reports, see Reconciliation Reports (see page 2428).

Add Assets from Unreconciled Discovered Records

The hardware reconciliation process can detect assets that cannot be reconciled with any of your owned assets. You can decide to add the unreconciled assets to your repository so that you can track and manage all assets in your network.

You can add the assets to your repository in one of the following ways:

- Configure CA APM to automatically add unreconciled discovered assets to your ownership repository.
- Add the unreconciled assets by generating and exporting the results of a report and then importing the report results through the Data Importer.

Important! Before you import data into CA APM, review the data to ensure accuracy and uniqueness.

Follow these steps:

- **To add assets from unreconciled discovered assets to your ownership repository automatically, complete the following steps:**

  1. Click Administration, Reconciliation Management.
  2. Click New Reconciliation Rule or search and select a reconciliation rule you created.
  3. The Reconciliation Rule Details page opens.
  4. Check the Add Assets to Ownership Repository check box.
  5. Under Add Assets to Ownership Repository, select the contact update details and the asset status.
  6. Select Add Models to add model details to the repository.

Note: If you select Add Models, and the unreconciled asset has no model information, CA APM does not add the asset details to the repository.

7. Click Save.

- **To add assets from unreconciled discovered records assets to your ownership repository manually, complete the following steps:**

1. Log in to Business Intelligence Launch Pad.
   The Reports pane opens.
2. Click Document List.
3. Expand Public Folders, CA Reports.
4. Click CA ITAM.
5. Double-click the icon to the left of the report that identifies the discovered assets that are not matched to any owned assets.
6. Enter the search criteria for the report.

   Note: Select one tenant only when you generate the report. You can import data into only one tenant at a time.

7. Click Run Query.
8. Click the link for the flat file format that you can export.
   The report is converted to a document format that you can view and export.
9. Save the document as a CSV file.
10. Log in to CA APM as the administrator.
11. Navigate to Administration, Data Importer, New Import.
12. Specify the CSV file name in the Data File field.
13. Select the main destination object and the delimiter.

    Important! Select the same tenant that you selected when you generated the report.

14. In the Advanced Settings area, verify that the following options are selected:

    Insert or Update
    Create Secondary Lookup Object
    Update Secondary Lookup objects
    Error on Secondary Lookup Object Errors

15. Click Save.
16. Specify the column mapping.
17. Click Submit in the Schedule area to start the import process.
    The unreconciled assets are added to your data repository.

Manage Reconciliation Rules

Note: Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

You can manage reconciliation rules in the following ways:

- Update the information for a reconciliation rule.
  If you modify the asset matching criteria associated with a reconciliation rule, the Hardware Reconciliation Engine reprocesses reconciled assets using the new criteria the next time the engine processes the rule.
- Delete a defined reconciliation rule.
  If you delete a rule, all asset matching links between discovered and owned assets that are associated with the rule are also deleted. Each tenant can have only one reconciliation rule. If you want to change the reconciliation rule for a tenant, update the current reconciliation rule or delete the current rule and define a new reconciliation rule.

  Note: You can also make a rule inactive if you want to suspend reconciliation processing temporarily for an individual tenant. To make a rule inactive, update the rule and select the Inactive check box. If the discovered and owned assets were already matched for the rule, the matching links are saved.

Follow these steps:

1. Click Administration, Reconciliation Management.
2. On the left, click Reconciliation Rule Search.
3. Search to find the list of available reconciliation rules.
4. To update a reconciliation rule, complete the following steps
   a. Click the reconciliation rule that you want to update.
   b. Enter the new information for the reconciliation rule.

Note: Select the Inactive check box if you want to suspend reconciliation processing for an individual tenant. If you select the Inactive check box, the Hardware Reconciliation Engine does not process the rule (no asset matching or data updates occur for the rule). For example, you can make a rule inactive temporarily while you define normalization rules or troubleshoot asset matching errors. If you make an existing rule inactive and the discovered and owned assets were already matched, the matching links are saved.

c. Click Save.

Note: After a reconciliation rule is saved, if you want to change the matched fields in an asset matching criterion to different fields, delete the criterion and create a new one.

5. To delete a reconciliation rule, complete the following steps:

   a. Click the rule that you want to delete.

   b. Click Delete and confirm that you want to delete the reconciliation rule.

Export the Reconciliation Results

Note: Verify that the user completing this task belongs to a role in which reconciliation management access is enabled.

After you view the message queue, you can export the queue to a comma-separated value (CSV) file for use in a spreadsheet application.

Follow these steps:

1. Click Administration, Reconciliation Management.
2. On the left, click Reconciliation Message Search.
   The message queue displays reconciliation log messages in the Search Results section.
3. Search to find the reconciliation log messages that you want to export.
4. Click Export to CSV.
   The message queue search results are exported to a CSV file and a link to the CSV file appears.

Reconciliation Reports

This article contains the following topics:

Use the reconciliation reports to view the following information and help you manage your IT assets based on your business practices:

Your security permissions determine the tenant data you see when generating reports. If you have access to multiple tenants, you see the data for all tenants to which you have access. If you only have access to a single tenant, you only see the data for that tenant.

Important! On an Oracle database, when you generate a report for the first time, you may encounter a database error. To resolve this issue, restart the *Server Intelligence Agent* service in the Central Configuration Manager.

- Owned assets that have been reconciled to a discovered asset, including both discovered inventory and network discovery records.
- Billed assets (that is, an active or received asset having a valid bill code) not matched to a discovery record.
- Discovered assets not reconciled to an owned asset.
- Discovered assets not processed due to missing or invalid data.
- Owned assets matched to discovery records.
- Owned assets not matched to discovery records.
- Matches between network discovery data and agent discovery data.
- Potential lost revenue, including assets not being billed, but discovered. This report exposes revenue opportunities based on the number of assets being billed. Use the information in this report to provide proof that an asset is active and discovered.
- Network discovery records that have not been matched to a corresponding discovered inventory. Network discovery provides limited data to identify an asset on the network. Discovery provides detailed hardware and software information about an asset.

Generate a Report

CA APM reports provide you with a detailed view of your owned and discovery assets to help with reconciliation.

Important! If you plan to add to your repository using the Data Importer the discovered assets that are not matched to any of your owned assets, select only a single tenant when generating the appropriate report.

Follow these steps:

1. Log in to BusinessObjects Enterprise Launch Pad.
   The Reports pane opens.
2. Click Documents.
3. On the left pane, click Folders.
4. Expand Public Folders, CA Reports.
5. Click CA Asset Portfolio Management.
6. Double-click the icon to the left of the report you want to generate.
7. Enter the search criteria for the report.
8. Click Run Query.

Remove the Tenant Drop-Down List

Any user belonging to more than one tenant can select a tenant in a drop-down list when generating a report. You can remove the tenant drop-down list so that you are not asked to select a tenant when generating a report.

Follow these steps:

1. Log in to BusinessObjects Enterprise Launch Pad.
   The Reports pane opens.
2. Click Documents.
3. On the left pane, click Folders.
4. Expand Public Folders, CA Reports, CA Service Management.
5. Click CA Asset Portfolio Management.
   All CA APM reports appear.
6. Right-click the report for which you want to remove the tenant drop-down list and select Modify.
7. Click Cancel.
8. Click Edit.
9. In the Query Filters pane, select the “Tenant - Multi-Mandatory” filter and click the Remove icon on the top-right of the pane.
10. Repeat the previous step for all tabs. Query Tabs appear below the Query Filters area of the page.
11. Click the Apply Changes and Close.

12. Save the report in the same location from where the report is opened.

13. When prompted, click Yes to override the existing report.

14. Click the Close document icon.
    When you generate the report, you are not asked to select a tenant.

Searching

This section contains the following articles:

Object Searching

Contents

An *object* represents something that you record and track in your repository. The primary objects in CA APM are models, assets, legal documents, contacts, companies, organizations, locations, and sites. At any time, you can search to find objects in the repository to manage. You can also search the audit history to see all changes made to an object record over time.

For example, you can search for objects for the following reasons:

- Search for a model so that you can define an asset from the model.

- Search for an asset so that you can define a support contact for the asset.

- Search for an asset from an inventory request that you want to fulfill.

- Search for a legal contract so that you can define terms and conditions for the contract.

- Search the audit history so that you can see when the cost center for a laptop changed, and who changed the cost center.

Based on the search criteria that you specify, a list of matching objects appear in the search results.

Most of the time, the objects that you want to view or update appear with the default search provided for each object. This type of search is intended for when you want to locate a single record for update from a simple list of objects. For example, you can enter the serial number when searching for a laptop to find the laptop matching the serial number.

When you search, you can use search operators (see page 2435) and search connectors (see page 243
to make your searches more precise and get more useful results.

Search Tips

Use the following information and techniques to help make your searches more effective:

- **Keep it simple**. For example, if you are looking for a specific asset or model, and you have the name available, enter the name. If you have additional information to identify the object, such as the serial number for an asset, enter that number. This additional information increases the chance that your search returns the object you want.

- **Expand your search with a wildcard**. Use the asterisk (*) or percent sign (%) wildcard character as a substitute for any number of characters in your search string to return search results. Use as many wildcard characters in your search string as you want. For example, enter *S** or *S%* when searching for contacts by last name to find contacts having the last name Sanders, Shelley, Smith, Spencer, Solomon, and so forth. Enter *Dell *" Monitor* when searching for assets by name to find any size Dell monitor; Dell 19" Monitor, Dell 21" Monitor, Dell 30" Monitor, and so forth.

- **Searches are not case-sensitive**. You can ignore capitalization in your searches. For example, a company search for *Document Management Company* returns the same results for *document management company.*

- **Search titles are unique in a tenant**.
  When you save a search and specify a title, the title must be unique within a tenant. You cannot save a search with the same title in a single tenant.

- **If you receive too many, or too few, search results** and cannot find an object, try the following suggestions:

  - Use different search criteria. For example, instead of searching for a contact by last name, search for their first name, department, user ID, or location.

  - Use operators (see page 2435) and connectors (see page 2435) to increase or decrease the objects returned in the results.

  - Verify that you have spelled the name of the object correctly, and have entered any additional search criteria correctly.

- **Expand your search with check box criteria**. Include check box fields such as Inactive in your searches. For example, search for all inactive assets and generate a report for management analysis. You can also search for all inactive assets to make them active again.

- **Expand your search within multiple asset families and legal template types**. Search within one or more asset families and legal template types. For example, search for a specific model under both hardware and software, or search for a legal document under a service contract and software addition.

- **Invalid Searches**. You can use the Invalid drop-down list when you manage searches to display or hide invalid searches. A search becomes invalid when your CA APM administrator configures the user interface and restricts access to any field that a search uses, or deletes an extended field that a search uses. If you have a search that you cannot use because of security restrictions, contact your CA APM administrator for assistance.

- Sort the search results (see page 2436) to help make it easier to find information.

- Save a search (see page 2436) you frequently use so that you do not have to enter the search criteria each time you use the search.

- Copy a search (see page 2438) and use the search as a template for creating another search that is similar.

- Export search results (see page 2439) for use in spreadsheet applications or reports.

- Configure your searches (see page 2447).

Search Security

Default searches let you find objects in the repository. For example, use the default searches to find assets, models, contacts, and so forth. The security for the default searches makes them available to all users and configurations. You can use these searches to create additional *user-defined searches*.

Consider the following security information for user-defined searches:

- All users that are assigned to a role and configuration can access the default searches and the user-defined searches that are assigned to the role and configuration. However, the search results that you see for the default searches do not display information and fields that your CA APM administrator hides and secures.

- When you configure the user interface and restrict access to any field that a search uses, or delete an extended field that a search uses, the search is invalid. As a result, the search is not available to any user that is associated with the role and configuration.

- Invalid and active searches appear together when you manage searches. When you try to use an invalid search, you receive a message. You should contact your CA APM administrator to troubleshoot the invalid search and make the search valid again.

- When a search becomes invalid, you may have no default search. When attempting to search, you receive a message. You should contact your CA APM administrator to have a default search assigned, or you can save a new search and set the search as your default search.

Example: Limit Asset Searches by Cost Center and General Ledger Code

In this example, an asset in your organization is assigned to a particular cost center and general ledger code. This information is used to identify the department responsible for the expense, and to allocate costs on order releases, shipments, and payment invoices. This information is sensitive and should not be available to all users who search for assets in your repository.

You can copy the default asset search and configure the search by adding the cost center and general ledger code to both the search criteria and search results. When you save the new configured search, you assign the search to only those individuals in your finance and procurement department (that is, users assigned to the finance user role). Users in the finance user role can now search and find assets based on the cost center and general ledger code. Users not assigned to this role cannot search for an asset using that information.

Search for Objects

At any time, you can search to find objects in the repository to manage. For example, you can search for a model and define an asset from the model. Based on the search criteria that you specify, a list of matching models appear in the search results.

To search for objects

1. Click the tab and optional subtab for the object that you want to find.

   In the Search Criteria area, specify the search criteria.

2. (Optional) In the Search Criteria area, click Advanced.

3. Click the Edit icon to specify the search criteria:

   - **Left Parenthesis**
     Determines if left parentheses are used to group search criteria and control the logic of the search. For example, you can select this check box to search for assets in which the asset name is OE001 or both the asset family is Computer and the asset name is Dell.

   - **Operator**
     Determines the standard search operators (see page 2435) to use to find objects. For example, you can search for assets in which the asset name is greater than OE001 and the asset family is Computer.

   - **Value**
     Determines the specific field value that you want to find. For example, you can search for an asset in which the asset name is OE001.

     Note: When you enter a search value in combination with the Like or Not Like operators, you can use all supported wildcard characters to expand your search.

   - **Right Parenthesis**
     Determines if right parentheses are used to group search criteria and control the logic of the search. For example, you can search for assets in which the asset name is OE001 or both the asset family is Computer and the asset name is Dell.

- **Connector**
  Determines the standard connectors (see page 2435) to use to find objects. For example, you can search for assets in which the asset name is OE001 or both the asset family is Computer and the asset name is Dell.

4. Click the Complete icon to accept your search criteria changes.

5. Click Go.
   A list of matching objects appears in the search results.

Search Operators

When you search for objects, CA APM lets you use the following standard search operators to find objects in the repository:

Operator	Description
Equal	Search for objects having the exact value specified.
Not Equal	Search for objects not matching the value specified.
Greater Than	Search for objects greater than the value specified.
Greater Than or Equal	Search for objects greater than or equal to the value specified.
Less Than	Search for objects less than the value specified.
Less Than or Equal	Search for objects less than or equal to the value specified.
Like	(Similar) Search for objects that match the value specified. When you use the Like search operator, the % wildcard is added after the characters you enter and searches for all objects that start with the characters. You can also add the % wildcard before the characters to search for all objects that end with the specified characters.
Not Like	(Not Similar) Search for objects that do not match the value specified. When you use the Not Like search operator, the % wildcard is inserted after the characters you enter and searches for all objects that do not start with the characters. You can also insert the % wildcard before the characters to search for all objects that do not end with the specified characters.

Search Connectors

When you search for objects, CA APM lets you use the following standard AND/OR connectors to connect search strings and find objects in the repository.

- **AND**
  The search must satisfy the criteria for both the current search field and the following search field.

- **OR**
  The search must satisfy the criteria for either the current search field or the following search field.

Sort the Search Results

CA APM lets you sort the search results to help make it easier for you to find the information in your search results. For example, you can sort the results in ascending order by asset family to find assets in the hardware asset family first, followed by assets in the software family.

To sort the search results

1. Search for objects.
   The search results appear.

2. In the Search Results area, click the appropriate icon next to a column heading.
   The sort results appear in either ascending or descending order.

> **Note:** You can extend the default sort of a single column by adding sort fields.

Save a Search

CA APM lets you save a search that you frequently use so that you do not have to enter the search criteria each time you use the search. For example, you can save a search to find assets by asset name, asset family, model, cost center, and creation date.

To save a search

1. Click the tab and optional subtab for the object that you want to find.

2. On the left, click New Search.
   The Add Fields dialog appears.

3. Specify the fields to appear in the search criteria and results.

> **Note:** When you search within multiple asset families and legal template types, only the assets, models, and legal documents for the selected families and template types appear in the search results.

4. At the top of the page, click CONFIGURE SEARCH: OFF.
   The configuration of the search is complete.

5. In the Search Details area of the page, specify the information to uniquely identify the search.

Note: When you save a search and specify a title, the title must be unique within a tenant. You cannot save a search with the same title in a single tenant.

6. In the Search Security area of the page, select the user roles for which the search is available. Roles are helpful so you can make the search available to all users having the roles you select. Administrators can also select specific configurations for the search.

Note: If you do not select either a role or configuration, the search is available to the current user.

7. Click Save.
   The search is saved and is available for future searches.

Update a Search

CA APM lets you change the search criteria in a saved search. For example, you can add the contact ID to a saved asset search.

To update a saved search

1. Click the tab and optional subtab for the object that you want to find.

   On the left, click Manage Searches.

   A list of saved searches displays.

2. Click the search that you want to update.

3. Update the search criteria.

4. (Optional) In the Search Security area of the page, select the user roles for which the search is available. Roles are helpful so you can make the search available to all users having the roles you select. Administrators can also select specific configurations for the search.

Note: If you do not select either a role or configuration, the search is available to the current user.

5. Click Save.
   The updates to the search are saved and available for future searches.

Search for Objects Using a Saved Search

CA APM lets you search for objects using a saved search. For example, you can use a saved weekly asset search to find all assets that have been added during the past week.

To search for objects using a saved search

1. Click the tab and optional subtab for the object that you want to find.

   On the left, click Manage Searches.

   A list of saved searches displays.

2. Click the search that you want to use.

3. Click Go.
   A list of matching objects appears in the search results.

Copy a Search

CA APM lets you copy a saved search and use the search as a template for creating another search that is similar. For example, you can copy the default asset search and add the asset creation date and user ID of the person who created the asset.

To copy a search

1. Click the tab and optional subtab for the object that you want to find.

   On the left, click Manage Searches.

   A list of saved searches displays.

2. Click the search that you want to copy.

3. Click Copy.
   A new search is created based on the copied search.

4. Change the information for the new, copied search.

5. (Optional) In the Search Security area of the page, select the user roles for which the search is available. Roles are helpful so you can make the search available to all users having the roles you select. Administrators can also select specific configurations for the search.

Note: If you do not select either a role or configuration, the search is available to the current user.

6. Click Save.
   The search is saved and is available for future searches.

Delete a Search

CA APM lets you delete a saved search that you do not need. You cannot delete the default searches provided by the product.

To delete a saved search

1. Click the tab and optional subtab for the object that you want to find.

   On the left, click Manage Searches.

   A list of saved searches displays.

2. Click the search that you want to delete.

3. Click Delete and confirm that you want to delete the search.
   The search is deleted.

Search Results Export

Contents

CA APM lets you export the results of an object, asset fulfillment, and audit history search so that you can report on and analyze the search results. For example, the asset manager, purchasing manager, and facilities manager require a weekly report that lists all of the assets that have been added during the past week. Based on this requirement, the administrator configures the search to return the list of assets and schedules the search and export to process at 10 p.m. every Friday. After the search and export processes, the managers receive an email notification that includes a link to the weekly report.

You can export the results of a search to the following formats:

- CSV file (see page 2440)
- Database view (see page 2440)

You can schedule a search and export for a particular time and automatically notify contacts by email so that the contact can access the latest information.

CSV File Export

When you export search results to a CSV file, the export includes the current data found by the search. CA APM lets you use the following methods to export to a CSV file:

- On demand export from a real-time search. This type of search includes the current data.
- Scheduled export from a saved search. This type of search includes the current data found each time you use the search according to the schedule.

Example: Export a Search for New Assets to a CSV File

In this example, a company adds new assets to its repository every week. The asset manager, purchasing manager, and facilities manager require a weekly report that lists all of the assets that have been added during the past week. Based on this requirement, the administrator configures the search to return the list of assets and schedules the search and export to process at 10 p.m. every Friday. After the search and export processes, the managers receive an email notification that includes a link to the weekly report.

Database View Export

When you export search results to a database view, the export contains the SQL statement that defines the columns and data in the search. The view does not collect data until you (or an external application) access and use the view in the database.

You can schedule the export from a saved search to export to a database view.

Example: Export a Search for Expiring Assets to a Database View

In this example, a company develops an external dashboard application that monitors asset allocation. The asset manager views the dashboard daily to verify that expiring assets are allocated properly - reallocated, retired, or returned to vendor. The company wants to configure the dashboard application to display CA APM asset data.

Based on these requirements, the administrator configures the search to display the list of expiring assets and their status and exports the search results to a database view. The administrator schedules the search and export to process weekly. The external dashboard application accesses the database view to gather the asset data, and the asset manager views the data in the external dashboard.

How Exporting Search Results Works

When you export search results to a *CSV file*, the process uses the following general steps:

1. The user defines a new search and exports the results; or the user accesses an existing saved search and schedules the export.
2. The search processes and the results include the current data.

> **Note:** The results for a scheduled search and export only include the results found by the current search and export. If you change the search or any part of the export criteria, you will not see the new search results until the next time the search and export process runs. For example, if you change the Export Format from CSV File with Column Headers to Database View or you change the Frequency of the Export Schedule, you do not see those changes in the current search and export.

1. The search results data is saved to a CSV file. The column heading labels in the CSV file (if requested with the export) match the column heading labels from the search results. If the user configured the default column heading labels in the search results, the configured labels are included in the CSV file.

2. An email notification is sent to the users assigned to the search. The email includes a link to the CSV file.

When you export search results to a *database view*, the process uses the following general steps:

1. The user accesses an existing saved search and schedules the export.

2. The search processes and the database view is exported. The column heading labels in the database view match the column heading labels from the search results. If the user configured the default column heading labels in the search results, the configured labels are included in the database view.

> **Note:** The results for a scheduled search and export only include the results found by the current search and export. If you change the search or any part of the export criteria, you will not see the new search results until the next time the search and export process runs. For example, if you change the Export Format from CSV File with Column Headers to Database View or you change the Frequency of the Export Schedule, you do not see those changes in the current search and export.

3. An email notification is sent to the users assigned to the search. The email specifies the name of the database view.

Export Search Results to a CSV File (On Demand)

CA APM lets you export the results of a search to a CSV file by searching for objects and exporting the results on demand or by scheduling a saved search and exporting the results.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to find.

2. Search for objects by entering search criteria or by selecting a saved search.
   A list of matching objects appears in the search results.

3. Click Export to CSV.
   The search results are exported. The column heading labels in the CSV file match the column heading labels from the search results. An email notification with a link to the CSV file is sent to all contacts associated with the export request.

Export Search Results to a Database View

CA APM lets you export the results of a search to a database view by scheduling a saved search and exporting the results.

Follow these steps:

1. Click the tab and optional subtab for the object for which you want to schedule a search and export.

2. On the left, click Manage Searches.
   A list of saved searches appears. If there are no saved searches, define and save a search that you want to schedule and export.

3. Click the search that you want to schedule and export.

4. On the left, click New Export.

5. Enter the basic information, schedule information, and security information as described in the steps to schedule the search and export.
   The search is processed and the results are exported according to the schedule. The column heading labels in the database view match the column heading labels in the search results. An email notification specifying the database view name is sent to all contacts associated with the export request.

Note: The results for a scheduled search and export only include the results found by the current search and export. If you change the search or any part of the export criteria, you will not see the new search results until the next time the search and export process runs. For example, if you change the Export Format from CSV File with Column Headers to Database View or you change the Frequency of the Export Schedule, you do not see those changes in the current search and export.

Schedule Searches and Exports

CA APM lets you schedule searches to process periodically and export the search results to a CSV file or a database view. For example, you can schedule a search to process at the end of the week and export all updated assets during that week to a CSV file. You can schedule the following types of searches:

- **Predefined**. Specify a recurring time for the search. For example, you can process the search at 3:00 p.m. on the 21st of every month.

- **Calculated**. Specify the start time and frequency for the search. For example, you can process the search at 10:00 p.m. on the 21st of September and use the search every five days thereafter.

Follow these steps:

1. Click the tab and optional subtab for the object for which you want to schedule a search.
2. On the left, click Manage Searches.
   A list of saved searches appears. If there are no saved searches, define and save a search that you want to schedule and export.
3. Click the search that you want to schedule.
4. On the left, click New Export.
5. Enter the basic export information.
   The following fields require explanation:

   - **Export Name**
     Specify the export name.
   - **Export Format**
     Select the format for the exported search results.
   - **View Name**
     Specify the database view name.

     Note: The View Name is required if you select Database View for the Export Format. The name must be a valid database view name. See your database product documentation for information about database view name requirements.
   - **Description**
     Specify a description for the exported search results.
   - **Retention Days**
     Specify the number of days that the exported search results are retained before the results are purged.
   - **Folder Name**
     Specify the folder for the exported CSV file search results.
   - **Never Expires**
     Select this check box to specify that the number of days of the selected period (Period Type) that the CSV file or database view is stored before being deleted never expires (the CSV file or database view is never purged). When you select this check box, any previous value that you added to the Retention Days field is removed, and the Retention Days field is disabled.
6. Schedule the search.
   The following fields require explanation:

- **Run Time**
  Select the time of the day, in 24-hour format, to process the search. When you schedule searches, use the local time zone on the CA APM application server.

- **Interval Type**
  Select the type of interval for the search. For example, you can select Day, Month, Quarter, Week, or Year.

- **Interval Day**
  Specify the day during the Interval Type to process the search. For example, if the Interval Type is Month and the Interval Day is 1, the search is processed on the first day of the month.

- **First Run Date**
  Select the date when the first search starts to process.

- **Interval**
  Specify how often the search processes, based on the specified Interval Type. For example, if the Interval Type is Weekly and the Interval is 2, the search processes every two weeks.

- **Last Day of Interval**
  Select this check box to specify that the search processes on the last day of the selected Interval Type. When you select this check box, any previous value that you added to the Interval Day field is removed, and the Interval Day field is disabled.

7. Specify whether all roles and configurations assigned to the search receive the exported search results.

8. Click Save.
   The search is saved. The search processes at the scheduled time and the search results are exported.

Note: The results for a scheduled search and export only include the results found by the current search and export. If you change the search or any part of the export criteria, you will not see the new search results until the next time the search and export process runs. For example, if you change the Export Format from CSV File with Column Headers to Database View or you change the Frequency of the Export Schedule, you do not see those changes in the current search and export.

How Exported Search Results are Retained and Purged

All exported CSV file and database view search results are retained and purged based on configuration settings you specify when you schedule searches and exports. The exported search results that are no longer needed are purged to release disk space.

The following information describes how exported search results are retained and purged:

- You specify the retention days when you schedule searches and exports. After the retention days elapse, the exported search results (CSV files and database views) are considered expired and are purged.
- The Export Service processes the purge once a day (by default, 5:00 a.m. Universal Time) and purges exported search results based on the specified retention days. Your administrator can configure the purge start time.

  Note: For information about the Export Service configuration settings, see Export Service Configuration Settings (see page 1595).

- The retention period depends on the processing time of the export and the time at which the Export Service purges the search results.

Example: Purge Search Results

In this example, you schedule an asset search named Weekly Asset Search to process every Friday and export all updated assets during the week. You set the retention days to 1 and the export completes at 5:00 p.m. Eastern time. The Export Service is scheduled to purge search results at midnight, Eastern time. Because the search results are less than one day old, the Export Service does not purge them until the next scheduled time (in this example, shortly after midnight the following day).

Search Results Mass Change

Contents

You can perform the following mass changes on a search results list:

- Change the value of a specific field for all objects or for selected objects in the list.
- Add a value to a specific field for all objects or for selected objects in the list that have blank values in that field.

Note: The following restrictions can affect the mass change functions that you can perform:

Configuration restrictions for your user role. For example, if your configuration does not allow you to modify a particular field, you cannot perform mass changes on that field.

- Multi-tenancy. If you have a multi-tenanted environment, the tenant name can be a part of the search results list. However, you cannot perform a mass change on the tenant name.

Example: Perform a mass change on the cost center

A data center administrator wants to assign all assets in the London data center to cost center 3218. The administrator configures the search to return a list of all assets in the London data center. The administrator then performs a mass change to change the cost center assignment for the assets to 3218.

How the Search Results Mass Change Works

When you perform a mass change on a search results list, the process uses the following general steps:

1. The user defines a new search, selects an existing search, or uses the default search.
2. The search processes and the results appear.
3. The user defines the mass change settings for all fields or selected fields and executes the mass change.

   Note: The user must be assigned to a configuration that permits mass changes.

4. The mass change job is created and displayed in the Mass Change Jobs list.
5. The user verifies the status of the mass change job and performs the original search again when the job is completed.
6. The search results list data is updated to show the new field values.

Perform a Mass Change on a Search Results List

You can change specific field values for all or selected objects in a search results list.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to find.
2. Search for objects by entering search criteria or by selecting a saved search.
   A list of matching objects appears in the search results.
3. Leave all objects selected, or clear the Select All check box and select specific object check boxes.
4. Click Mass Change Settings.
5. Click New.
6. Enter the information to define the mass change. The following fields require explanation:

   - **Mass Change Field**
     Specifies the field in the search results that you want to change.

> **Note:** The fields that are included in the search results list are available for selection.

- **Value**
  Specifies the new value for the selected field.

  > **Note:** Leave the Value field blank to specify a null value for a field.

- **Update Only Blank Values**
  Specifies that only blank values in the selected field are updated with the new value for the selected objects.

7. Click the Complete Record Edit icon.
8. (Optional) Click New to define more mass change settings.
9. Click the Mass Change button above the search results list when you have defined all mass change settings.
   A mass change job is created.
10. Click Mass Change Jobs on the left to see the Mass Change Jobs list.

    > **Note:** You can click Go to update the jobs list.

11. Click Status Message for your mass change job to verify when the processing is completed.
12. Click View Log for your selected job in the Mass Change Jobs list after the job is completed.
    The log file provides more information about the mass change job activity.
13. Perform your original search again.
    The search results display the new field values.

How to Configure Searches

This article contains the following topics:

CA APM lets you configure object, asset fulfillment, and audit history searches to simplify how you search for information in the repository. To configure searches, complete the following steps:

- Set a search result limit.
- Make it easier to search by specifying a default search.
- Make it easier to specify search criteria by completing the following tasks:
  - Adding fields
  - Removing fields
  - Moving fields
  - Changing the field name
  - Replacing fields
- Make it easier to find information in the search results by completing the following tasks:
  - Adding columns
  - Moving columns
  - Changing the column label
  - Removing columns
  - Adding sort fields
  - Preventing duplicate records from appearing
  - Preventing the ability to open records

Set a Search Result Limit

When you search for an object and the results are difficult to manage because too many object records appear, you can set a limit. For example, when you search for assets, over 2,000 assets appear in the search results. The results are difficult to navigate, you cannot find the assets you want, and the performance is negatively impacted. Therefore, you set a maximum of 50 object records to return.

Follow these steps:

1. Click the tab and optional subtab for the search that you want to configure.
2. On the left, click Manage Searches.
   A list of saved searches displays.
3. Click a search in the list.

4. In the Additional Settings, Maximum Search Results Returning area, specify the total number of objects to appear.

   Note: For performance reasons, we recommend that you set this value to less than 500.

5. Click Go.
   The limited search results appear and help you see the impact on the results before you save the limit. All future search results are limited to the specified number or percentage.

Specify a Default Search

CA APM lets you specify a search that you frequently use as the default each time you click a tab or subtab. For example, to find the contact search you click Directory, Contact. You copy the contact search, rename it, and then set it as your default. The next time you access the Contact Search page, the default search appears instead of the previous search.

Note: You cannot specify a search as the default when the search does not have a selectable column in the results.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.
   A list of saved searches appears.
3. Click a search in the list.
4. Click Set As Default.
5. Click Save.
   The search is saved as the default.

Manage Fields

CA APM lets extend or modify your new and saved searches by letting you manage fields in search criteria. Management of fields includes adding, removing, moving, and changing a field in your search criteria. As a result, you can extend or modify the information that appears in your search criteria and results.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to find.

2. On the left, click Manage Searches.
   A list of saved searches appears.

3. Click a search in the list.

4. At the top of the page, click CONFIGURE SEARCH: ON.

5. Complete the following steps to add a field.

   a. Click Add Fields.

   b. Select the fields to add to the search criteria, results, or both.

   > **Note:** You can add fields to a new and saved search. You cannot add fields to the default searches provided by the product.

6. (Optional) To move a field complete the following step:

   a. Drag-and-drop the field to a new location in the search criteria.
      The new location of the field is saved.

7. (Optional) To remove, replace, and change a field, complete the following steps:

   a. In the search criteria area of the page, click Advanced.

   b. Click the Mark for the Deletion icon next to the field you want to remove from the search criteria.
      The field is removed.

   c. Click the Search icon next to the field that you want to replace with a different field.

   d. Select the replacement field and click OK.
      The field is replaced.

   e. Click the Edit Record icon next to the field for which you want to change the label.
      Enter the new field label.

   f. Click the Complete Record Edit icon.
      The field name is changed.

8. At the top of the page, click CONFIGURE SEARCH: OFF.
   The configuration of the search is complete.

9. Click Save.
   The addition, movement, removal, replacement, and name change of a field is completed.

Manage Columns in Search Results

CA APM makes it easier for you to find the information you need in search results by letting you manage columns in search results. Management of columns includes adding, removing, moving, and changing a column in your search result. As a result, you can easily find the information in your search results.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.
   A list of saved searches appears.
3. Click a search in the list.
4. At the top of the page, click CONFIGURE SEARCH: ON.
5. Complete the following steps to add a column.
   a. Click Add Fields.
   b. Select the fields to add to the search results.

   > **Note:** You can add columns to a new and saved search. You cannot add columns to the default searches provided by the product.

6. (Optional) To move a column complete the following step:
   a. In the search results list, drag-and-drop the column to a new location.
      The new location of the column is saved.
7. (Optional) To remove a column and change a column label, complete the following steps:
   a. In the search results, click the appropriate icon for the Deletion next to the column.
      The column is removed.
   b. In the search results, select the column heading and enter the new label.
8. At the top of the page, click CONFIGURE SEARCH: OFF.
   The configuration of the search is complete.
9. Click Save.
   The addition, movement, removal, and change of a column is completed.

Add a Sorting Field

CA APM lets you add sorting fields to the search results and extend the default sort of a single column using either ascending or descending order. For example, you currently sort assets by asset name. You can add asset family to the sorting so that you can sort on both asset name and asset family.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.
   A list of saved searches displays.
3. Click a search in the list.
4. In the Additional Settings, Search Results Sorting area, add the additional field for sorting.
5. Click Go.
   The results appear with the extended sorting and help you see the impact on the results before you save the sorting. The new field is added and you can use the field to sort the search results.

Prevent Duplicate Object Records

CA APM lets you prevent duplicate object records from appearing in the search results. For example, you have several people in your enterprise with the name John Smith. Their first and last names are the same, but their additional contact information (email address, supervisor, department, and so forth) is different.

You have a saved contact search in which only the first and last name of the contact appears in the results. When you search using the saved contact search and specify *John* as the first name and *Smith* as the last name, two instances of John Smith appear in the search results. When you prevent duplicate records from appearing, only one instance of John Smith appears.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.
   A list of saved searches displays.
3. Click the search for which you want to prevent duplicate records from appearing.
4. In the Additional Settings, Unique Search Characteristics area, select the Make Results Unique check box.
5. Click Go.
   The results appear without the duplicate records and help you see the impact on the results before you save your settings. The DISTINCT argument is added to the SQL statement, preventing duplicate records from appearing in the search results.

Prevent Opening Records

CA APM lets you disable the ability to open individual records from the search results. For example, you do not want users to open and display contact information from the contact search results.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.
   A list of saved searches displays.
3. Click a search in the list.
4. In the Additional Settings, Unique Search Characteristics area, clear the Allow Selection of Results check box.
5. Click Save.
   A hyperlink does not appear in the search results to open the object.

Software Asset Management

This section contains the following articles:

Software License Management

CA APM provides visibility into the software environment in your organization by tracking detailed information about software licenses. This information includes internal allocations (locations, companies, contacts, and assets), payment history, purchasing information, and the location of hard copy license agreements or attachments of the relevant license and payment documents required by an audit.

Software license management in CA APM involves working with the following objects:

- Software internal allocations (see page 2454)
- Software assets (see page 2457)

Important! We do not recommend that you manage software assets in CA APM. To take advantage of the enhancements that this release provides, we recommend that you use CA SAM to manage your software assets and licenses.

For more information, see SAM Documentation (https://support.ca.com/irj/portal/newhome).

Software Internal Allocations

This article contains the following topics:

A *software internal allocation* describes how your organization is internally approved to use a software asset, as specified in your software license agreement. For example, a license can stipulate that the software can be used only on a particular computer, or that a limited number of users can use the software at one time.

You track and maintain allocations in CA APM using an allocation record. Define an allocation record for any software asset in your repository.

CA APM lets you record an allocation in the following ways:

- For a software asset, you can add, edit, or delete a relationship to a hardware asset on which the software is internally approved for use.
- For a hardware asset, you can edit or delete information about an allocation that is specific to that hardware asset.

Note: Internal allocations are not legal restrictions. Legal information, including software usage constraints, can be maintained in legal document records and in CA SAM.

Add a Location Allocation

CA APM lets you add a location allocation to list the places where your organization is internally approved to use a software asset, as specified in your software license agreement. For example, you are licensed to use 100 copies of version 4.0 of a software product in your North American office.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Asset.
2. Search to find the list of available assets.

3. Click the software asset for which you want to add a location allocation.
4. On the left, expand Relationships and click Location Allocation.
5. Click Select New to search for and select a location.
6. Click the Edit Record icon and enter the location allocation details.
7. Click Save.
   The location where your organization is internally approved to use the software asset is added.

Add a Company Allocation

CA APM lets you add a company allocation to list the subsidiary companies where your organization is internally approved to use a software asset, as specified in your software license agreement. For example, you are licensed to use 25 copies of version 4.0 of a software product in a sales office.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Asset.
2. Search to find the list of available assets.
3. Click the software asset for which you want to add a company allocation.
4. On the left, expand Relationships and click Company Allocation.
5. Click Select New to search for and select a company.
6. Click the Edit Record icon and enter the company allocation details.
7. Click Save.
   The company where your organization is internally approved to use the software asset is added.

Add a Contact Allocation

CA APM lets you add a contact allocation to list the people who are internally approved to use a software asset, as specified in your software license agreement. For example, the members of your IT department are licensed to use ten copies of version 4.0 of a software product in a development office.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Asset.
2. Search to find the list of available assets.
3. Click the software asset for which you want to add a contact allocation.
4. On the left, expand Relationships and click Contact Allocation.
5. Click Select New to search for and select a contact.
6. Click the Edit Record icon and enter the contact allocation details.
7. Click Save.
   The contact who is internally approved to use the software asset is added.

Add an Asset Allocation

CA APM lets you add an asset allocation to list the hardware assets on which your organization is internally approved to use a software asset, as specified in your software license agreement. For example, the members of your IT department are licensed to use 10 copies of version 4.0 of a software product on their Dell Precision Workstation 410 computers.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Asset.
2. Search to find the list of available assets.
3. Click the software asset for which you want to add an asset allocation.
4. On the left, expand Relationships and click Asset Allocation.
5. Click Select New and select a different hardware asset, other than the asset previously selected.
6. Click the Edit Record icon and enter the asset allocation details.
7. Click Save.
   The hardware asset on which your organization is internally approved to use the software asset is added.

Delete an Allocation

CA APM lets you delete the details of an allocation record. For example, your organization purchases Adobe Acrobat Professional and internally allocates the licenses to 100 users. One user does not need the license. Therefore, you remove the software from the computer and delete the allocation. By completing these steps, you make the license available to another user in a new allocation record.

Follow these steps:

1. Click Asset.
2. Search to find the list of available assets.
3. Click the software asset for which you want to delete the allocation.
4. On the left, expand Relationships and click the appropriate allocation type.
   The allocation list appears.
5. Click the Mark for Deletion icon next to the allocation that you want to delete.
6. Click Save.
   The allocation record is deleted.

Software Assets

CA APM lets you track and manage licensing information for *software assets* that your company is entitled to use. The following fields on the Asset Details page represent the licensing information that you can manage for software assets:

- License Class
- License Count
- License Key
- License Duration
- License Duration Units

You can define and maintain this license information for software assets only.

Vendor Management

Take control of your vendor relationships by understanding their interdependencies between your organization and among one another. CA APM lets you track and manage detailed information about the vendors with whom you do business, including contact information and their relationships to other companies. You can gather complete information about the total amount of money spent and what you will spend with a vendor, allowing you to negotiate product prices and purchases with your vendors.

Vendor management in CA APM involves working with the following objects:

Directories

Directory information is maintained in the repository so that you can locate the contact, company, location, and organization information you need for your IT assets. Having a directory offers you consistency for all of your assets to help make analysis easier. In addition, the directory serves as a contact repository when you must contact someone associated with an asset.

Companies

This article contains the following topics:

A *company* buys, sells, services, manages, or uses your IT assets in CA APM. You define company records for key organizations with which you have a business relationship, such as the following examples:

- Your own company, its parent company, or subsidiaries.
- IT manufacturers, vendors, escrow agents, maintenance providers, and service providers.

Before you define a company record, you must define records for the parent company, if any, and the default location, such as the headquarters. This additional information makes it easier to enter the information when defining the company record.

You can have multiple associations between locations and companies. These associations are useful to track companies with worldwide offices. For example, to track the contact details of a large vendor with worldwide offices, define location records for each office and associate them with the company record of the vendor.

You can specify one of the locations as the default location. The default location can be the headquarters of the company or the location that you contact most frequently.

Note: Although associating locations is not mandatory, it is considered good practice. Location records must exist in your repository before you can select locations for any objects.

You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

Manage Companies

You can define, update, and delete company records for key organizations with which you have a business relationship. For example, you can define a company as an IT manufacturer, vendor, escrow agent, maintenance provider, or service provider.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click Directory, Company.
2. Perform one of the following actions.
3. Define a company.
    a. Click New Company.
    b. Enter the new company information and click Save.

    Note: You can also define a company by copying an existing company, supplying a new name, changing the information, and saving the new company.

4. Update a company.
    a. Search for the list of available companies.
    b. Click the company that you want to update.
    c. Enter the new information for the company and click Save.

Note: You can also view the details for an object that is related to your company, if the related object has a Browse icon. When you click the Browse icon, you leave the company page and you navigate to the related object page. To keep the company page in view and preserve the company information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.

5. Delete a company.
    a. Search for the list of available companies.
    b. Click the company that you want to delete.
    c. Click Delete and confirm that you want to delete the company.

Associate Locations to a Company

Associating multiple locations to a company is a recommended best practice to track companies with worldwide offices. For example, you can associate your company with the North America office, Latin America office, Asia Pacific office, and European office. Location records must exist before you can associate the location with a company.

Follow these steps:

1. Click Directory, Company.
2. Search for the list of available companies.
3. Click the company that you want to associate with multiple locations.
4. Click Locations on the left.
5. Click Select New to display the list of all available locations.
6. Select the company locations.
7. Click Save.

Add an Acquired Company

CA APM lets you maintain the details of the companies that you acquire and track acquisitions made by external companies. This information is useful when tracking the association between parent and subsidiary companies. For example, to understand the relationship between two companies, you can review the list of acquired companies.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Directory, Company.

2. Search for the list of available companies.
3. Click the company to which you want to add an acquired company.
4. Expand Relationships on the left and click Company Acquisition.
5. Click Select New and select a different company, other than the company previously selected.
6. Click Save.
   The acquired company is added to the list.

Add a Company Allocation

You can add a company allocation to list the software assets that your organization is internally approved to use, as specified in your software license agreement. For example, you are licensed to use 25 copies of version 4.0 of a software product in a sales office.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Directory, Company.
2. Search for the list of available companies.
3. Click the company for which you want to add a company allocation.
4. Expand Relationships on the left and click Software Allocation.
5. Click Select New to search for and select an asset.
6. Click the Edit Record icon and enter the company allocation details.
7. Click Save.
   The software asset that your company is internally approved to use is added.

Contacts

This article contains the following topics:

A *contact* is a person or department who buys, sells, services, manages, or uses your IT assets in CA APM. Define contact records for key individuals and departments in which you have a business relationship, such as the following examples:

- Users, asset management staff, contract administrators, and IT staff.

- Representatives of other companies, such as manufacturers, vendors, escrow agents, maintenance, and service providers.

Before you define a contact record, define a company record (see page 2459) to associate with the contact. Having the company record available makes it easier to add the company information when you are defining the contact record.
You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

Manage Contacts

You can define, update, and delete contact records for key people or departments in which you have a business relationship. For example, you can define contacts as asset management staff, contract administrators, IT staff, manufacturers, vendors, and service providers.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click Directory, Contact.
2. Perform one of the following actions.
3. Define a contact.
    a. Click New Contact.
    b. Enter the new contact information.
    c. Click Save.

    Note: You can also define a contact by copying an existing contact, supplying a new name, changing the information, and saving the new contact.

4. Update a contact.
    a. Search for the list of available contacts.
    b. Click the contact that you want to update.
    c. Enter the new information for the contact.
    d. Click Save.

Note: You can also view the details for an object that is related to your contact, if the related object has a Browse icon. When you click the Browse icon, you leave the contact page and you navigate to the related object page. To keep the contact page in view and preserve the contact information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.

5. Delete a contact.
    a. Search for the list of available contacts.
    b. Click the contact that you want to delete.
    c. Click Delete and confirm that you want to delete the contact.

Add a Contact Allocation

You can add a contact allocation to list the software assets that people in your organization are internally approved to use, as specified in your software license agreement. For example, the members of your IT department are licensed to use ten copies of version 4.0 of a software product in a development office.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Directory, Contact.
2. Search for the list of available contacts.
3. Click the contact for which you want to add a contact allocation.
4. Expand Relationships on the left and click Software Allocation.
5. Click Select New to search for and select an asset.
6. Click the Edit Record icon and enter the contact allocation details.
7. Click Save.

Organizations

This article contains the following topics:

An *organization* is an internal department. CA APM lets you assign organizations to assets, locations, and contacts. For example, use an organization to identify the department for which an employee works.

Note: Administrators or users with administrative privileges can manage organizations. In addition, if you are using CA Service Desk Manager, you do not have to create the organization. You can use the information from the service desk.

You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

Manage Organizations

You can define, update, and delete an organization for an internal department, division, or external company. For example, you can define an organization for research and development, corporate finance, worldwide law, or global human resources.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click Directory, Organization.
2. Perform one of the following actions.
3. Define an organization.
    a. Click New Organization.
    b. Enter the new organization information.
    c. Click Save.

    Note: You can also define an organization by copying an existing organization, supplying a new name, changing the information, and saving the new organization.
4. Update an organization.
    a. Search for the list of available organizations.

b. Click the organization that you want to update.

c. Enter the new information for the organization.

d. Click Save.

Note: You can also view the details for an object that is related to your contact, if the related object has a Browse icon. When you click the Browse icon, you leave the contact page and you navigate to the related object page. To keep the contact page in view and preserve the contact information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.

5. Delete an organization.

a. Search for the list of available organizations.

b. Click the organization that you want to delete.

c. Click Delete and confirm that you want to delete the organization.

Locations

This article contains the following topics:

A *location* is a place where assets, companies, contacts, and legal documents are placed or situated. CA APM lets you associate locations with assets, companies, and contacts. You can define locations for the following objects:

- Assets
- Company offices and other locations where you track IT assets.
- Manufacturing companies, vendors, escrow agents, maintenance, and service providers.
- Contacts within and outside the company.

You can define multiple associations between locations and companies. The associations are useful when you want to track a large vendor with worldwide offices. For example, to track the contact details of a large vendor with worldwide offices, you can define location records for each office and associate them with the company record of the vendor. You can define location records for each office and associate them with the vendor company record.

You can specify one of the locations as the default location. The default location can be the headquarters of the company, or the location that you contact most frequently.

Note: Although associating locations is not mandatory, it is considered a best practice. Location records must exist in your repository before you can select locations for any objects.

You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

Manage Locations

You can define, update, or delete a location to manage the addresses of assets, contacts, and companies. For example, you can define the address for your North American office, Latin America office, and Asia Pacific office.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Directory, Location.
2. Perform one of the following actions.
3. Define a location.
    a. Click New Location.
    b. Enter the new location information.
    c. Click Save.

    Note: You can also define a location by copying an existing location, supplying a new name, changing the information, and saving the new location.

4. Update a location.
    a. Search for the list of available locations.
    b. Click the location that you want to update.
    c. Enter the new information for the location.
    d. Click Save.

Note: You can also view the details for an object that is related to your location, if the related object has a Browse icon. When you click the Browse icon, you leave the location page and you navigate to the related object page. To keep the location page in view and preserve the location information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.

5. Delete a location.
    a. Search for the list of available locations.
    b. Click the location that you want to delete.
    c. Click Delete and confirm that you want to delete the location.

Associate Companies to Locations

Associating companies to locations is a best practice to track companies with worldwide offices. For example, you can associate your company with the North America office, Latin America office, Asia Pacific office, and European office.

Follow these steps:

1. Click Directory, Location.
2. Search for the list of available locations.
3. Click the location that you want to associate with companies.
4. Click Companies.
5. Associate the new location with the company.
6. Click Save.

Add a Location Allocation

You can add a location allocation to list the software assets that the locations in your organization are internally approved to use, as specified in your software license agreement. For example, you are licensed to use 100 copies of version 4.0 of a software product in your North American office.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Directory, Location.
2. Search for the list of available locations.

3. Click the location for which you want to add a location allocation.
4. Expand Relationships on the left and click Software Allocation.
5. Click Select New to search for and select an asset.
6. Click the Edit Record icon and enter the location allocation details.
7. Click Save.
   The software asset that the location is internally approved to use is added.

Sites

This article contains the following topics:

A *site* is a group of locations, which lets you use the new site in the location. For example, a site can be a city in which your enterprise has one or more physical locations, or a region in which you have customers that you support.

For more information about defining date-specific and non-date-specific terms and conditions for legal documents, see Define Legal Document Terms and Conditions (see page 1535).

You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

Manage Sites

You can define, update, and delete sites. Sites specify groups of locations, such as a city in which your enterprise has one or more locations, or a region in which you have customers.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click Directory, Site.
2. Perform one of the following actions.
3. Define a site.
   a. Click New Site.
   b. Enter the new site information.
   c. Click Save.

Note: You can also define a site by copying an existing site, supplying a new name, changing the information, and saving the new site.

4. Update a site.
    a. Search to find the list of available sites.
    b. Click the site that you want to update.
    c. Enter the new information for the site.
    d. Click Save.

Note: You can also view the details for an object that is related to your site, if the related object has a Browse icon. When you click the Browse icon, you leave the site page and you navigate to the related object page. To keep the site page in view and preserve the site information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.

5. Delete a site.
    a. Search to find the list of available sites.
    b. Click the site that you want to delete.
    c. Click Delete and confirm that you want to delete the site.

Configuration Management

This section contains the following articles:

Configuration Items

Contents

Configuration items are the devices, software, and services that make up your business infrastructure. The information that is associated with a configuration item uniquely identifies the configuration item and indicates its precise location. Configuration items can be associated with contacts (private configuration items) and organizations (shared configuration items). Configuration items let you:

- Identify configuration items by name, class, and family.
- Specify inventory information.
- Specify additional properties to define the configuration item.
- Log and view comments that are associated with the configuration item.
- Specify location information for the configuration item.
- Specify service information, such as a service type, for the configuration item.
- View and define contacts and organizations that are assigned to the configuration item.**CMDB Attributes**
- Identify hierarchical and peer-to-peer relationships between configuration items.
- View tickets that are associated with the configuration item.

You are not required to define all this information for configuration items. Defining an optimal amount of configuration item information gives you a clearer picture when you perform impact analysis for the organization.

Important! You can attach configuration items only if they are Active. You cannot search for an Inactive CI when working on a ticket.

Important! Depending on your role, you do not have access to all the functionality described in this section. For example, some predefined roles can edit records but cannot create new ones.

Depending on your role, you can perform user and administration tasks on configuration items (CIs) by using the following features:

- Scoreboards allow you to perform user tasks and manage CIs and CI relationships.
- The Administration tab lets you perform administration tasks with CIs and relationships.
- CMDB Visualizer lets you perform user and administration tasks for visualizing CIs and relationships.

Create a Configuration Item

You can create a configuration item to be linked to tickets. Configuration items give analysts information about the entities that tickets affect.

Follow these steps:

1. On the Scoreboard, select File, New Configuration Item on the menu bar.
2. Enter a name and class for the configuration item.
   The class is a unique identifier that categorizes the CI class you are adding to the database. You can enter a class directly into the field or click the search icon to search for a defined class.
3. Click Continue and complete the Configuration Item fields (see page) as appropriate.
4. Click Save.

   The configuration item definition is saved and the Configuration Item Detail page appears. After you create a CI, the CI Detail page does not display some identifying attributes in the following cases:

   - The attributes have no associated value.
   - The attributes do not apply to the CI family.

However, identifying attributes with non-blank values always display. Configuration Item Detail pages identify a CI and determine which type of page appears so that you can create or manage the CI. CI Name and the CI Class are required. An asterisk (*) identifies a field that is required. If you use change verification (see page 2643), informational messages appear at the top of the detail form.

When you assign the new CI to a CI class, the CI family is automatically assigned (because a class is already associated with a family). When you click Continue on the initial Create New Configuration Item page, the appropriate CI page appears, depending on the family.

Note: A notification appears for successful and unsuccessful changes. A warning message is displayed for an unsuccessful change indicating the policy, attribute, and the corresponding action that occurred.

The following buttons are available for viewing configuration item information:

Asset Viewer: Opens the Common Asset Viewer. The viewer displays a detailed view of the configuration item that includes all properties that are managed or discovered.

Affected Tenants: Displays the tenants that are affected by this CI, based on its associated contacts and organizations.

Note: This button only appears when multi-tenancy is installed.

CMDBf Viewer: Displays the Federated View, a side by side view of CI attributes across registered MDRs.

Visualizer: Opens the Visualizer, which displays a graphical representation of the configuration item showing its relationship to other resources.

Configuration Item Fields

The following fields are required to create or update or search for a CI:

- **Family**
  Categorizes the classes of CIs.
- **Standard CI**
  Configuration item that is used for comparison.
- **Host Name**
  Identifies the IP host name of the CI.
- **MAC Address**
  Identifies the Media Access Code for the device. This field is automatically filled when the system creates a record for a device it detects.

- **Alt CI ID**
  Specifies the alternate identifier for a CI; for example, a barcode.

- **DNS Name**
  Identifies the Domain Name System name of the CI.

- **Serial Number**
  Identifies the serial number for the CI. The serial number applies to devices or software.

- **Active?**
  Specifies whether the record is active in the database. The inactive CI records do not appear on display lists.

- **Asset?**
  Categorizes an asset for filtering purposes and to control display in CA CMDB or other products such as CA APM. You cannot change the Asset flag to NO when an asset is managed by CA APM.

- **CI?**
  Categorizes a CI for filtering purposes and to control display in CA CMDB or other products such as CA APM. By default, a CI created by CA CMDB is flagged as a CI but not as an Asset.

- **Superceded By**
  Indicates the CI that has rendered this CI inactive due to its ambiguity.

- **Action**
  Sets or resets the Actual Date/Time to the current date and time.

- **Target**
  Specifies the current Service Target.

- **Target Date/Time**
  Specifies date and time when this Service Target is due. If the ticket is in a Hold status, this value is blank.

- **Actual Date/Time**
  Specifies the time when the target condition was met. If no value appears, the target condition has not been met.\

- **Time Left**
  Specifies the amount of remaining time for the service target when the ticket is on hold. If the Service Target has been met, Time Left shows the unused time. A negative value indicates the time that elapsed since the missed target date.

- **Violation Cost**
  Specifies the incurred cost when the service type time limit is violated.

Note: The CI Detail page does not display identifying blank attributes and attributes that do not apply to the CI family. However, identifying attributes with non-blank values always display.

Configuration Item Tabs

The following tabs can be available on the Create New Configuration Item, Configuration Item Detail, and the Update Configuration Item pages:

CMDB Attributes

- **Attributes**
  Itemizes and manages CI attributes associated with the class that is assigned. The CI Family determines what appears on the Attributes tab.

- **CMDB Relationships**
  Displays the relationships for this CI. All links display the CI Relationship Detail page.

- **Versioning**
  Displays and manages the history of the CI (see page 2497), associated snapshots, milestones, and other views. Versioning also displays pending Change Specifications that are associated with Change Orders. For example, view details about the future state of a CI.

- **Reconciliation**
  Lists all active CIs that are ambiguous with this CI. You can select Exclude Ambiguity to remove this CI from ambiguity calculations and ambiguity management. For more information, see the Reconcile CI Ambiguities Using MDR. (see page 2556)

- **Inventory**
  Stores detailed inventory information about the CI.

- **Service**
  Stores detailed service information that is related to servicing a CI. The following sub-tabs are required for a Service:

  1. **Service Type**: The level of support service received for this configuration item. For example, some items may receive problem resolution within four hours, while problems with others may be resolved within 72 hours. Enter the service type directly, or click the search icon to select the desired type.

  2. **Cost Center**: The code to which expenses related to this configuration item are charged. Enter the cost center directly, or click the search icon to select the desired cost center.

  3. **Responsible Organization**: The organization that is responsible for this configuration item.

  4. **Maintenance Organization**: The organization responsible for the maintenance of this configuration item.

  5. **Priority**: The level of attention given to problems with this configuration item.

  6. **Supply Vendor**: The vendor responsible for maintaining supplies for this configuration item.

  7. **Responsible Vendor**: The vendor responsible for maintaining the service provided by this configuration item.

8. **Maintenance Vendor**: The vendor responsible for the maintenance of this configuration item.

9. **Service Impact**: The level of importance of this service to the business.

Contacts, Location, Organizations

- **Contacts**
  Stores detailed contact information about the contacts responsible for the CI. The following sub-tabs are required for Contacts:

  1. **Primary Contact**: The primary person or group in charge of the CI.
  2. **Phone Number**: The primary telephone number of the person or group in charge of the CI
  3. **Email Address**: The email address of the person or group in charge of the CI
  4. **Billing**: The address that is listed by room number and building
  5. **Support 1**: The first contact for support in charge of the CI
  6. **Support 2**: The second contact for support in charge of the CI
  7. **Support 3**: The third contact for support in charge of the CI
  8. **Disaster Recovery**: The contact for disaster recovery in charge of the CI
  9. **Backup Services**: The contact for backup services in charge of the CI
  10. **Network Operations**: The contact for network operations in charge of the CI

- **Location**
  Stores detailed information about the geographical location of the CI.

- **Organizations**
  Stores detailed organization information about the organizations responsible for the CI.

Related Tickets

Information about related CA SDM tickets is displayed through Incidents, problems, requests, change orders, change specifications, and verification log.

Additional Information

- **Maintenance Windows**
  Displays global maintenance windows that are associated with the CI.

- **Service Contracts**
  Displays information about service contracts that are associated with the CI, to identify the level of support the item receives.

- **Activities**
  Displays the activity log for the CI. You can display the analyst or activity details.

- **Attachments**

  Note: This feature will only be available if you apply a patch for CA Service Management Release 14.1.01. Find the patch and the download details from CA Support Online.

  Enables you to attach documents or URLs with this CI. Depending on the requirement, click Attach Documents or Attach URL and follow the on-screen instructions. The URL or the document is added to the record and is listed on the Attachments tab of the Configuration Item Detail page. A notification is sent to the related contacts of the CI when the attachment is attached successfully. Similarly when an attachment is removed from the CI, a notification is sent.

  Note: CA SDM is integrated with CA IT Asset Management and this CI is also an asset in CA IT Asset Management. If you have added an attachment to this CI from CA SDM, it will not be visible when this CI is viewed in CA IT Asset Management.

Knowledge Management

- **Knowledge**
  Lists the Knowledge documents that are related to the CI.

Inactivate a Configuration Item

If a configuration item is no longer used, you can edit the configuration item details to make it inactive. An inactive status removes the configuration item from the Scoreboard Configuration Item List. You cannot delete a configuration item.

Edit a CI and select Inactive from the Active drop-down list. The configuration item continues to appear in any existing relationships until the relationships are inactivated.

Note: Inactivating a Family or Class does not affect existing CIs in that Family and Class. Inactivating only prevents new CIs from being created in that Family and Class.

Reactivate a Configuration Item

To use a configuration item that is inactive, you can reactivate it. Edit a CI and select Active from the Active drop-down list.

View CI Attributes in Other CA Products

You can use the Common Asset Viewer page to view configuration item attributes in other CA products.

Follow these steps:

1. Locate and open the configuration item.
2. Click Asset Viewer.
   The Common Asset Viewer page appears.
3. Click the links on the Owned Resources tab to locate attribute information from other CA products.
4. Click Close Window when you are done.
   You have viewed configuration item attributes in other CA products.

Add a Discovered Asset

You can change non-owned assets in the Management Database (MDB) into owned configuration items.

Follow these steps:

1. Click the Discovered Assets button on the Configuration Item List page.
   The Discovered Asset Search page appears.
2. Click Search to display the Discovered Asset List.
3. Select the asset from the list that you want to add as a configuration item.
4. Right-click the asset and select Create New Configuration Item from the pop-up menu that appears.
   The Create New Configuration Item page appears with information about the item populating some of the fields.
5. Complete any remaining fields that apply to the new configuration item and click Continue.
6. Enter data as required in the appropriate fields on the Attributes tab.
   The family of the class that you selected for the configuration item determines the attributes that appear on the tab. Your business processes and the information you want to store and view for a configuration item determines the information that you enter here.
7. Click Save.
   The discovered asset is added.

Asset and CI Flags

To categorize the type of CI/asset for filtering purposes and to control what entities are visible in CA SDM or other products such as CA APM, use the following flags:

- **CI? (YES/NO)**
  Identifies configuration items.

- **Asset? (YES/NO)**
  Identifies the assets.

By default, a CI created by CA CMDB is flagged as a CI and not as an Asset. You can override this behavior if necessary. A CI can also be an Asset. CA CMDB does not allow the Asset flag to be changed once it has been set to Yes. The Asset flag is typically set to Yes when CA APM creates an asset.

These flags appear on all CI detail forms and in the CI search facility. The values can be updated in the CI detail form, GRLoader, and CA CMDB web services. The Edit in List feature also supports updating the new flags in multiple records.

The object attribute name for the CI flag is **is_ci**. The object attribute name for the Asset flag is **is_asset**. These names are SREL attributes that reference bool. The attribute names can be used as GRLoader XML tags. For example, to change the default value of the Asset flag when creating a CI with GRLoader, add the following XML to define the new CI:

```
<is_asset>YES</is_asset>
```

Create a CI Company

The companies supply the hardware, software, and services associated with your system.

Follow these steps:

1. From the Administration tab, navigate to Service Desk, Application Data, Configuration Items, Companies.

2. Click Create New and fill in the field information as appropriate.

   - **Company Type**
     The company type assigned to this vendor. For example, a company type of Lessor can be assigned to suppliers leasing out products. A company type of Provider can be assigned to companies offering services. A company type of Vendor can be assigned to companies selling assets.

   - **Primary Contact**
     The name of the person primarily responsible for issues related to this company. This person must be a defined contact in your system.

   - **Alias**
     An alternate name for this company. For example, if the full company name is John Smith Company, Incorporated, you might enter an alias of Smith Company.

   - **Parent Company**
     If this company is part of or a subsidiary of a larger organization, enter the name of that larger organization. The parent company must be a defined company in your system. You can enter the company name directly into this field, or click the search icon to select the company.

A new company is created for CI use.

Create a Company Type

Company types are supplier classification for the hardware, software, and services that are associated with your system. Company Types classification helps to organize and select the vendor on the basis of services provided. From the Administration tab, navigate to Service Desk, Application Data, Configuration Items, Company Types.

Families and Classes

Families classify configuration items by type and assign meaningful attributes for each one. *Classes* identify general categories of configuration items that your enterprise supports. Families are broad categories of configuration items such as hardware, software, and services. Classes are more specific categories within the broader family category. For example, the family hardware could contain classes such as, modem, router, repeater, and bridge.

Organizing your configuration items into families and classes makes it easier to manage your configuration items. For example, you can generate a list of configuration items that belong to a particular family or class.

Create a Configuration Item Class

Configuration item classes are general categories of hardware, software, and services. For example, workstation, printer services. The configuration item classes are grouped into broader categories known as configuration item families.

When you assign the new CI to a CI class, the CI family is automatically assigned (because a class is already associated with a family). When you click Continue on the initial Create New Configuration Item page, the appropriate CI page appears, depending on the family.

Follow these steps:

1. From the Administration tab, navigate to Service Desk, Application Data, Configuration Items, Configuration Item Classes.
2. Click Create New.
3. Fill in the following fields:
   - **Family** -- The Configuration Item Family associated with this Configuration Item Class. Families are broader categories for configuration items than classes. The families include computers, other hardware, software, and services. This field is updated automatically and cannot be modified.
   - **Record Status** -- Status indicates whether the configuration item class is active or inactive.
4. Click Save.

Create a Configuration Item Families

Configuration item families are broad categories you can use to classify your network resources. You can assign configuration item classes to families. By doing this, individual configuration items are automatically assigned to families when they are assigned to classes. The configuration item family controls the kind of record displayed.

Follow these steps:

1. From the Administration tab, navigate to the Configuration Item Families List.

   The Configuration Item Family List page displays.

2. Click Create New.

   The Create New Configuration Item Family page displays.

3. Fill in the following fields:

   - **Record Status** -- Indicates whether the configuration item family is active or inactive.
   - **Extension Name** -- Specifies an extension value related to a physical table name in the database. When you select an extension name in the drop-down list, the Physical Table Name field appears in the read-only Physical Table Name field.

4. Click Save.

Create a Service Status

A service status indicates the disposition of a configuration item (for example, In Service, Discontinued, In Repair, and so on).

Follow these steps:

1. Select Service Desk, Application Data, Configuration Items, Service Status on the Administration tab.

2. Click Create New.

3. Fill in the following fields:

   - **Name**
     A unique identifier for the service status.
   - **Record Status**
     Status whether the service is active or inactive.
   - **Description**
     A detailed description of the service status.

4. Click Save.
   The service status definition is saved and the Service Status Detail page appears.

1. Specifies the contact for Backup Services in charge of the CI.

Configuration Item Events and Logs

Contents

View Configuration Item Event History

You can view a record of significant actions that occur regarding a CI. The event list contains a record of the events that are associated with the CI. You maintain events, or procedures the system follows after a certain amount of time has elapsed. For example, an event can send a notification to an analyst if a CI has been updated.

You can view historical events and the status of a configuration item.

Follow these steps:

1. On the Administration tab, select Service Desk, Application Data, Configuration Items, Configuration Item List.
   The Configuration Item Search page appears.

2. Search for a Configuration Item and select it.

3. Click the Event History button.
   The Event History page displays the events and their status. The following fields require explanation:

   - **Condition**
     Indicates the condition that is checked for by the event. CA SDM provides macros that verify standard conditions such as priorities and object status (open or closed).

   - **Check Time**
     Indicates the time that the event was checked, based on the time parameters that the event configuration specifies.

   - **Time Loaded**
     Indicates the time that the event was loaded, based on the time parameters that the event configuration specifies.

Add Configuration Item Log

You can add log entries to record activities for the configuration item.

Follow these steps:

1. On the Scoreboard, browse to Configuration Items, Active, or Inactive. Select the Priority, Warranty, and Ownership for the configuration item you want to edit.
   The Configuration Item List appears.

2. Select the Configuration Item.
   The Configuration Item Detail page appears.

3. Click Edit.
   The Update Configuration Item page appears.

4. Select the Log tab.
   A list of log entries for this configuration item appears.

5. Click Add Log.
   The Create New Configuration Item Log page appears.

6. Enter the information that you want to record in the log and click Save.
   The Configuration Item Detail page displays the new log entry that is listed on the Log tab.

View Log History

You can view the log entries to see a history of activity for the configuration item.

Follow these steps:

1. On the Scoreboard, browse to Configuration Items, Active, or Inactive. Select the Priority, Warranty, and Ownership for the configuration item you want to edit.
   The Configuration Item List appears.

2. Select the Configuration Item.
   The Configuration Item Detail page appears.

3. Click Edit.
   The Update Configuration Item page displays.

4. Select the Log tab.
   A list of log entries for this configuration item displays.

CI Naming Conventions and Restrictions

CIs have the following naming conventions and restrictions:

- CI Name
  The CI Name is the common or display name that is used in all CI lists. The total length of the name must not exceed 255 characters. The CI name does not need to be unique, but we recommend that it is globally unique. In addition, when MDR determines the name, we recommend that MDR administrators emphasize the human readability factor when populating this field.

- Software CIs
  For third-party software, follow the same naming convention as the names that you manually create using the Administration tab. Matching naming conventions lets CA Cohesion ACM-discovered CIs reconcile to the manually created ones. If you do not follow this convention, you can create multiple CIs with only one software instance.

Use of systemname Attribute
The systemname attribute uniquely associates a *single* CI with a particular host name.
If multiple CIs are imported and specify the same systemname as an existing CI, reconciliation results only one CI.

Example

The following output lines show the creation of a Server CI (provider), a Software CI (dependent), and a *runs* relationship between them:

```
CI:  Name: Server1     Class: Server   Systemname: Server1
CI:  Name: Apache1   ON Server1      Class: Software
Relationship:  Server1 runs Apache1   ON Server1
```

The resulting relationship represents a server that runs Apache software.

Add a Discovered Asset

CA SDM does not operate on the entire set of resources that are stored in any database. Only configuration items (CIs) registered by CA Service Desk Manager are immediately available. From a business process perspective, a help desk is only concerned about supporting *owned* resources that are part of the organization through a purchasing process. For example, if a visiting consultant from an outside company plugs his laptop computer into the network, should this device automatically be entered into the help desk's inventory of supported configuration items? Probably not. The collection of configuration items that are used by CA Service Desk Manager are represented in the owned resource table: (ca_owned_resource).

You may need to track issues with configuration items that are registered in the database, but do not yet exist as owned resources. The Discovered Asset Selector allows the users to browse non-owned configuration item resource records in the database and transform them into owned resource records that can be used by CA Service Desk Manager.

The information from the nonowned asset is merged with the CA Service Desk Manager information into the same master record. If you search for Discovered Assets again, you can see that the original record has been updated to include the CA Service Desk Manager information you entered.

Follow these steps:

1. From the Configuration Item List page, click the Discovered Assets button.
   The Discovered Asset Search page appears.

2. To display the Discovered Asset List, click Search.

3. Select the asset from the list that you want to add as a configuration item. Right-click the asset and select Create New Configuration Item.
   The Create New Configuration Item page appears with information about the item populating some of the fields.

4. Complete any remaining fields that apply to the new configuration item and click Continue.

Note: Only name and class are required values for creating a configuration item.

5. Enter data as required in the appropriate fields on the Attributes tab.
   The family of the class that you selected for the configuration item determines the attributes that appear on the tab. The information you enter here is determined by your business processes and the information you want to store and view for a configuration item.

6. Click Save.
   The discovered asset is added.

Configuration Item Search Fields

The following search fields are available for filtering searches of configuration items. All search fields that allow text entry support use of the % wildcard character.

If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

- See the Configuration Item Fields (see page 2472) to filter based on the field values.

(Optional) Click the first  link to display the following fields:

- **Contact**
  Identifies a contact that is associated with the configuration item.

- **Manufacturer**
  Specifies the manufacturer of the item. This field is automatically populated, based on the value of the Model field, and cannot be changed.

- **Model**
  Specifies the manufacturer model identifier.
  Priority
  Specifies the priority ranking of the record that determines the amount of attention it receives. The predefined priority levels are 1 (highest) through 5 (lowest).

- **Product Version**
  Specifies the version number of the item, typically used for software and hardware.

- **License Number**
  Specifies the license number of the service provider (if applicable).

- **Financial Reference**
  Indicates the association of the configuration item with your financial software.

(Optional) Click the second  link to display the following fields:

- **Supply Vendor**
  Specifies the vendor responsible for maintaining supplies for this configuration item.

- **Responsible Vendor**
  Specifies the vendor responsible for maintaining the service that this configuration item provides.

- **Maintenance Vendor**
  Specifies the vendor responsible for the maintenance of this configuration item.

- **Cost Center**
  Specifies the code to which expenses related to this configuration item are charged. Enter the cost center directly, or to select the desired cost center, click the magnifier.

- **Responsible Organization**
  Specifies the organization that is responsible for this configuration item.

- **Maintenance Organization**
  Specifies the organization responsible for the maintenance of this configuration item.

(Optional) Click the third  link to display the following fields:

- **Earliest Acquire Date**
  Specifies the start date and time range for filtering your search that is based on when configuration items were acquired.

- **Latest Acquire Date**
  Specifies the end date and time range for filtering your search that is based on when configuration items were acquired.

- **Earliest Installation Date**
  Specifies the start date and time range for filtering your search that is based on when configuration items were installed.

- **Latest Installation Date**
  Specifies the end date and time range for filtering your search that is based on when configuration items were installed.

- **Earliest Warranty Start Date**
  Specifies the start date and time range for filtering your search. The search is based on when warranty coverage for configuration items began.

- **Latest Warranty Start Date**
  Specifies the end date and time range for filtering your search. The search is based on when warranty coverage for configuration items began.

- **Earliest Warranty End Date**
  Specifies the start date and time range for filtering your search. The search is based on when warranty coverage for configuration items ends.

- **Latest Warranty End Date**
  Specifies the end date and time range for filtering your search. The search is based on when warranty coverage for configuration items ends.

- **Earliest Expiration Date**
  Specifies the start date and time range for filtering your search that is based on when configuration items expire.

- **Latest Expiration Date**
  Specifies the end date and time range for filtering your search that is based on when configuration items expire.

You can click the More icon to display the Additional Search Arguments field. This field is intended only for expert users who understand SQL and Majic. You can enter a SQL WHERE clause in this field to specify an additional search argument.

Define CI Details

This article contains the following topics:

Define Service Information

You can store detailed information that is related to servicing a configuration item.

Follow these steps:

1. On the Service Desk tab, browse to Configuration Items, Active or Inactive. Select the Priority, Warranty, and Ownership for the configuration item you want to edit.
   The Configuration Item List appears.

2. Select the Configuration Item.
   The Configuration Item Detail page displays.

3. Click Edit.
   The Update Configuration Item page displays.

4. Select the Service tab and fill in the fields as appropriate.

5. Click Save.
   The configuration item definition is saved and the Configuration Item Detail page appears.

The following buttons are available for viewing configuration item details:

- **Asset Viewer**

  Opens the Common Asset Viewer. The viewer displays a detailed view of the configuration item that includes all properties that are managed or discovered.

Affected Tenants

Displays the tenants that are affected by this CI, based on its associated contacts and organizations.

Note: This button only appears when multi-tenancy is installed.

CMDBf Viewer

Displays the Federated View, a side by side view of CI attributes across registered MDRs.

Visualizer

Opens the Visualizer, which displays a graphical representation of the configuration item showing its relationship to other resources.

Service Fields

- **Service Type** -- The level of support service that is received for this configuration item. For example, some items can receive the problem resolution within four hours, while others can take up to 72 hours. Enter the service type directly, or click the search icon to select the desired type.
- **Cost Center** -- The code to which expenses related to this configuration item are charged. Enter the cost center directly or select the desired cost center by clicking the search icon.
- **Responsible Organization** -- The organization that is responsible for this configuration item.
- **Maintenance Organization** -- The organization responsible for the maintenance of this configuration item.
- **Priority** -- The level of attention that is given to problems with this configuration item.
- **Supply Vendor** -- The vendor responsible for maintaining supplies for this configuration item.
- **Responsible Vendor** -- The vendor responsible for maintaining the service that this configuration item provides.
- **Maintenance Vendor** -- The vendor responsible for the maintenance of this configuration item.
- **Service Impact** -- The level of importance of this service to the business.

Define Contact Information

You can define detailed information about the contacts that are responsible for a configuration item.

Follow these steps:

1. On the Scoreboard, select Configuration Items, Active or Inactive.

2. Select the Priority, Warranty, and Ownership for the configuration item you want to edit.
   The Configuration Item List appears.

3. Select the Configuration Item that you want to edit.
   The Configuration Item Detail page appears.

4. Click Edit.
   The Update Configuration Item page appears.

5. Select the Contacts tab.

6. Complete the tab fields as appropriate.

7. (Optional) Click Update Contacts.
   The Contact Search page displays.

8. Complete one or more of the search fields, and click Search.
   The Contact List page displays the contacts that match your search criteria.

9. From the list on the left, select the contacts that you want to assign to this configuration item.
   To select multiple contacts, hold down the CTRL key while clicking the left mouse button.

10. When you have selected all the contacts that you want, click the move button (>>).
    The selected contacts move to the Assigned to CI list on the right.

11. Click OK.
    The Configuration Item Detail page displays the selected contacts that are listed on the Contacts tab.

Define Location Information

You can store detailed information about the location of a configuration item.

Follow these steps:

1. On the Scoreboard, browse to Configuration Items, Active or Inactive. Select the Priority, Warranty, and Ownership for the configuration item you want to edit.
   The Configuration Item List appears.

2. Select the Configuration Item.
   The Configuration Item Detail page displays.

3. Click Edit.
   The Update Configuration Item page displays.

4. Select the Location tab, and fill in the fields as appropriate for the configuration item.

Note: The Address fields are filled in automatically when you select a location from the drop-down list.

5. Click Save.
   The location information is stored in the configuration item record.

Define Organization Information

You can define detailed information about the organizations that are responsible for a configuration item.

Follow these steps:

1. On the Scoreboard, select Configuration Items, Active or Inactive. Select the Priority, Warranty, and Ownership for the configuration item you want to edit.
   The Configuration Item List appears.

2. Select the Configuration Item.
   The Configuration Item Detail page appears.

3. Click Edit.
   The Update Configuration Item page appears.

4. Select the Organizations tab and click Update Organizations.
   The Organization Search page displays.

5. Complete one or more of the search fields, and click Search.
   The Organization List page displays the organizations that match your search criteria.

6. From the list on the left, click an organization that you want to assign to this configuration item. To highlight multiple organizations, hold down the CTRL key while selecting.

7. When you have selected all the organizations that you want, click Move (>>).
   The selected organizations move to the Assigned to CI list on the right.

8. Click OK.
   The Configuration Item Detail page displays the selected organizations that are listed on the Organizations tab.

CI Relationships

Contents

CA SDM provides a list of predefined relationship types that help you describe a relationship, or an association between configuration items. How the relationship is expressed depends on which configuration item is the focus. For example, a provider supports a dependent configuration item, but the dependent is supported by the provider. These are different expressions of the same relationship. The relationship type label that you see depends on whether you are viewing a provider-to-dependent or a dependent-to-provider relationship.

CIs in the CMDB can be related to other CIs. For example, a computer as a configuration item can result in additional configuration items, such as a printer and a monitor. The CI Relationship List displays sets of related CIs. For information about the relationship types that CMDB provides, see *CMDB Technical Reference* (see page 4168).

The CI relationships have the following characteristics:

- The *relationship type* defines how two configuration items are related.
- Hierarchical relationship types are paired as *provider/dependent*. For example, A (provider) *hosts* B; B (dependent) *is hosted by* A.
- Nonhierarchical relationship types are defined as *peer-to-peer*. For example, *is connected to*, which is the same in either direction.

You can do the following relationship functions by using the CMDB Relationships tab:

- View Active or Inactive relationships by searching on the Active? field.
- From the CI Relationship List, click any link for a relationship to launch its CI Relationship Detail page.

Create a Relationship Type

You can create a relationship type, and can make it available to create or update relationships.

Follow these steps:

1. On the Administration tab, expand the CMDB folder from the left pane, click CI Relationship Types.
   The CI Relationship Type List appears in the right pane.
2. Click Create New.
   The Create New CI Relationship Type page appears.
3. Complete the following fields:
   - **Provider to Dependent Label**
     Describes the relationship from the provider to the dependent. This is the name that appears in the list of relationship types. For example, "services" or "manages" is a Provider to Dependent relationship.

- **Dependent to Provider Label**
  Describes the relationship from the dependent to the provider. This is the name that appears in the list of relationship types. For example, "is serviced by" or "is managed by" is a Dependent to Provider relationship.

- **Peer-to-Peer?**
  Specifies that the relationship does not have a provider CI and dependent CI but instead consists of two equal CIs. For example, "connects to" and "fails over" are Peer-to-Peer relationships.

- **Active?**
  Makes the relationship type available for selection in configuration item relationships and lists.

4. Click Save.
   The relationship type is created and you can use it to create or update relationships.

Create a CI Relationship

You can add a CI relationship by starting from a focal configuration item. To launch a CI Relationship Detail page from the list, click any link in a relationship row. The Create New button allows you to create a new relationship from the CI detail.

The Impact Explorer button lets you view related providers and dependents using a search. The default search retrieves immediate providers one level deep. The related CIs are listed with the Relationship type with these additional fields:

- Family
- Contact

Follow these steps:

1. Select Search, Configuration Items on the menu bar of the Scoreboard.
   The Configuration Item Search page appears.

2. (Optional) Complete the filter fields to limit the search to the configuration items of interest and click Search.
   The Configuration Item List page displays the items that match your search criteria.

3. Select the Configuration Item to edit.
   The Configuration Item Detail page appears.

4. Select the CMDB Relationships tab.
   The tab lists any existing relationships for this CI.

5. Click Create New.
   The Create New Relationship page appears.

6. Enter the required data for this relationship:

- **Tenant (if multi-tenancy is installed)**
  The tenant level for this relationship.

- **Provider/Peer CI**
  The configuration item that provides the relationship. Enter the configuration item name directly into this field. To select the configuration item from a list, click the search icon.

- **Relationship Type**
  Use the Relationship Type Search and List to select relationship type.

- **Dependent/Peer CI**
  The dependent configuration item in this relationship. Enter the configuration item name directly into this field. To select the configuration item from a list, click the search icon. This field is required.

- **Symbol**
  (Optional) The unique identifier for this relationship. Assign a symbol that makes the relationship easily recognizable from the list.

- **Description**
  (Optional) A detailed description of the relationship. You can also use this field to describe the repositories that are assigned in the relationship.

- **Source Repository**
  (Optional) A detailed description of the relationship. You can also use this field to describe the repositories that are assigned in the relationship.

- **Cost**
  (Optional) The dollar value of the relationship between the configuration items.

7. Click Save.
   The CI relationship is saved and the CMDB Relationships tab displays the new relationship.

Manage a CI Relationship

The Configuration Item Relationship page provides all necessary settings in one location to simplify the CI relationship process.

You can use the page to do the following functions:

- Toggle the provider/dependent relationship between two CIs.
  Click Reverse to switch the Provider CI and Dependent CI for the relationship. The focal CI changes. If the reversed relationship is not valid, clicking Reverse clears the Relationship field.

- Set the Optional fields such as Symbol, Description, and Cost.
  Click Optional to set optional fields.
  If a Symbol is not supplied, a unique Symbol is automatically generated with prefix **cmdb bmhier:** and a unique number when the relationship is created.

Note: If your installation is integrated with CA Network and Systems Management (CA NSM), you must specify the CA NSM repository and cost.

Inactivate a CI Relationship

There are two ways to inactive a relationship. Consider a process depending on your organization needs.

Process 1: By setting the CI relationship status to Inactive.

Follow these steps:

1. Navigate to the CI Detail page, click the CMDB Relationships tab, and click Edit.
   The CMDB Relationships tab displays in Edit mode.

2. Choose a relationship and click any link on its row.
   The CI Relationship Detail page displays.

3. Click Edit.

4. Set the Active? attribute to Inactive. Click Save.
   The relationship is made Inactive. On the CI Relationship Detail page, the “Active?” attribute displays the Inactive attribute value.

Process 2: Using GRLoader to submit XML

Follow these steps:

1. Write XML that uses a Relation tag to identify the following parameters:
   - Provider CI
   - Dependent CI
   - Relationship type

2. Set the delete_flag to true (or yes or 1).

3. Submit the XML.
   The CI Relationship is deleted.

For more information about GRLoader, see the General Resource Loader (see page 4289) topic.

Example: Delete a CI Relationship Using GRLoader

In the following XML example, the "connects to" relationship between ci_1 and ci_2 is deleted.

```
<GRLoader>
    <relation>
        <dependent>
            <name>ci_2</name>
```

```
        </dependent>
    <type>connects to</type>
        <provider>
            <name>ci_1</name>
        </provider>
    <delete_flag>true</delete_flag>
    </relation>
</GRLoader>
```

Reactivate a CI Relationship

There are two ways to reactivate a CI relationship. Consider a process depending on your organization needs.

Process 1: Reactivate a deleted CI relationship

Follow these steps:

1. Navigate to the CI Detail page.
   The CI Detail page displays in Read-Only mode.

2. Click Edit.
   The CI Detail page displays in Edit mode.

3. Click the CMDB Relationships tab.

4. To open a CI Relationship Detail page, click any link on a row.

5. Click Edit.
   The Update CI Relationship page appears.

6. Change the Active? attribute to “Active”. Click Save.
   The relationship is reactivated.

Process 2: Reactivate using GRLoader to submit XML

Follow these steps:

1. Write XML that uses a relation tag to identify the following parameters:

   - Relationship type
   - Dependent CI
   - Provider CI

2. Set the delete_flag to false (or no or 0).

3. Submit the XML.
   The CI Relationship is reactivated.

For more information about GRLoader, see the General Resource Loader (see page 4289) topic.

Example: Reactivate a CI Relationship

In the following XML example, the "connects to" relationship between ci_1 and ci_2 is reactivated.

```
<GRLoader>
        <relation>
                <dependent>
                        <name>ci_2</name>
                </dependent>
        <type>connects to</type>
                <provider>
                        <name>ci_1</name>
                </provider>
        <delete_flag>false</delete_flag>
        </relation>
</GRLoader>
```

CI Relationship History and Comparison

The Versioning tab displays CI relationships and lets you do the following actions:

- View the relationship history for any CI in the CMDB. Changes that are made to a relationship are logged automatically when the relationship is created, updated, or deleted. You can view all current and historical relationships for a CI.

  Note: Relationships that are created with previous versions of CMDB do not have audit history information.

- Compare the relationships at any snapshot or milestone.

Versioning

This article contains the following topics:

Versioning promotes control over the IT infrastructure. Use versions for tracking and managing the life cycles of the CIs that constitute the authorized state of the CMDB. Versioning also applies to auditing the history of an object. Versioning provides the following functions to control the IT infrastructure:

- **Snapshots**
  Recorded automatically for changes to the value of any update to an object, such as when you update a CI. Versioning creates a snapshot with the complete state of the hardware CI after the

memory size of a computer is modified. Versioning can display the snapshot and can indicate which CI attributes have changed. Versioning can also compare it against all other historical snapshots of that CI. You require this critical information to understand the impact of changes on the availability and performance of a CI.

- **Milestones**
  Recorded as special-purpose snapshots with a user-defined label, such as First Day of Production or January Baseline. These labels can help find specific snapshots more quickly.

  Note: Milestones do *not* apply to change specifications, verification policies, managed change states, and managed attributes.

- **Comparisons**
  Compare a CI to another CI that acts as a standard. You can use any CI as a standard for comparison, but we recommend that you dedicate specific CIs as *Standard CIs*. A Standard CI lets you define a standard configuration to which other operational CIs in the same family can be compared. For example, define Server Large as a Standard CI to define the attribute values of this type of server. The Standard CI for a family can be made an attribute of an operational CI in that family. This relationship enables you to compare the current state or any historical state of a CI to its associated standard configuration. Like other comparisons, you can print this information or can export it as a comma-delimited file. Milestones can act as unshared, unchangeable baselines, but Standard CIs provide shared, dynamic baselines for your CIs.

  Important! A Standard CI must never contain values for any attribute that is used for CI reconciliation.

- **Change Specifications**
  View pending scheduled or unscheduled change specifications that a user specified for Change Orders for the CI. You can compare the change specification with the current state of the CI. For example, compare a planned value to the current state of a CI. This comparison can show conflicts with changes, identify overlapping changes in the schedule, and so on.

Versioning helps you complete the following tasks:

- Automatic capture of all CI modifications
- Snapshots of a CI at any time that are based on date or attribute changes
- Various levels of display including detailed Log, Basic, and Advanced views
- Multiple attribute comparisons with other snapshots, user-defined milestones for CIs, or a Standard CI
- Automatic snapshots whenever CA SDM change tickets change states

  Note: The automatic snapshot does not apply to change specifications, verification policies, managed change states, and managed attributes.

- Advanced filtering and comparison with Print and CSV Export support

Uses of Versioning

Versioning includes the following uses:

- **Problem Determination**
  To correct a problem with a CI, identify what changed in the environment of the CI. Versioning shows its current defective state, and its state at any point in the past. To identify potential problems, compare the two states.

- **Performance and Capacity Planning**
  By reviewing the history of a CI, a performance or capacity planner can determine the causes of performance issues. The history also helps in planning for future system growth.

- **Compliance**
  You can compare the state of a CI to its family Standard CI. To verify CI compliance and to identify attributes that need corrections, compare the state at any point in its change management lifecycle.

- **Change Verification**
  You can view the audit history of the object. For example, see who modified a verification policy, the date of the request, and the attributes and values that were modified. You can compare and contrast the changes between specific dates.

CI Versioning and Future State

View change Specifications in the CI Detail form Versioning tab. Provide more information, identify Change Order and corresponding change specifications. This tab also shows the future state of the CI as if the changes were applied. View snapshots of the CI, as of the scheduled date of the Change Order. If the Change Order has not been scheduled yet, it shows as an unscheduled change.

Versioning enables the following functionality:

- Quickly identify overlapping or conflicting change specification.

- Launch directly to change specification and view the corresponding change details by clicking Change Order in the detail view.

- Snapshots showing an *Unscheduled Change* indicated a change that is scheduled for some unspecified time in the future.

- The Change Order number is displayed with each change specification shown on the right side of snapshot label.

- Informational text displays in the bottom pane providing the following information about the change specification as hover text:

  - Change Order number.

  - Date of the scheduled change, if the Change Order specifies a scheduled date.

- Date need by, only shown if Change Order specifies a need by date.

Shared Asset and CI Audit Trail Records

The Versioning feature includes audit trail changes made to CA APM. Versioning also supports launch in context from CMDB to CA APM directly. The launch can be from an attribute log entry that is associated with each CA APM change. The CA APM audit trail is only available for CI/Assets from the CMDB families with CA APM audit logging enabled.

The Versioning tab that includes the CA APM audit trail information supports all families for which logging is enabled.

By default, CA APM does not log Asset attribute changes. To use CMDB Versioning with a CA APM-managed Asset/CI, enable Store Audit Trail Data on each asset attribute that requires logging. For more information about how to enable auditing, see the CA APM documentation.

When asset attributes are modified in CA APM, the Versioning tab data on the CI Detail page can be updated before the Attributes tab data due to caching activity. To resynchronize the values, click Edit.

Sources of Versioning Data

Versioning data generates whenever you create or modify an object by any component that supports the Audit Log facility. Snapshots that are generated from multiple sources are indistinguishable from one another. In a properly configure environment, snapshots appear automatically whenever CIs and their relationships are changed.

All CMDB families are enabled for versioning. CIs in CA Service Desk base families must be converted to CMDB families to take advantage of versioning.

Versioning data includes the following sources:

- **CMDB CI updates** -- Updates to common CI attributes and family-specific CI attributes by using the user interface.

  Note: For more information, see *CMDB Technical Reference (see page 4168)*.

- **CMDB relationship updates** -- Updates to relationships on the Relationships tab and the CI Relationship List by using the Edit and Edit In List feature.

- **GRLoader** -- CI insert and attribute updates, relationship updates, Standard CI assignments, and Milestones imported by using GRLoader. When the updates from an MDR are sent using GRLoader, the MDR source is also recorded. Recording the source helps you track attribute changes directly to their source.

- **CA SDM Change History** -- A snapshot is automatically created for all CIs associated with a change ticket. Up to four snapshots are taken when the CI is opened, closed, active, or resolved.

- **CA Asset Portfolio Management (CA APM) CI changes** -- Changes that CA APM makes to CIs that have logging enabled.

- **Change Verification** -- Updates to change specifications, verification policies, managed change states, and managed attributes.

Note: CIs created in CA SDM or previous CMDB releases only contain modification changes. The initial attribute values such as name, family, and class were not logged and do not appear in snapshots. In addition, Relationships created with CA Service Desk or previous versions of CMDB do not have audit history information.

CA SDM Change Management Integration

Versioning data is generated for each CI that is associated with a CA SDM change ticket. As the change ticket moves from *open* to *active* to *resolved* to *closed*, a snapshot is taken for each of the associated CIs. Thus, snapshots are created for opened, closed, active, or resolved statuses. If no CIs are associated with a change request, no snapshots are taken.

Note: The versioning feature requires no special configuration and is supported automatically in integrated installations.

The versioning feature handles the change ticket as follows:

1. Compares the state of the CI at the time the ticket was opened with its current state.
2. Verifies that all the required changes have been properly executed and that no additional changes were introduced.
3. Closes the ticket after the changes have been validated.

For auditing purposes, you can readily compare the state of the CI before and after each change was made. The comparison information helps answer questions including the state of a CI before and after a change request, for example:

- Did the appropriate change occur as requested?
- What other changes occurred to the CI not related to the change ticket?
- What time did the changes occur?
- How does this CI compare against the standard configuration, both before and after the change?

CA APM Integration

Versioning displays changes that CA APM makes to its CIs. Versioning also supports launch in context from CMDB to CA APM directly. The launch can be from any attribute log entry that is associated with a CA APM change. CA APM audit information is only available for CIs from CMDB families when CA APM auditing logging is enabled.

Note: When the CI attributes are modified in CA APM, the Versioning tab on the CI Detail page can be updated before the Attributes tab. This is due to caching activity. To resynchronize the values, click Edit.

By default, CA APM does not log CI attribute changes. To use Versioning with a CA APM-managed CI, enable Store Audit Trail Data on each asset attribute that requires logging.

By default, a 10-minute delay exists from the time a CI is updated in CA APM and the time it becomes available to versioning in the CMDB. You can modify this delay by changing the @NX_DBMONITOR_TIMER_MINUTES variable in an integrated installation.

Note: For information about how to enable attribute logging for assets, see the CA APM documentation.

CA SDM provides the following integration capabilities with CA APM:

- Shared records and audit log that differentiate between CA APM CIs and assets
- CMDB and CA APM launch in context to CI/asset information
- Shared extension table fields
- A CA SDM contact updates when CA APM changes a primary contact
- CA APM asset type modification to use CI families

CI Versioning Management

Contents

You can display and manage the history of the CI, associated snapshots, milestones, unscheduled changes, and other views. You use the left pane to navigate and the right pane to display CI details and the audit log.

Note: Versioning works similarly for managed attribute history and managed change state history. For example, the Managed Attribute History tab displays versioning information about a managed attribute.

To identify change specifications and the associated Change Orders, use versioning information. Versioning identifies unscheduled changes in the change specifications in the snapshot view. These changes correspond to Change Orders with no scheduled start date. You can view the snapshot and log of a change specification in CACF.

Example: Unscheduled Change

In this example, a user tries to change the value of a managed attribute. You view the Versioning tab on the CI detail page that displays Unscheduled Change in the snapshot. This snapshot displays information about the change, such as the date, time, username, and attribute value.

Select a snapshot or milestone in the left pane. The right pane displays the attribute values of that CI state, event, or comparison. The left pane displays CI snapshots or milestones by date and time (Basic mode) or by CI characteristics (Advanced mode). The left pane also includes the following links to help you manage a CI:

- **Create Milestone**
  Labels the state of a CI.

- **Show Log**
  Displays unfiltered CI history.

- **Advanced/Basic**
  Toggles between snapshot views.

- **Hide Empty Values**
  Permits filtering of blank data fields. When not selected, all CI attributes appear.

- **Print and Export**
  Print or cut-and-paste to save the versioning data on display.

Configuration Item Log

The log lets you view configuration item history. The Filter option permits filtering of log rows. Print and Export allow you to print or cut-and-paste to save the versioning data on display.

The Versioning information pane displays the following fields:

- Category
- Date
- Log
- Attribute
- New Value
- Old Value
- Changed By
- MDR

Note: The log only displays attribute *updates* for CIs that were created in previous releases of CA SDM or CA CMDB. The log does not display their initial CI attribute values. Relationships that were created in previous releases of CA SDM or CA CMDB do not include audit history information and do not appear in the log.

Log Filtering

The log can be filtered by entering a simple string in the Filter field. The Filter is case insensitive. If the filter string appears anyplace in a log row, the row is displayed. No special characters or wildcards are used in the filter. Log rows matching the filter criteria are displayed hiding rows that do not match.

You do not need to press Enter or refresh to update the display. The log view is filtered as each keystroke is entered and applies to all fields, Date, Log, Attribute, Old value, New Value, MDR, and Name.

CSV Export Support

You can export the CA CMDB log content to a Comma Separated Value (CSV) format file. Third-party reporting tools or applications can import the CSV file. The export is based on what is currently displayed, which can be filtered or unfiltered.

Integrated CA SDM and CA APM Logs

In addition to changes that were made using CA CMDB facilities, the CI log also includes CA SDM change ticket update activities and CA APM updates.

MDR Launch-in-Context and Source Identification

CA CMDB provides a way to launch in context, directly from the log to the MDR data provider for a particular CI log entry. You can also launch in context to the change specification. This launching feature does the following tasks:

- Tracks the attribute changes back to the source MDR, when the MDR used the <mdr_name> <mdr_class> and <federated_asset_id> tags in the GRLoader input.
- Identifies when multiple MDRs update a CI attribute. This situation occurs when multiple MDRs contribute data independently to a CI definition.
- Identifies which MDR is acting as the authoritative source.

Note: Log entries that are created in CA SDM or previous CA CMDB releases do not contain MDR launch in context information. In addition, CA Configuration Automation provides MDR launch information for most but not all attributes or relationships.

Attribute Names

Attribute names that are displayed in the log match the attribute name that is shown in the user interface. The attribute name is not same as the internal object name. For example, CA CMDB displays “Maintenance Type” instead of “mtce_type”.

Logging Custom Families and Attributes

To enable logging for modified families and attributes, specify new MDR attributes and audit triggers. If you create new families or attributes, you also must create metadata files to specify human readable attribute names to display in the log; otherwise, the internal object name appears.

For more information, see the Extending CMDB (see page 2603) topic.

Create a Milestone

You can create a milestone from the user interface or by using GRLoader.

Follow these steps:

1. To create a milestone from the user interface, complete the following steps:
   a. Select a CI and click its Versioning tab.
   b. Click Create Milestone.
   c. Enter descriptive text for the milestone. Click Save.
      The Create Milestone page closes.

d. Select View, Refresh.
The Basic view displays a new snapshot with the current date and time that represents the milestone that you created. Switching to the Milestone view, displays only those snapshots with assigned names. Milestones are displayed in descending date/time sequence, with the most recent at the top.

2. To create a milestone using GRLoader, complete the following steps:

a. Add the <milestone> tag to the XML for that CI.

b. Apply the same reconciliation rules apply as when associating a milestone with a CI.

Note: The value of the milestone tag is the label that is associated with that milestone.

c. Save and close the XML for the CI.
The milestone is created.

Example: Use GRLoader to Create a Milestone

The following GRLoader sample creates the milestone **Fiscal year end 2008**.

```
<ci>
<name>server1 </name>
<milestone>Fiscal year end 2008</milestone>
</ci>
```

Create a Standard CI

You create a Standard CI like you create any other CI. Any CI can act as a Standard CI, but the following cautions apply:

- A Standard CI must follow a naming convention so that it is not confused with regular CIs.
- A Standard CI must only act as a baseline for CIs in the same family as the Standard CI.
- A Standard CI must *not* be assigned values for any attributes that are used in reconciliation. For example, MAC Address, Serial Number, Alt CI ID, DNS, and so on.
- Because standard CIs are indistinguishable from regular CIs, they appear in your Scoreboard and count in the total number of CIs.
- As a best practice, Standard CI must not represent any actual instance of a business object.

Follow these steps:

1. Select Create New Configuration Item from the File menu.

2. Select the family that you want to use for the new Standard CI.

3. Define the attributes, as with any regular CI.
   The Standard CI is created.

Assign a Standard CI to a CI

You can assign a Standard configuration item to a configuration item by using the CI Detail page. You can assign a Standard CI to a list of CIs or using Edit in List.

Follow these steps:

1. To assign a Standard CI to a CI using the CI Detail page, complete the following steps:

   a. Select a CI and click Edit.
      The Update Configuration Item page appears.

   b. Click the icon next to the Standard CI field.
      The CI List displays.

   c. Select a CI to serve as the Standard CI. Click Save.
      The Standard CI is assigned.

2. To assign a Standard CI to a list of CIs, using edit in list, complete the following steps:

   a. From the Scoreboard or Administration tab, specify the search filter and click Search.

   b. Click the Edit In List button at the top right of the list results.
      The CI Edit in List controls is displayed.

   c. Select a row containing CI to assign the Standard CI too.
      The row is shown in highlighted color.

   d. Click the icon next to the Standard CI field.
      The CI List displays.

   e. Select a CI to serve as the Standard CI. Click Save to update the single CI or Change All to update all CIs in the list.
      The Standard CI is assigned to the single CI (Save) or all CIs listed (Change All)

Note: Any CI can act as a Standard CI, but the following cautions apply:

- A Standard CI must follow a naming convention so that it is not confused with regular CIs.
- A Standard CI must only act as a baseline for CIs in the same family as the Standard CI.
- A Standard CI must *not* be assigned values for any attributes that are used in reconciliation. For example, MAC Address, Serial Number, Alt CI ID, DNS, and so on.
- Because standard CIs are indistinguishable from regular CIs, they appear in your Scoreboard and count in the total number of CIs.
- As a best practice, Standard CI must not represent any actual instance of a business object.

Assign a Standard CI to a CI Using GRLoader

To assign a Standard CI to a CI, include the <standard_ci> tag in the description of a CI.

Example: Assign a Standard CI to a CI

If you have a standard workstation configuration that is stored in a CI named **standard workstation configuration.** You can assign the Standard CI to Joe's Workstation by using GRLoader to load the following XML:

```
<ci>
        <name>Joe's Workstation</name>
        <class>Server</class>
        <standard_ci>standard workstation configuration</standard_ci>
</ci>
```

Use the Basic View

You can select snapshots in either Basic or Advanced view. The same kinds of versioning data can be displayed in either mode. The Basic view lets you easily view the state of a CI.

Follow these steps:

1. Open the CI in the user interface and click the Versioning tab.
   The existing snapshots are listed on the left side of the page.

2. Select a snapshot type from the Snapshot type drop-down list:

   Note: If you select a Standard CI for the focal CI, it displays at the top of the snapshot or milestone list. If you click a Standard CI, the attributes for the Standard CI appear and not the focal CI.

   - **Snapshot**
     Lists all CI snapshots identified based on date/time and the Standard CI. The Snapshot view is the default option.

   - **Milestone**
     Lists all user-defined Milestones and the Standard CI.

Note: You can select two or more snapshots, milestones, or Standard CIs to compare them.

Use the Advanced View

You can select snapshots in either Basic or Advanced view. The same versioning data can be displayed in either mode. The Advanced view lets you view snapshots that are based on the attribute type, value, and time stamp. The Advanced view also lets you compare any with attributes, milestones, or a Standard CI with each other. A tree hierarchy shows a folder for each attribute of the CI, and each attribute folder contains a history of the values of the attribute. The hierarchy is organized as follows:

```
Root
     Attribute name
          Attribute value1
          Attribute value2
```

This hierarchy lets you view history of unique values for any particular attribute at a glance.

Follow these steps:

1. Open the CI in the user interface and click the Versioning tab.
   The existing snapshots are listed on the left side of the page.

2. Click Advanced.
   Advanced Selection shows a folder hierarchy.

3. Navigate the folder hierarchy, and click the folder that includes the information you want to view:

   - **Date**
     Lists Snapshots that are based on date/time, which is identical to the Basic view. If there are 30 or more snapshots for the CI, the snapshots can be divided further based on year /month. If a Standard CI is assigned to the focal CI, it is also listed in this folder.

   - **Milestone**
     This folder lists all user-defined Milestones. This view is identical to the Basic view. If a standard CI is assigned to the focal CI, it also appears in this folder.
     Standard CI attributes are displayed as special tree leaf nodes with a "Standard CI".
     Standard CI values only appear for attributes for which there is a standard CI value. If the value for an attribute is not set, it does not appear.

   - **Relationship**
     Contains all the relationships (past and present) for the CI. The folder hierarchy conveys the following information:

     ```
     Relationship

          Relationship Type

               Partner CI

                    Status and Date
     ```

Relationship Type specifies the kind of relationship, such as “is contained by”, “hosts” or “communicates with”.
Partner CI is name of the CI associated with the relationship.
Status and Date specify the Status of the relationship at the specified Date and Time.
Status values include the following ones:

- Relationship Created -- The state of the CI when the Relationship was created.
- Relationship Terminated -- This CI is no longer involved in the relationship. The relationship still exists at the partner end of the relationship, but the focal CI is not involved.
- Relationship Deleted -- The relationship was marked as deleted.
- Relationship Changed -- The relationship was reactivated from deleted state.
- New Partner and Type -- The partner end of the relationship was assigned to a new CI, and the relationship type was changed simultaneously.
- New Relationship Type -- The relationship type between two CIs has changed.
- Partner CI Assigned -- The partner end of the relationship has changed.

4. Click an attribute value.
   The complete state of the CI at the time that the attribute value was set displays.

Example: Use Advanced View to Show Disk Space Attributes

In the following example, Advanced Selection shows that disk space increased from 10 to 20 to 100 GB.

```
Root
      Disk space
            10 GB
            20 GB
            100 GB
```

Click any value to see the following information:

- When the change occurred
- The state of the other attributes when the change occurred
- The change request number that was open when the disk space was changed

View Snapshot Details

You can view snapshot details in the Basic or Advanced view. For example, the basic view displays a snapshot of an unscheduled change to a CI.

Follow these steps:

1. Open the object in the user interface and click the Versioning tab.
   A list of existing snapshots appears on the left side of the page.

2. Click a snapshot.
   Details are displayed in the right pane of the Basic and Advanced views. When you select only a single item, the right pane shows information about the selected snapshot, milestone (only for CIs), or standard.
   The displayed data includes the following details and indicators:

   - **Hide Empty Values**
     Permits filtering of blank data fields. When unchecked, all CI attributes are displayed.

   - **Bolded Value field text**
     Indicates that an attribute or relationship has changed since the last snapshot was taken. When viewing details for a Standard CI, all values are bold.
     Value
     Shows the previous value of the attribute and the time of the last change.

   - **"(blank)" Value**
     Indicates whether a previous value was cleared.

   - **Relationship Category**
     Shows information about the relationship, including the type and partner CI information.

   - **MDR Launch in Context and Source Identification**
     Provides launch-in-context to a provider MDR from the CI detail entry.

     Note: CIs created in CA SDM or previous versions of CA CMDB can lack MDR and Changed-By information. In addition, CA Cohesion ACM provides MDR launch-in-context for most but not all attributes or relationships.

     Tracks the attribute changes back to the source MDR.
     Detects when multiple MDRs update a CI attribute. This situation occurs when multiple MDRs contribute data independently to a CI definition.
     Identifies which MDR acts as the authoritative source.

Launch the MDR That Set an Attribute

If the history for a CI references an MDR, you can launch an MDR to view CI details.

Follow these steps:

1. Select a CI and navigate to its CI Detail page.

2. Click the Versioning tab.

3. Click Show Log, or select the CI snapshot or milestone you want to view.

4. Select the attribute row that you want to investigate.

5. If the CI history references an MDR, click the MDR link.
   The provider MDR shows more CI details.

Export Data

The Versioning Export to CSV page lets you export the snapshot and log information in a Comma Separated Value (CSV) format. Data displays in an Export page. The formatted data corresponds to the view you obtained. The filtering and data comparison you select on the Versioning tab is what is formatted for export.

Follow these steps:

1. Select an object and click the Versioning tab.
   Click the view that you want of the CI.
   For example, click Show Log, a snapshot comparison, milestone (CIs only).

2. Click Export.
   The Export Log to CSV for CI page appears.

3. Use the Select All action (from either context menu or keyboard shortcut).

4. Use cut and paste to transfer the data from the formatted page to a CSV file or third-party application. For example, you can Export to an Excel spreadsheet.
   The data is exported.

CI Family Changes and Snapshots

Family changes can affect a snapshot of a CI.

A snapshot includes the following different kinds of attributes:

- Common attributes
- Family-specific attributes

When you change the family of a CI, the following snapshot changes occur:

- The Family-specific attributes that are associated with the CI change.
- The Snapshot details reflect the family at the time of the snapshot.

The family of a CI determines the attributes of the CI. If you first change a *family-specific* attribute and then the family of the CI, the resulting CI no longer possesses the *family-specific* attribute you changed. Changing the family of a CI has no impact on its *common* attributes.

Example: Change the Family Associated with a CI

This example shows how CI family changes affect a snapshot of a CI.

Time	Status/Changes

0	The CI is in Family1.
1	One Family1-specific attribute value is changed.
2	Several common attribute values are changed.
3	The family of the CI is changed from Family1 to Family2. When this occurs, all Family1-specific attributes become unavailable to this CI.
4	One Family2-specific attribute value is changed.
5	Several common attributes are changed.
6	The CI family is changed back to Family1. When this occurs, all Family2-specific attribute values become unavailable to this CI, but previous Family1-specific attribute values are restored.
7	Several common attributes are changed.
8	One Family1-specific attribute is changed.

In the example, a snapshot at Time=7 does not contain information from the changes that are made at Times 3 or 4. Those changes represent changes that are made to Family2-specific attributes.

Compare Snapshots (Basic View)

You can compare two or more snapshots, milestones, or Standard CIs.

Follow these steps:

1. Select a CI and navigate to its CI Detail page.
2. Click the Versioning tab.
3. Select a Milestone or Snapshot from the Snapshot type drop-down list.
   Milestones or snapshots are listed.
4. Select two or more snapshots, milestones, or Standard CIs.
   The comparison view displays the following results:
   - A column is displays how the snapshots or milestones differ.
   - Each row displays the attribute values for the selected snapshots.
   - Only the attributes with differences are displayed. Date is always displayed unless snapshots are identical.
   - Standard CI comparisons are not time-specific, so their Date fields are set to say **Standard CI**.
   - Comparison results can be printed or exported to a CSV file.

Compare Snapshots (Advanced View)

You can compare two or more snapshots, milestones, or Standard CIs.

Follow these steps:

1. Select a CI and navigate to its CI Detail page.

2. Click the Versioning tab, and click Advanced.
   Advanced Selection displays the CI.

3. Navigate the folder hierarchy to the value you want to use for the snapshot comparison.

4. Select a value for each snapshot comparison.
   The comparison for the CI displays; for example, snapshot comparison that is based on the folder values selected.
   The comparison view displays the following results:

   - A column is displays how the snapshots or milestones differ.
   - Each row displays the attribute values for the selected snapshots.
   - Only the attributes with differences are displayed. Date is always displayed unless snapshots are identical.
   - Standard CI comparisons are not time-specific, so their Date fields are set to say **Standard CI**.
   - The comparison results can be printed or exported to a CSV file.

Note: In Advanced view, two CIs can have a relationship with no relationship type assigned (for example, CIs created by CA NSM). Such relationship nodes are identified as (blank).

CA SDM Change Management

Versioning data is automatically generated for each CI that is associated with a CA Service Desk change ticket. As the change ticket moves from *open* to *active,* and from *resolved* to *closed*, a snapshot is taken for each of the associated CIs. Versioning lets you do the following tasks:

- Compare the state of the CI to its Standard CI at any point in a change management lifecycle.
- Help ensure that the CI is in compliance and help identify those attributes which need remediation.
- Perform comparisons between states of the CI at any point in lifecycle of the change order, and any date or time in-between.
- View progress at each stage of the change, including any milestones.

The integration between CA Service Desk and CA CMDB is illustrated by demonstrating how you can audit changes that are performed during the service management lifecycle of a CI. In this example, a change request is used to upgrade components of a hardware server.

Follow these steps:

1. To create a change order and associate it with a CI, complete the following steps:

a. Create a CA Service Desk change ticket by clicking File, New Change Order.

b. Enter the change request information and order summary, for example: Upgrade hard drive to 500 GB.

c. Click the Configuration Items tab, and then click Update CIs.

d. Specify CI search criteria (for example, the name of the hardware server) and click Search.
In the Affected Configuration Items Update form select the CIs associated with the change ticket (for example, the hardware server from Step 4). Add them to the Affected Configuration Items list and click OK.

e. Save the change request.

2. To perform the changes, complete the following steps:

a. Make the changes for the CI. For example, install the hard drive on the physical computer, and then update the Disk Capacity attribute for the hardware server CI.

b. Close the change request.

c. Ensure that the change was completed: View the CI, click the Versioning tab, and compare snapshots of the CI before and after the change.
Suppose that you compare the state of the CI between the times when the change order was opened and closed. You notice that the hardware server drive size was 100 GB before the change and 500 GB after the change was completed. You also see the date and times that the changes occurred. Any other attributes that were modified between the open and close times also display.

CA CMDB Versioning Terminology

This article contains the following topics:

Versioning is the practice of representing and tracking *service transitions*. Versioning typically uses a naming convention to identify the dates, sequences, and meanings of such transitions. These records can be used to identify and compare specific states of a configuration item (CI).

Example: Version Comparison

For a Payroll Application CI, a comparison of Version 3 against Version 2 indicates the enhanced features and other differences.

States

In the context of versioning, the *state* of a CI represents all the attribute values of that CI at a single point in time. The state of a CI can be the result of attribute changes from multiple MDRs.

Versions

A *version* is an identified instance of an object such as a CI within a product breakdown or configuration structure. Use versions for purposes of tracking and auditing change history.

Snapshots

A *snapshot* is a representation of the complete state of an object at a single point in time. For example, a typical CI has many snapshots that are associated with it. A snapshot consolidates all modification events that occur to an object during a one-minute time interval. For example, if you update a CI (edited and saved) several times within one minute, CA SDM creates a single snapshot and includes all the updates during that minute.

Snapshot is a general term that refers to time and date-based snapshots, and milestones or Standard CIs. To help you to locate meaningful points in time, CA SDM lets you label snapshots meaningfully. These named snapshots are named milestones.

Every time an object is changed, CA SDM creates a snapshot automatically. Versioning captures all changes to the object. For example, snapshots originating at an MDR and came to the CMDB through GRLoader or CMDB Web Services.

Categories

A *category* identifies a class of attributes. The category is typically the name of the tab that displays the attributes.

Note: Items such as name, serial number, active flag are assigned to a category that is not a tab name.

Examples: Tabs and Categories

The following examples show how categories correspond to tabs:

- Because the *disk space* appears on the Attributes tab, its category is *Attributes*.
- Because *IP address* appears on the Inventory tab, its category is *Inventory*.
- *Milestone* appears in the *General* category.
- A *Standard CI* appears in the Classification category.
- *Relationships* appear in the Relationship category.

Milestones

A *milestone* is an on-demand labeled snapshot of a CI. It is created to mark an event, a logical breakpoint, or an accumulation of changes. The milestone contains the actual state of the CI at the time that the snapshot was created. Milestones let you quickly identify and navigate to significant points in the history of a CI. Creating a milestone, creates an equivalent “date” snapshot.

Milestones are CI-specific, not shared. The subcomponents of a milestone for a high-level object such as a service do not automatically create milestones. To take a milestone for an object which is composed of several subcomponents, you can generate several independent milestones.

Milestones are static and can never be changed or be deleted. When you create a milestone, the snapshot is of the current state of the CI. Later, when displayed or used in a comparison, milestones always reference a point in the past. A good naming convention for your milestones helps you easily identify critical points in the life of a CI.

Important! Milestones do *not* apply to change specifications, verification policies, managed change states, and managed attributes.

Standard CIs

A *Standard CI* is an abstracted configuration for a CI family. It can be used for baseline comparisons to "real" CI instances in the same family. A Standard CI can be a real CI in the sense that it represents a physical object or it can exist only for comparison. Standard CIs can have the following associations:

- A Standard CI can be shared among several CIs.
- A CI can only have a single Standard CI associated with it at any given time. When the Standard CI is changed, the change is shown in any comparison between the associated CIs and the Standard CI.
- A family can have multiple Standard CIs. For example, one family might have standard CIs named “Standard Test Server,” “Standard Production Server,” “Standard Acceptance Server.” We recommend that you name Standard CIs in such a way that they can be easily searched for and identified.

Because a Standard CI is itself a CI, it can be managed. It has an audit trail, security, a history of changes, and so on, like any other CI. After you define a Standard CI for a particular CI, you can use it to verify compliance with corporate standards.

The concept of “date” or “time” does not apply when comparing a Standard CI with a snapshot or milestone. Only the Standard CI attribute values are used for comparison, snapshots and milestones specific to the Standard CI do not apply.

Example: Standard CI Use

A company defines an **Employee Workstation** configuration as a Standard CI to compare with its actual desktop computers in the Hardware.Workstation family. A comparison reveals that a specific computer has only 1 GB of RAM, instead of the Standard CI memory value of 2 GB.

Stage CI Transactions Before Loading into CMDB

CMDB provides a facility where you can store data before you load it into the CMDB. This "staged" data is stored as transactions in the transaction work area (TWA). A staged transaction is a unit of work that creates or updates a CI or Relationship. The TWA can contain many transactions for a given CI or relationship.

You can capture data being loaded into the CMDB before that data is committed so that you can:

- Clean up and standardize nonstandard data.
- Supplement incomplete data. For example, CI names starting with "NY" can have their location set to "New York".
- Modify data that does not match existing lookup tables (SRELs).
- Schedule transactions for implementing later.
- Reconcile transactions to existing CIs in the CMDB before you load the data.
- Validate the CI and relationship transactions. Validating prevents the creation of invalid data or creation of new CIs when a single or existing CI can be updated. View each transaction and the potential CIs that it can update. This helps you reconcile the transaction manually to the target CI.

You can use the TWA to help you proactively manage the reconciliation process. You can configure GRLoader to load the data into the TWA. When the data is loaded, CMDB lets you modify it to handle transactions that can potentially update or reference the wrong CI.

For more information, see Review and Modify Inbound Data Using Transaction Work Area (TWA) (see page 2566).

How To Load Transactions into the CMDB

This article contains the following topics:

Instead of creating CIs and relationships through XML, specify the following options to select the TWA as its input source:

- lftwa (load from TWA)

- lftwai (load from TWA and inactivate)

Note: Unlike other GRLoader modes that use an err.xml file, loading from the TWA returns error messages to the transaction Message field.

As the transactions are processed, GRLoader sets the transaction status to indicate success or failure of each TWA transaction. If GRLoader -lftwa is run multiple times continuously, set the status of the transaction to Ready between runs of GRLoader. GRLoader does not attempt to load data that is already loaded.

The transaction is executed from the TWA as if GRLoader were running using XML input. Transaction security is based on the user that loads from the TWA, not the user that loaded the TWA transaction originally.

Auditing occurs when the transactions are processed successfully.

Note: Before you load the transactions, you can predetermine whether a set of transactions will create new CIs or relationships. Use the simulation options (-simci and -simrel). See How to Simulate TWA Operations (see page 2525) for more information.

How To Prevent Data Regression

While transaction data for a CI is in the TWA, some other action can update that CI in the CMDB. The update can then cause the TWA transaction data to become invalid. To prevent unwanted data regression, GRLoader compares the TWA tran_dt (Transaction Date) field with the CI last_update_dt (Last Modified Date) or relationship last_mod_dt (Last Modified Date). If the last_update_dt is more recent, GRLoader rejects the TWA transaction and posts an error message to the tran_message column.

You can resolve this situation by completing one of the following actions:

- Use the web interface to edit the CI or relationship tran_dt (Transaction Date) field to a more appropriate value.
- Set the GRLoader option grloader.workarea.ignore_transaction_dates="yes" to ignore the transaction dates and insert the data.

Note: If GRLoader rejects a transaction as older than the target CI, you must verify that the transaction is running. Se t the transaction date to a current or recent date and rerun GRLoader.

The ignore transaction dates option can cause data back-leveling or regression. When a single CI or relationship is updated multiple times in the same GRLoader -lftwa run, the last_update date is set to the current time during the first update. To allow for multiple updates to the same CI or relationship, another verification is made to see if the CI or relationship was updated after GRLoader started. If it was, then the update is allowed. If it was, then the update is allowed.

Filter By Change Order Number

The GRLoader -chg option can be used to select only transactions that are associated with a change ticket. To filter by change number, set the Change Order attribute (tran_chg_ref_num) to the appropriate change request number.

Note: The Change Order string is not validated when loaded into the CMDB.

Example: Filter By Change Ticket

The following option loads only transactions that are related to Change Order 23434.

```
grloader -lftwa -chg 23434
```

How to Use the Web Interface to Update Data in the TWA

Content

You can stage CI and relationship transactions before execution, by copying data into TWA staging area. Once in the staging area, you can manipulate CIs and relationships by using the web interfaces.

You also can validate the CI and relationship transactions. Validating prevents the creation of invalid data or creation of new CIs when a single or existing CIs must be updated. In this approach, you view each transaction and the potential CIs that it can update. It helps you reconcile the transaction manually to the target CI.

To manage the transaction work area, select the Administration tab and navigate to the CA CMDB, Transaction Work Area node. From this node, you can manage the Transaction Work Area pages.

Manage CI Transactions

The CI Transaction Detail page displays all nonblank attributes in the transaction. If you clear the Hide Empty Values check box, all CI attributes are displayed. For more attribute information, point to the attribute name.

You can do the following actions:

- View a transaction
- Create a transaction
- Edit the transaction
- Save or Cancel transaction changes (Edit mode)
- Reset the original transaction data (Edit mode)
- Show or hide data (Attributes tab)

- Set the target CI (Reconciliation tab)

The TWA accepts free-form text as case sensitive by default unless you enable case insensitivity. Use the -I GRLoader option to enable case insensitivity. Attribute values are not validated until load-from-TWA run time, so values must be entered exactly as required. If you enter string values for nonstring MDB fields, GRLoader issues warnings when loading to the CMDB. You can also simulate loading the data to predetermine (-simci) whether a set of transactions can create new CIs or report errors in the data.

Restrictions:

- If tgt_id is defined for a transaction, it displays as a CI name in the Target CI field.
- If superseded_by is defined for a transaction, it displays as a CI name in the Superseded By field.
- TWA entries are not logged.

Important! Data that you enter using this web interface must have the same format as native SQL or XML. For example, when you enter data for a lookup field, refer to the section on XML Input. When you want to specify an owner to look up by userid, use braces { } to specify the lookup field. For example, to find the name that is associated with the userid "admin", enter admin{userid} in the owner column.

After you save a single transaction, click the Reconciliation tab for that transaction. Verify whether any ambiguity exists in its intended target CI. If there is any ambiguity, you can specify a target CI (see page 2562). When all data entry is complete, you can simulate loading the data (see page 2525) to validate the data and verify reconciliation.

Important! Data that you enter into the TWA using this interface must follow certain rules. For more information about the rules, see the "How to load data into the TWA Using GRLoader (see page)" section.

The web UI does not validate case-sensitive data in the TWA. Verify that the values you enter exactly match the lookup values. Alternately, when you run GRLoader, you can specify the - I option to enable case insensitive lookups.

Note: Although tgt_id or superseded_by are stored as UUIDs in the transaction, they are displayed as CI names in the web interface.

Manage Ambiguous CI Transactions

Review and modify transactions that have ambiguous CI targets before loading the transaction data. Resolve CI transactions that do not have a target CI, but have identifying attributes for one or more existing CIs. This resolution ensures that the appropriate CI is updated and prevents incorrect or inconsistent data from being created.

After you save a single transaction, click the Reconciliation tab for that transaction. Verify whether any ambiguity exists in its intended target CI. If there is any ambiguity, you can specify a target CI (see page 2562). When all data entry is complete, you can simulate loading the data (see page 2525) to validate the data and verify reconciliation.

For more information about reconciling the data in the TWA, see Review and Modify Inbound Data Using Transaction Work Area (TWA) (see page 2566).

Manual Reconciliation

To reconcile a CI transaction manually, determine the target CI that matches the identifying attributes of the transaction. Set the tgt_id of that transaction to the UUID of the target CI.

When GRLoader processes a transaction with a tgt id, it updates the target CI with the transaction information. GRLoader registers that CI again when its identifying attributes have changed.

You can specify the target CI explicitly in the transaction. You also can use the Reconciliation tab to select a target CI.

For more information, see Review and Modify Inbound Data Using Transaction Work Area (TWA) (see page 2566).

Specify a Target CI for an Ambiguous CI Transaction

You can specify a CI for an ambiguous transaction so that its data is directed to a specific target CI regardless of the values of the identifying attributes specified in the transaction.

Follow these steps:

1. Select a CI transaction from the Ambiguous Transaction List page.
   The Configuration Item Transaction Detail page appears.

2. Click Edit.
   The Update Configuration Item Transaction page appears.

3. On the Reconciliation tab, select a CI from the list to designate the CI as the Target CI for the transaction. Click Set Target and then click Save.
   The selected CI becomes the target CI for the transaction.

Populating the TWA

This article contains the following topics:

Input data can come from a number of sources, including the following sources:

- CA products such as CA Configuration Automation, CA Wily CEM, CA Introscope, and CA Spectrum that import data by using GRLoader
- Any other MDR that imports data by using GRLoader
- Another CMDB
- Microsoft Excel spreadsheets
- Database tables
- An ETL tool that a vendor chooses

See Database Limitations (see page 2534) for more information.

How to Load Data into the TWA Using GRLoader

The following GRLoader options support the uses of the TWA:

- **-lttwa**
  Loads XML data to TWA in initial state.
- **-lttwar**
  Loads XML data to TWA in ready state.
- **-lftwa**
  Loads transactions to the CMDB from TWA.
- **-lftwai**
  Loads transactions to the CMDB from TWA and inactivates successful transactions.

GRLoader input XML documents can be loaded into the CMDB or the TWA without modification.

Loading data into the transaction work area can be accomplished by using GRLoader with the - lttwa (load to TWA) option. In the GRLoader configuration file:

```
grloader.loadtotwa=yes
```

In TWA mode, instead of creating CIs and relationships directly, GRLoader inserts the information into the transaction work area tables. Data that has been loaded into the TWA can be edited, changed, and verified. After the data modification process is complete, individual transactions can be loaded into the CMDB by using - lftwa or -lftwai.

When loading CI data into the CMDB, CIs undergo automatic reconciliation. Successful reconciliation results in data from a single business object updating a single CI in the CMDB. When loading *CI transactions* into the TWA, no automatic reconciliation occurs. Multiple transactions with identifying attributes targeting a single CI can appear in the TWA. The existing rows in the TWA are not updated when new rows are added in load to TWA mode, despite an identical match to an existing CI. Even identical CI definitions can appear many times in the TWA.

GRLoader validates data values when running in load from TWA mode (-lftwa or -lftwai) to create objects in the CMDB. Or, when running using the simulation mode (-simci or - simrel). See How to Simulate TWA Operations (see page 2525) for more details. The data values are not validated when GRLoader is run in load to TWA (-lttwa or -lttwar) mode.

The -lttwai parameter (or configuration option grloader.loadtotwa.inactivate) inactivates successfully loaded TWA transactions. After a successfully loaded transaction has been marked inactive, it can be permanently purged from the TWA by using Archive/Purge.

Example: Load to CMDB

The following command loads data directly into the CMDB:

```
grloader ... -i mydata.xml  - a  - n
```

The XML file mydata.xml contains:

```
<GRLoader>
  <ci>
     <name>server1</name>
     <class>Server</name>
   </ci>
</GRLoader>
```

Example: Load to TWA

The following command loads the data into the TWA, so that it can be manipulated before loading into the CMDB:

```
grloader ... -i mydata.xml -lttwa
```

XML Input

GRLoader uses XML input data. When loading to TWA, conflicts may occur when the column names overlap with the standard column names in the database. To prevent the conflict, the following XML columns are mapped:

FROM XML Name	TO Database Column
tenant	tgt_tenant
id	tgt_id

delete_flag	tgt_delete_flag

For relationships, the following mapping applies:

FROM XML Name	TO Database Column
name	provider_name or dependent_name
dns_name	provider_dns_name or dependent_dns_name
delete_flag	tgt_delete_flag

Mappings are reversed when loading from the TWA database tables.

lookup

When you specify data for lookup (SREL) attributes in the TWA, maintain the same format as specified in native XML for GRLoader. Lookup attributes accept only a specific set of values that must be defined in related tables in CA SDM. These attributes also can have more restrictions and exceptions that must be met for the assignment to occur. The specified values are the same whether specified using XML, SQL, or the TWA web interface.

To determine whether an attribute is an SREL, refer to the following *CMDB Technical Reference* sections:

- Families and Classes (SREL attributes are identified)
- Contact and Other Lookup Fields
- Fields Validated Against Data in Existing Tables (SREL)

Example: lookup XML

In the following example, the alternate SREL column is set by specifying the lookup parameter:

```
<ci>
<name>server1</name>
<owner lookup="userid">mckpe99</owner>
</ci>
```

In the TWA, the same thing can be accomplished by suffixing the alternate SREL column to the data value, which is included between delimiters. For more information, see the grloader.workarea. delimiters configuration given later. The equivalent transaction is represented in the transaction work area as:

ID	Name	Owner
100	server1	mckpe99 {userid}

You also can set the delimiter character that is used previously in the GRLoader configuration file:

```
grloader.workarea.delimiters=xy
```

x and y are different characters that typically do not appear in the work area.

Date Format

GRLoader supports the following date format options in XML:

- datefmt=UTC
- datefmt=localtime (the default)

Examples: datefmt XML

```
<ci>
<name>server1</name>
<purchase_date datefmt="UTC"> 1241197235</purchase_date>
</ci>
<ci>
<name>server3</name>
<purchase_date> 2009/05/01</purchase_date>
</ci>
```

The equivalent transaction is represented in the transaction work area as:

ID	Name	purchase_date
101	server1	1241197235
102	server2	2009/05/01

Note: If a date contains a special character such as a slash (/), then the format is assumed to be "localtime". If a date contains no special characters, the date is assumed to be UTC.

EMPTY

GRLoader supports the update_if_null option in the XML, which clears a field in the CMDB. The following example clears the owner field for server1. Without that attribute, the owner field is not affected. When using the TWA, you can use the keyword EMPTY instead.

Example: update_if_null XML

```
<ci>
<name>server1</name>
<owner update_if_null="yes"></owner>
</ci>
```

In the TWA, the database value is cleared by specifying the keyword EMPTY as the string value. The equivalent transaction in the work area is:

ID	Name	Owner
102	server1	EMPTY

The keyword value can be set by using the grloader.emptyvalue configuration option:

```
grloader.emptyvalue=xxxx
```

xxxx represents any string that typically does not appear in the work area data.

How To Simulate TWA Operations

You can predetermine whether a set of transactions can create new CIs or relationships and therefore create new ambiguities for other CIs. Use the following options:

- **- simci**
  Simulates processing CI transactions only. The option can be used to determine whether transactions create or update CIs. When the -simci option is used, GRLoader performs data validation.

- **- simrel**
  Simulates processing relationship transactions only. The option can be used to determine whether relationship transactions create or update relationships. The - simrel option checks relationships for the existence of the provider and dependent CIs, validates relationship types, and so on.

The output from simulation mode is directed to the TWA or to the _err.xml file. In normal load mode, the _err.xml file contains the CI input and a comment indicating whether the CI was inserted or updated. When a simulation is used, the GRLoader message on the CI Transaction List indicates whether the CI or relationship was inserted or updated. The transaction state remains unchanged.

Simulation can also be enabled in a configuration file by using the **grloader.simulateloadci** and **grloader.simulateloadrelation** options.

Note: If the GRLoader input creates CIs and relationships simultaneously, the - simrel option can only process actual CIs. The option cannot process CIs that are scheduled to be created. Because of this limitation, -simci and - simrel are mutually exclusive.

How to Use SQL to Update Data into the TWA

The TWA is stored in the MDB and you can update it directly with SQL queries.

TWA Tables

Transaction Work Area (TWA) tables include:

- **ci_twa_ci**
  A single table that contains all attributes across all CI families. The table stores data in a de-normalized form to enable customers and services to understand and manipulate the content.

- **ci_twa_relation**
  Complements the ci_twa_ci table. This table contains CI relationship information.

TWA column names correspond to the attributes that are used with GRLoader, with some exceptions.

TWA SQL Column Names

Column names in the ci_twa_ci and ci_twa_relation tables match the CI and Relationship attribute names with some exceptions.

TWA fields common to ci_twa_ci and ci_twa_relation

- **apply_after_dt (Apply After Date)**
  GRLoader executes the transaction only if the current date is after the Apply After Date. Measured in number of seconds since the epoch. If the value is zero (0), this field is ignored.

- **tran_chg_ref_num (Change Order)**
  Specifies the change order identifier that is associated with this transaction. The GRLoader - chg option uses this attribute to select only transactions with the specific change order number.

  Note: For more information about using the - chg option option, see Filter By Change Order Number (see page 2518).

- **tran_status (Transaction Status)**
  Specifies the status of the transaction. The tran_status must be one of the following values. Only the transactions with tran_status=1 are executed.

Value	Short Description	Long Description
0	Initial	Default value. Requires intervention to move to "Ready" for GRLoader to act upon this transaction.
1	Ready	The transaction is ready to be loaded into either the appropriate CI or relationship tables.
2	Successful	Transaction that is processed successfully.
3	Warning	Warning that is detected during load into ca_owned_resource/bmhier.
4	Error	Error that is detected during load into ca_owned_resource/bmhier.
40000+	For customer use	

- **tran_message (Message)**
  GRLoader message showing results of the load or simulation.

- **tran_dt (Transaction Date)**
  Prevents accidental overlaying of current information by old transaction data. The transaction date is compared with the last modification date of the CI. GRLoader rejects the transaction if the CI is more recent.
  If GRLoader rejects a transaction as older than the target CI, verify that the transaction is still applicable. Set the transaction date manually to be more current. Run GRLoader again.

- **tgt_delete_flag (Active?)**
  Inactivates the target CI or relationship. Set this value to 1 (one). This setting is not the same as setting delete_flag to 1, which indicates that the transaction must be deleted.

ci_twa_ci columns

In addition to the following column names, you can specify CI attribute names as column names in your SQL statements:

- **tgt_id (Target CI)**
  Specifies the UUID of the target CI. Used when performing manual reconciliation.

- **superseded_by (Superseded By)**
  Specifies the UUID of the superseded CI.

- **tgt_tenant (Tenant)**
  Specifies the tenant name that is assigned to the target CI. Tenant can only be assigned at the time of creating CI if the GRLoader user has proper authorization. This setting applies only when multi-tenancy is enabled.

ci_twa_relation columns

In addition to the following column names, you can specify relationship attribute names as column names in your SQL statements:

When using SQL to define relationship transactions, use the following database column names:

provider_name (Provider Name)

provider_mac_address (Provider MAC Address)

provider_serial_number (Provider Serial Number)

provider_system_name (Provider Host Name)

provider_asset_num (Provider Asset Number)

provider_dns_name (Provider DNS Name)

provider_tenant (Provider Tenant)

AND

dependent_name (Dependent Name)

dependent _mac_address (Dependent MAC Address)

dependent _serial_number (Dependent Serial Number)

dependent _system_name (Dependent Host Name)

dependent _asset_num (Dependent Asset Number)

dependent _dns_name (Dependent DNS Name)

dependent_tenant (Dependent Tenant)

If provider or dependent CI UUIDs are known, you can use the following fields:

provider_id specifies the UUID of the provider CI

dependent_id specifies the UUID of the dependent CI

Note: provider_tenant and dependent_tenant only apply when multi-tenancy is enabled.

Insert New Records in the TWA

You can insert a new record into the ci_twa_ci and ci_twa_relation tables from outside of CA SDM.

To insert records into the ci_twa_ci and ci_twa_relation tables, specify 0 in the ID column as:

```
insert into ci_twa_ci values(id, name) values(0,'test-ci');
insert into ci_twa_relation values(id, type) values(0,'test-relation-type');
```

Caution: If multi-tenancy is enabled, provide the tenant, tgt_tenant, provider_tenant or dependent_tenant attributes as appropriate. If you create a TWA transaction without specifying a tenant, the Public tenant is assumed.

How to Use the ODBC Driver

You can use SQL instead of GRLoader to load the TWA. We recommend that you use the ODBC driver that is provided with CA SDM, instead of native SQL services. Using the ODBC driver provides the following benefits:

- Performance
- Security
- Database independence
- Data integrity when the database updates come from the CA SDM server and the bulk editing tool is running simultaneously

Cautions

- Only the CA SDM ODBC drivers honor security features such as multi-tenancy, data partitioning, and role access. SQL that is executed using the native DBMS drivers does not enforce security.
- Make frequent data backups when performing updates using native SQL.

CI Identifiers in the TWA

In the ci_twa_ci table, three identifiers are associated with a CI transaction: ID, tgt_id, and superseded_by, These attributes are:

- ID is the transaction sequence number. **Do not modify this field.** IDs 1-2,000,000,000 are reserved for use by systems that modify the TWA outside the CA SDM server. IDs from 2,000,000,001 to approximately 4 billion are reserved for use by CA SDM. When the system runs out of IDs, reinitialize the table.
- tgt_id, provider_id, or dependent_id are the UUID of the target CI. Set this field whenever you perform manual reconciliation.
- superseded_by is the UUID of the superseding CI. Set this field whenever you manually designate the superseding CI for the transaction.

How to Set Transaction Status

You can set the transaction status (tran_status) of each transaction in the TWA. For GRLoader to process a transaction, it must be set to Ready (tran_status=1).

Value	Short Description	Long Description
0	Initial	Default value. Requires intervention to move to "Ready" for GRLoader to act upon this transaction.
1	Ready	The transaction is ready to be loaded into either the appropriate CI or relationship tables.
2	Successful	Transaction that is processed successfully.
3	Warning	Warning was detected during load into ca_owned_resource/bmhier.
4	Error	Error was detected during load into ca_owned_resource/bmhier.
40000+	For customer use	

If GRLoader - lftwa is run multiple times, the status is updated after the first run and all subsequent runs do not find any transactions. Reset the status of the ready transactions before every GRLoader - lftwa execution.

For information about how to represent XML data in the TWA tables, see the XML examples in previous sections.

How to Share Tables with CA SDM

SQL Server Only

When using SQL to update the ci_twa_ci and ci_twa_relation tables, set the last_mod_dt column manually, as follows:

```
SET last_mod_dt = DATEDIFF(s,'19700101', GETUTCDATE())
```

Example: Set last_mod_dt

The following example sets the last_mod_dt:

```
UPDATE ci_twa_ci
    SET tran_status=1,
        last_mod_dt = DATEDIFF(s,'19700101', GETUTCDATE())
    WHERE tran_status=1
```

Note: TWA table updates can take several minutes to appear in the web interface or GRLoader. For more information about update timing, see the NX_DBMONITOR_TIMER_MINUTES option.

Transaction Work Area

Use the Transaction Work Area (TWA or work area) to inspect and modify CI and relationship data before loading the data into the CMDB.

The transaction work area is a data warehouse to store, review, and modify CI and relationship transaction information from multiple sources. In the TWA, you can modify incoming transaction data to conform to your CMDB requirements. You also can use the TWA to modify data input that could create false positives or false negatives during the reconciliation process. False positives are multiple CI representations of the same business object. False negatives are multiple business objects that are identified as the same CI.

Transaction information can apply to new objects or to objects that are already in the CMDB.

The TWA process works as follows:

1. Load the data (see page 2520) into the TWA. The content can include CI transactions or relationship transactions. The input process does not attempt to reconcile records. The process simply populates the work area with CI and relationship transaction records in one of the following ways:
   - GRLoader - Reads XML data and stores it in the TWA using the -lttwa or -lttwar options.
   - Native SQL - Places data into the TWA using standard SQL processing.
   - Create a CI transaction or relationship transaction using the web interface.
2. (Optional) Manually reconcile transactions to existing CIs in the CMDB before you load the data. You can also simulate loading the data (see page 2525) to predetermine whether a set of transactions can create new CIs or relationships. For more information, see Review and Modify Inbound Data Using Transaction Work Area (TWA) (see page 2566).
3. Modify the data. You can modify the TWA from the following sources:
   - **CA SDM user interface**
     The web-based user interface lets you view and modify transactions in the work area.

- **Native SQL**
  When performing many changes to multiple transactions, native SQL can modify the data in the TWA.

  Note: Changes that are made using native SQL can bypass all CA SDM security.

GRLoader loads the data from the TWA to the CMDB using the -lftwa or -lftwai options. Each TWA row is treated as a separate transaction.

a. If there is an error after a GRLoader run, the error code is populated into the transaction to indicate that it is incomplete (to facilitate future retries).

b. All other records are identified as completed transactions.

4. Review the transaction results and correct any errors using the web interface. Consider the following points:

   - If you want the columns of custom families or attributes to appear in the work area, modify the work area to include the modified columns. For more information, see Extend the TWA Object (see page 2532).
   - To take advantage of the TWA, use the latest version of GRLoader. If you are using a product that includes a previous release of GRLoader, upgrade GRLoader to the latest version.
   - Changes made to transactions in the TWA are not audited.

5. Repeat steps 3 as needed.

TWA Administration

This article contains the following topics:

The TWA may require the following administration:

- Extend the TWA - required when you extend any OOB families or when you define your own custom families.
- Archive and purge of the TWA
- How to use the TWA with CA Configuration Automation
- Database limitations

Extend the TWA Object

Any modifications to the CMDB family schema require parallel modifications to the TWA schema. If no custom families or attribute have been defined, the TWA requires no modifications.

To extend the TWA object:

1. Modify the user-defined families and attributes *using the procedures in Extending CMDB*. (see page 2603)

2. Add the new family attributes to the ci_twa_ci schema using Web Screen Painter Schema Designer.
   To add a new attribute to ci_twa_ci schema:

   a. Using Web Screen Painter Schema Designer, open the schema for the ci_twa_ci table.

   b. Add the desired family attribute to the extension table.

   c. Publish the modified ci_twa_ci schema.

   Note: The new attributes must be type STRING and must hold the longest possible text value.

3. Add the metadata for the custom family to the TWA as follows:

   a. Using Web Screen Painter, open the cmdb_metadata_site_families.htmpl file.

   b. Add an PDM_INCLUDE for the appropriate cmdb_metadata_*extension*.htmpl file that was created for the custom family.

Archive and Purge of the TWA

To maintain the TWA, CA SDM provides the following archive/purge rules:

- **CI Inactive Transactions**
  Archives and purges the CI transactions that are marked for deletion.

- **CI Successful Transactions**
  Archives and purges the CI transactions that have completed successfully.

- **Relationship Inactive Transactions**
  Archives and purges relationship transactions that are marked for deletion.

- **Relationship Successful Transactions**
  Archives and purges relationship transactions that have completed successfully.

You can select how often the rules run or whether they are enabled.

You can modify and enable the rules for enabling archive and purge of the TWA. If you are a heavy user of the TWA, be aware of the limitations on the number of records in the TWA imposed by the DBMS.

If you have to reinitialize the TWA to clear out all data in the TWA, complete the following tasks:

- Set all transactions to inactive
- Run archive purge

Important! Do not use SQL to delete all records in the TWA because it deletes required header records.

TWA GRLoader Command Options

CA SDM provides the following command options for use in GRLoader TWA processing:

- **-lttwa**
  Loads XML into the initial state.
- **-lttwar**
  Loads XML into the ready state.
- **-lftwa**
  Loads transactions from the TWA.
- **-lftwai**
  Loads transactions from the TWA and inactivates successful transactions.
- **-chg *nnnn***
  Used with - lftwa and -lftwar. Loads only those transactions that are associated with change order *nnnn*.
  Note: The Change Order string is not validated when loaded into the CMDB.
- **-I**
  Ignore case of lookup attributes. By default free-form text for lookup attributes is processed as case sensitive unless you use this option.
- **-simci**
  Determines whether the CI transactions can create or update CIs. When this option is used, GRLoader perform error checking against CIs only.
- **-simrel**
  Determines whether relationship transactions can create or update relationships. This option verifies relationships for the existence of the provider and dependent CIs, validates relationship types, and so on.

TWA GRLoader Configuration File Options

CMDB provides the following TWA options for the GRLoader configuration file:

grloader.emptyvalue=EMPTY

grloader.loadfromtwa=yes

grloader.loadfromtwa.inactivatesuccessful=yes/no

grloader.loadtotwa=yes

grloader.loadtotwa.ready=yes/no

grloader.workarea.delimiters={ }

grloader.workarea.ignore_transaction_dates=yes

grloader.simulateloadci=yes/no

grloader.simulateloadrelation=yes/no

How to Use the TWA with CA Configuration Automation

To use the TWA with CA Configuration Automation processing, apply patch RO08739 to CA Configuration Automation r5. This patch allows you to specify the - lttwa option in the Other Options field on the Export Options tab of the CMDB Export Report definition. Upgrade the GRLoader component. Contact CA support for questions.

Database Limitations

The TWA is subject to the data limitations of the underlying database, as follows:

- When using TWA and Microsoft SQL Server, the total length of one data transaction must not exceed 8060 bytes.
- When using the dbload and pdm_load utilities, a load operation is restricted to 512 columns.
- Oracle has a 1000-column limitation. If you modify CMDB, verify that the total number of attributes does not exceed 1000 across all families (both CA-supplied and user-defined).
- SQL Server 2005 limitations as described in the following table:

Limitation Type	Limit (32-bit and 64-bit)
Columns per wide table	30000
Columns per base table	1024
Columns per SELECT statement	4096
Bytes per row	8060
Rows per table	Limited by available storage

Manage Relationship Transactions

The Relationship Transaction List displays relationship transaction data input.

Using this page, you can search for relationship transactions.

On the list, you can do the following actions:

- Create a relationship transaction
- Edit in list (except for identifying attributes)

Update a Relationship Transaction

You can view and modify data for a single relationship transaction. On the Relationship Transaction Detail page, you can do the following actions:

- Create a relationship transaction
- View the transaction
- Edit the transaction
- Save or Cancel transaction changes (Edit mode)
- Reset the original transaction data (Edit mode)

To update a relationship transaction:

1. Click Edit.
   The Update Relationship Transaction page appears.
2. Modify and complete fields.
3. Select Active.
4. Click Save.
   The relationship transaction is saved.

When all data entry is complete, you can simulate loading the data to validate the data and verify reconciliation.

Important! Data that you enter into the TWA using this interface must follow certain rules. For more information about the rules, see the "How to load data into the TWA Using GRLoader (see page)" section.

The web UI does not validate case-sensitive data in the TWA. Verify that the values you enter exactly match the lookup values. Alternately, when you run GRLoader, you can specify the - I option to enable case insensitive lookups.

Note: The provider_id or dependent_id are stored as UUIDs in the transaction. However, they are displayed as CI names in the web interface.

Define the Business Infrastructure

Contents

Implement your service desk using CA SDM by defining your business infrastructure with the following objects:

- Configuration item families and classes
- Manufacturers and models
- Service statuses
- Vendors and vendor types

The following information provides a general description for each object and explains how the object is used in the product.

Object Definition Order

You start at the bottom levels of the object hierarchy when you define objects. Therefore, when you define objects at higher levels, you can select from existing objects at lower levels in the hierarchy. For example, because a class has (references) a family, you define families first, followed by classes. Define configuration objects last, after you define all the supporting objects, because they are the top of the hierarchy. Therefore, you define data objects in the following order:

Define First	Define Second	Define Third
Families	Classes	Configuration items
Manufacturers	Models	Configuration items
Service statuses	Configuration items	
Vendor types	Vendors	Configuration items

Manufacturer and Models

Manufacturers identify the manufacturers of the various configuration items of concern to your enterprise. *Models* contain specific information about the products that a particular manufacturer provides to your enterprise. For example, you might define as a manufacturer a particular software company. Then, you would define as models each one of the applications that the company provides for your enterprise.

Defining manufacturers and models makes it easier to manage your configuration items. For example, you can generate a list of models that are provided by a particular manufacturer. You can also generate a list of configuration items of a particular model.

You can enter information about the manufacturers and models of the hardware, software, and services that are associated with your system. You can also reference this information in configuration item records. To create a model. from the Administration tab, navigate to Service Desk, Application Data, Configuration Items, Models. Click Create New and enter the fields as appropriate.

Service Status

Service status identifies the readiness condition of configuration items. Examples of service status include: *in service*, *in repair*, or *discontinued*. Defining service status lets you track the availability and use of configuration items in your enterprise. For example, you can generate a list of configuration items that are currently in repair.

Vendor Types and Vendors

Vendor types are classifications for vendors that identify the type of company providing configuration items. For example, you could classify vendors that you lease configuration items from as leasers. You can classify vendors that provide service to you as providers.

Vendors identify the companies that supply your enterprise, including the type of company and a primary contact. You can also reference a vendor in a user's contact record.

Defining vendor types and vendors gives you a convenient way to organize your configuration items. For example, you can generate a list of vendors that fall under a particular vendor type. You can also generate a list of configuration items from a particular vendor.

External Asset Management Tools

You can integrate CA SDM with other asset management tools such as CA NSM, CA Client Automation, and CA APM. The asset management features of these tools from CA SDM include the following features:

- CA NSM provides the pdm_nsmimp utility (for Windows only) to add asset information to CA SDM.
- CA Client Automation provides a complete set of hardware and software inventory functions. When viewing a CI in the CA SDM client, click Asset Viewer to display more information about the asset.
  Integration between CA SDM and CA Asset Management is activated when the products are installed on the same MDB.

- CA Asset Portfolio Management provides a complete set of asset lifecycle functions. When viewing a CI in the CA SDM client, click Asset Viewer to display more financial information about the asset.
  Integration between CA SDM and CA Asset Portfolio Management is activated when the products are installed on the same MDB.

About MDR

This article contains the following topics:

The Configuration Management Database Federation (CMDBf) is a working group that is composed of representatives from CA, IBM, HP, Microsoft, and other companies. The CMDBf defines a Management Data Repository (MDR) as anything that collects information about configuration items (CIs).

To create the relationship between an MDR and its CIs when implementing MDR Launcher, complete the following tasks:

1. Define the MDR.

2. Define the CIs that reference that MDR.
   You cannot have a CI that references a non-existent MDR. You can define a CI without defining an MDR association. You can add the MDR information during an update or can edit to take advantage of the MDR Launcher capability.

Multiple MDRs can discover the same CI. After the CI is discovered, each MDR attempts to manage that CI, and an MDR can do the following actions:

- Discover detailed attributes about the CI.

- Attempt to modify the CI state.

Example: A CI Discovered by Multiple MDRs

Both Network Management software and an Asset Management software package discover a CI.

- The network management software maintains information about network configuration and network topology.

- The asset management software contains information regarding cost, depreciation, licensing, and maintenance contracts for that particular CI.

MDR Classes and MDR Names

An IT enterprise can include many MDRs. Each MDR has an identifier that is known as an *MDR name (mdr_name*). It is common for an MDR to use the host server name as the mdr_name. The server name is used to allow multiple MDRs to reside on the same host server. Therefore, an MDR class (mdr_class) is appended to the mdr_name to identify each MDR uniquely.

CA Configuration Automation is an enterprise discovery tool that integrates tightly with CMDB Each CA Configuration Automation MDR defined to the CMDB must have an *mdr_class* of **Cohesion**. For more information about CA Configuration Automation, see the CA Configuration Automation online help. For CA Configuration Automation-CMDB integration, see the *CA Configuration Automation Implementation documentation*.

How does an MDR Complement CA SDM?

An MDR typically contains more detailed CI information than CMDB. However, a single MDR is not typically aware of the existence of other MDRs. It does not focus on the relationships that a particular CI can have with other CIs, especially if they are contained in other MDRs. CMDB manages this type of environment well, because it focuses on managing CIs regardless of their MDR source.

CMDB is not intended to store all attributes for all CIs. CMDB is used to consolidate the most important attributes that must be managed centrally. Attributes that are under the control of change management are excellent candidates for inclusion in the CMDB. Attributes that CMDB does not manage can be accessed by using the MDR Launch capability. In addition, CMDB provides the CMDBf Viewer. CMDBf Viewer allows side by side comparison of CI attributes across multiple CMDBs and MDRs.

MDR Launcher

The MDR Launcher lets you view data from almost any MDR by using a web page, without any coding. MDR Launcher lets anyone viewing a CI to obtain more details about the CI, and to gain control over it (if the MDR supports such control).

Some uses of the MDR Launcher include the following ones:

- From the hardware.server detail page, launch CA Configuration Automation to verify a change.
- From an Air Conditioning CI detail, launch to a vendor web page for diagnostic information and incident reporting.
- From a Contract CI, launch a contracts management system to learn contract details.
- From an SLA CI, launch CA Service to review Service Level Agreements before modifying.
- From a Server CI, launch CA Remote Control to take over the server to diagnose and correct a problem.

Define a URL to Launch an MDR

CMDB uses a URL to start a web page session with the source MDR to operate the MDR Launcher. You define the URL that CMDB uses.

Follow these steps:

1. Click the Administration tab.

2. In the left pane, open the CMDB, MDR Management tree.

3. Click MDR List.
   The Management Data Repository (MDR) List page appears.

4. Click an existing MDR (or create and save a new one).
   The MDR Provider Definition page appears.

5. Click Edit.
   The Update MDR Definition page appears.

6. Complete the following parameters:

   - **Hostname**
     Specifies the Network address or DNS name of the web server that serves up web pages for the MDR.

   - **Port**
     Specifies the port number that the Hostname web server uses.

   - **Path**
     Specifies the path to the web page, including the page itself.
     Parameters
     Specifies any parameters that are used to identify the desired CI to the MDR. CMDB posts this information to the MDR.

   - **Userid**
     Specifies the userid, if a common userid is allowed access to the MDR.

   - **Shared Secret**
     Specifies information that is shared between CMDB and the MDR. For CA Cohesion MDRs, this value must match the value that is specified in the CA Cohesion properties file, for the com.cendura.security.oneclickauth.secret value.

   - **CMDBf Namespace**
     Specifies the federated_asset_id that is passed to the query as a local ID. For CA CMDB, the value is http://cmdb.ca.com/r1.

   - **CMDBf Timeout**
     (Optional) Specifies time limit for CMDBf endpoint query.
     Default: 10 seconds

   - **CMDBf Endpoint**
     Specifies the Query Service endpoint for the MDR. Required for CMDBf Viewer and retrieving updated MDR data. If you use CA CMDB as an MDR provider, the value is http://cmdb_hostname:cmdb_port/axis/services/QueryPort (http://cmdb_hostnamecmdb_port/).

7. Save the definition.

The URL is defined. In addition, the URL can contain the substitution variables to further qualify the CI to the MDR. For more information, see the Using the MDR Launcher (see page 2542) topic.

Set Up a CA APM MDR Provider

You can set up an MDR to be the CA APM provider.

Follow these steps:

1. On the Administration tab, click CMDB, MDR Management, MDR List.

2. Click Create New to specify the CA APM MDR.
   The MDR Provider definition appears.

3. Enter the following required MDR provider information:

   - Button Name -- Specify APM or any other valid button name. We recommend using a Button Name of APM.

   - MDR Name -- Specify APM for CA Asset Portfolio Management r11.3.4 or ITAM for CA APM r12.6

   - MDR Class -- Specify GLOBAL.

   - Hostname -- Specifies the CA APM server name by using the network address or the DNS name of the CA APM web server.

   - URL for Launch in Context -- Specifies http://{hostname}:{port}/{path}?{parameters} and must not be changed.

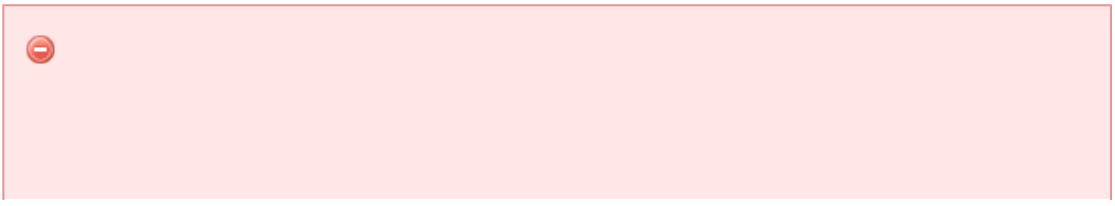
   The MDR provider form automatically populates the path and parameter values with the required CA APM launch in context information.

4. Click Save.
   The CA APM MDR provider is set up. For more information about the MDR launcher, see the MDR Launcher (see page 2542) topic.

Launch in Context from CMDB to CA APM

The CMDB MDR Launcher facility supports launch in context to CA APM when the tools share the same MDB. The CMDB UI provides a launch in context button on the Attributes tab in the CI detail form. The button appears when the user creates a special CA APM MDR provider definition.

The CA APM MDR definition has all the capabilities of a traditional MDR. The CMDB Versioning feature also supports launch in context directly from an attribute log entry that is associated with each CA APM change.



Important! Unlike other MDRs, the CA APM MDR is automatically associated with each CI or Asset. The MDR class of GLOBAL and MDR name of APM are used to identify the CA Asset Portfolio Management r11.3.4 MDR. The MDR class of GLOBAL and MDR name of ITAM are used to identify the CA APM r12.6 MDR. Use of the CA APM MDR is fully compatible with other MDRs, even for the same CI.

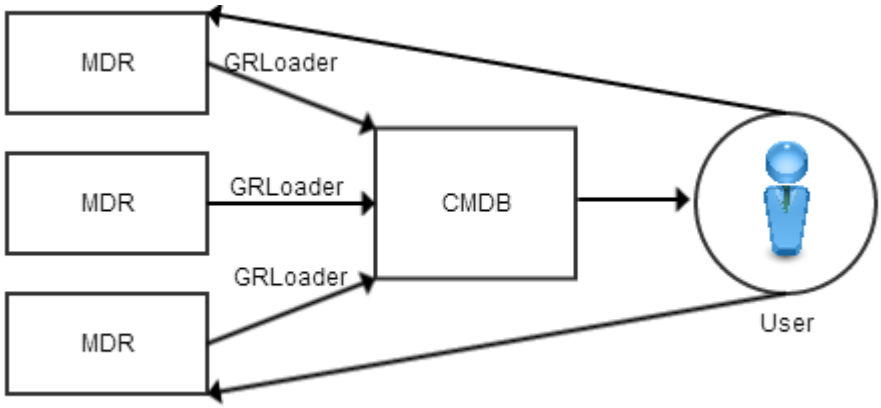
Using the MDR Launcher

This article contains the following topics:

The MDR Launcher

One of the main purposes for implementing CMDB is to aggregate data from multiple data sources (known as MDRs). However, a CI must always include a reference back to its MDR origin.

CMDB provides facilities for importing and loading CIs and also for associating the CIs with their origins. To view a CI in the CMDB, use the MDR Launcher. When you use the MDR Launcher for this purpose, you can return seamlessly to the CI-originating system. See the following diagram.



Using the MDR Launcher, it is possible to implement a “closed loop” change management process such as the following one:

1. Create a change record.
2. Implement the change.
3. Verify the change by checking the MDR source.
4. To indicate that the change has been made, update the CMDB.

From a Problem Management process perspective, you can use the MDR Launcher in the following way:

1. Detect a problem.
2. Determine the severity and pervasiveness of the problem. To determine what dependent CIs are affected, use the CI relationship data.
3. Determine possible causes of the problem by researching provider CIs.
4. Perform an in-depth analysis if necessary using the detailed information available in the MDR. To take corrective action, use the MDR.

MDR Terminology

The following terms are used in CMDB-MDR integration:

A management data repository (MDR) represents software or data that contains source information about a CI. An MDR generally contains more unrefined CI information than the CMDB, which contains a managed subset of that data.

An *MDR class* (MDR_CLASS) is used to group MDRs that CMDB processes similarly. Three special MDR classes include: **COHESION**, **GLOBAL**, and **cmdbf**.

An *MDR name* (MDR_NAME) is the name that an MDR uses to reference itself. Verify that the mdr_name and mdr_class value combination must be unique within your enterprise.

A Federated asset ID (FEDERATED_ASSET_ID) is a unique MDR identifier for a CI.

The different CI families typically use different respective MDRs as data providers. However, a single CI can have multiple MDR data providers. For example:

CI Family	MDR_CLASS
Contact	human resources system telephone directory single sign-on authentication system
Document	document management system
Air Conditioning	document management system contract management system air conditioning control system
Mainframe	tape management system DASD management system performance management system job scheduler
Storage	storage management system asset management system
Location	asset management system education calendar office directory
Network	network management systems problem management system

There can be multiple MDRs in each MDR class, and each MDR can contribute data to multiple CIs. A given CI can receive data from zero or more MDRs. A CI also can have data contributed to it independently. Consider the following example: One mainframe CI has data that Disk Management System 1 donated. Another mainframe CI has data that Disk Management System 2 and Job Scheduler 2 donated. CMDB manages the relationships among CIs and all their related MDRs.

MDR Mapping

Every MDR has a unique way of identifying the CIs that it manages. Those identifiers are seldom synchronized across MDRs. For example, when referencing a specific Contact CI, different MDRs can use different identifiers. A national identity number, telephone number, license number, or Employee ID can identify the same person. The process of associating these disparate identifiers with the same unique identifier (UUID) maintained in the MDB is named *mapping*. Mapping occurs automatically when data is imported using GRLoader when the CI contains the <mdr_name> <mdr_class> and <federated_asset_id> tags. Mapping can also be accomplished manually through the Administration functions in the user interface. A CI that has no mappings that are associated with it is named *unfederated*. Every CI is automatically mapped to global MDRs using the UUID as the federated_asset_id.

MDR Launching

When you view a CI with the CMDB user interface, click buttons to launch an MDR user interface directly. One button per MDR mapping exists for the focus CI. To verify that a change request has completed successfully, use this launching. To obtain more information about a CI than the CMDB has collected, use this launching.

CMDBf Viewer

CA SDM provides the CMDBf Viewer with the results of CI federation across MDRs. From a CI Detail page, click CMDBf Viewer to see CI attributes of federated CMDBs and MDRs in parallel. On the Federated View page, you can click Retrieve to update the information from any of the federated MDRs. For better readability, CMDB metadata files can reconcile MDR attribute names and CMDB attribute names.

Note: This feature requires MDRs that support Query. You configure the MDR CMDBf Endpoints to display their results on Federated View.

Define an MDR to CMDB

Before you use the CMDBf Viewer, define the MDR to CMDB.

Follow these steps:

1. On the Administration tab, navigate to CMDB, MDR Management, MDR List.

2. Click Create New.
   The Create New MDR Definition page appears.

3. Complete the following fields:

   - **Tenant**
     Identifies the tenant owner of this MDR (if multi-tenancy is installed).

   - **Button Name**
     Specifies the button label to appear on the CI Detail page. This name must be unique for each MDR. Required for “launch in context” and CMDBf Viewer.

   - **MDR Name**
     Specifies the string to match the XML data that is sent in the mdr_name field. While the MDR can use any string, the host name is used frequently. This name together with the mdr_class form a unique name for the MDR. Required for “launch in context” and CMDBf Viewer.

   - **MDR Class**
     Specifies the class that must match the data that is sent in the mdr_class field in the XML. While this name can be anything, it must together with the mdr_name field form a unique identifier for the MDR. Global MDRs are defined with an MDR Class of GLOBAL.

     - CA Configuration Automation MDRs must specify an MDR class of COHESION, which automatically sets the Path, Parameters and URL to be Launched fields to the required CA Configuration Automation launch-in-context values.

     - CA Asset Portfolio Management r11.3.4 MDRs must specify an MDR name of APM and MDR class of GLOBAL, which sets the Path, Parameters, and URL to be Launched fields to the required CA Asset Portfolio Management r11.3.4 launch-in-context values.

- CA APM r12.5 MDRs must specify an MDR name of ITAM and MDR class of GLOBAL, which sets the Path, Parameters, and URL to be Launched fields to the required CA APM 12.5 launch-in-context values.

- For CMDBf Viewer, MDR Class must be cmdbf.

- **Active**
  Denotes this MDR definition as active or inactive. The Inactive MDR definitions are logically deleted, but they can be made active again by using the Search utility.

- **Owner**
  Specifies the contact responsible for this MDR.

- **Description**
  Specifies a description in free-form text.

- **Hostname**
  Specifies the host name, DNS name, or IP address of the host, which contains the web server. The web server is the one that hosts the web page to be launched. Required for “launch in context”.

- **Port**
  Specifies the TCP/IP port that is used by the MDR web server to serve up web pages. Port 80 is the default. Required for “launch in context”.

- **Path**
  Specifies the portion of the URL that precedes the question mark (?) character. This information can be obtained from your MDR documentation.

  - For mdr_class of Cohesion, the value is set automatically to "CAisd/html /cmdb_cohesion.html" and cannot be changed.

  - For mdr_name of APM and mdr_class of GLOBAL, the value is set automatically to apm /frmObject.aspx and cannot be changed.

  - For mdr_name of ITAM and mdr_class of GLOBAL, the value is set automatically to ITAM/Pages/Asset.aspx and cannot be changed.

- **Parameters**
  Specifies the portion of the URL that follows the question mark (?) character. This information can be obtained from the MDR documentation.

  - For mdr_class of Cohesion, the value is set automatically to "hostname={hostname} +port={port}+family={family}+name={name}+secret={password}+federated_asset_id= {federated_asset_id}". The value cannot be changed.

  - For mdr_name of APM and mdr_class of GLOBAL, the value is set automatically to ObjectID={cmdb_asset_id}&obj=11&FUNCTION=1&WinID=OBFRASSET{cmdb_asset_id} &WinContainerID=. The value cannot be changed.

  - For mdr_name of ITAM and mdr_class of GLOBAL, the value is set automatically to ParentClass=Asset&assetid={cmdb_asset_id}&TicketID={itam_ticketid}. The value cannot be changed.

- **Userid**
  Specifies the MDR user logon, if necessary. This value is substituted into the URL wherever {userid} is found. If blank, userid defaults to whomever is signed on.
  For CA Configuration Automation, "Shared Secret" is the secret that is used to access CA Configuration Automation, if necessary. This value is substituted into the URL wherever {password} is found. For more information about defining the MDR, see the *CA Configuration Automation Implementation documentation*.

- **Shared Secret**
  Specifies information that is shared between CMDB and the MDR. This value is substituted into the URL wherever {password} is found. For CA Configuration Automation MDRs, the value must match the value of the “com.cendura.security.oneclickauth.secret”. For more information about creating a shared secret, see "Integrating with CA CMDB" in the *CA Configuration Automation Implementation documentation*. Required for CMDBf Viewer.

- **CMDBf Namespace**
  Specifies the federated_asset_id that is passed to the query as a local ID. For CMDB, the value is http://cmdb.ca.com/r1.

- **CMDBf Timeout**
  (Optional) Specifies time limit for CMDBf endpoint query. Default is ten (10) seconds.

- **URL to be Launched**
  Default value of http://{hostname}:{port}/{path}?{parameters}. For some MDRs, it can be overridden if necessary to accommodate MDR-specific requirements. Required for "launch in context".
  For mdr_name of APM and mdr_class of GLOBAL, the value is http://{hostname}:{port}/{path}?{parameters}
  For mdr_name of ITAM and mdr_class of GLOBAL, the value is http://{hostname}:{port}/{path}?{parameters}
  For mdr_class of Cohesion the default value is http://*cmdb_hostname*:*cmdb_port*/{path}?{parameters}
  where:
  cmdb_hostname is the host name, DNS name, or IP address of the CMDB web server. Defaults to the current hostname that is accessing the CMDB web server.
  cmdb_port is the TCP/IP port of the CMDB web server. Defaults to the current port number used to access the CMDB web server.

  > **Note:** If you have enabled SSL support for CA Configuration Automation, set the URL to: http://hostname:port/{path}?{parameters}+https=yes (http://hostnameport/)

  For information about enabling CA Configuration Automation HTTPS support, see the CA Configuration Automation online help topic Creating the HTTPS Certificate and Enabling HTTPS.

- **CMDBf Endpoint**

  Specifies the Query Service endpoint for the MDR. Required for CMDBf Viewer and retrieving updated MDR data. If you use CA CMDB as an MDR provider, the value is http://cmdb_hostname:cmdb_port/axis/services/QueryPort.

4. Click Save.

   The MDR is defined.

MDR URL Definitions

The URL to be launched has the default value of http://{hostname}:{port}/{path}?{parameters}. If necessary, you can modify this expression to accommodate any MDR-specific requirements. The URL is required for "launch in context".

For mdr_name of APM or ITAM and mdr_class of GLOBAL, the default value is:

```
http://{hostname}:{port}/{path}?{parameters}
```

For mdr_class of Cohesion, the default value is:

```
http://cmdb_hostname:cmdb_port/{path}?{parameters}
```

- ***cmdb_hostname***
  The cmdb_hostname variable specifies the hostname, dnsname, or IP address of the CMDB web server. The variable defaults to the current hostname currently accessing the CMDB web server.

- ***cmdb_port***
  The cmdb_port variable specifies the TCP/IP port of the CMDB web server. The variable defaults to the current port number that is used to access the CMDB web server.

Include http=yes when you set the URL if you have enabled SSL support for CA Configuration Automation. See the following example:

```
http://hostname:port/{path}?{parameters}+https=yes
```

For information about enabling CA Configuration Automation HTTPS support, see the CA Configuration Automation online help.

MDR Launch URL

The MDR launch URL has the following default value:

```
http://{hostname}:{port}/{path}?{parameters}
```

You can modify this expression to accommodate any MDR-specific requirements. The URL is required for "launch in context."

- For mdr_name of APM or ITAM and mdr_class of GLOBAL, the default value is:

  ```
  http://{hostname}:{port}/{path}?{parameters}
  ```

- For mdr_class of Cohesion, the default value is:

  ```
  http://cmdb_hostname:cmdb_port/{path}?{parameters}
  ```

- ***cmdb_hostname***
  The cmdb_hostname variable specifies the host name, DNS name, or IP address of the CMDB web server. The variable defaults to the host name currently accessing the CMDB web server.

- ***cmdb_port***
  The cmdb_port variable specifies the TCP/IP port of the CMDB web server. The variable defaults to the current port number that is used to access the CMDB web server.

Set the URL to include https=yes in the query string, if you have enabled SSL support for CA Configuration Automation. See the following example:

```
http://hostname:port/{path}?{parameters}+https=yes
```

For information about enabling CA Configuration Automation HTTPS support, see the Cohesion online help.

Defining Launch Parameters for URL Substitution

When defining an MDR, the following parameters can be used to construct its URL for display. These parameters are substituted with their appropriate values at run time. These variables must be specified in the fields that were described previously.

hostname is the MDR host name from the MDR definition.

alarm_id is the IP address of the selected CI.

federated_asset_ID is the unique identifier of the selected CI in the MDR.

cmdb_asset_id is the asset ID for the CI.

port is the MDR port number from the MDR definition.

userid is the user ID from the MDR definition. If blank, userid defaults to whomever is currently signed on.

password is the shared secret from the MDR definition.

mdr_name is the mdr_name from the MDR definition.

mdr_class is the mdr_class from the MDR definition.

class is the class of the selected CI.

family is the family of the selected CI.

path is the path as described in the MDR definition.

name is the name of the selected CI.

model is the model of the selected CI.

manufacturer is the manufacturer of the selected CI.

itam_ticketid is the ticket id to log in to CA APM.

Example: Launching an MDR

A CMDB user is looking at a Server CI named server1. Server1 has a map to an internally developed application that is named Comet. Comet uniquely identifies server1 as server:server1.

Comet is defined as an MDR with the following properties:

- Hostname: CometServer
- Port: 80
- Path: index.php
- Parameters: item={federated_asset_id}
- Launch_url: http://{hostname}:{port}/{path}?{parameters}

In CMDB, when the user clicks Comet on the Attributes tab of the server1 CI, a web browser opens the following URL:

http://CometServer:80/index.php?item=server:server1

Parameters for URL Substitution

When defining an MDR, you can use the following parameters to construct its URL for display. These parameters are substituted with their appropriate values at runtime. These variables must be specified in the MDR field definitions.

- **{hostname}**
  Specifies the MDR host name from the MDR definition.
- **{alarm_id}**
  Specifies the IP address of the selected CI.
- **{federated_asset_ID}**
  Specifies the unique identifier of the selected CI in the MDR.
- **{cmdb_asset_id}**
  Specifies the asset ID for the CI.
- **{port}**
  Specifies the MDR port number from the MDR definition.
- **{userid}**
  Specifies the user ID from the MDR definition. If blank, userid defaults to whomever is currently signed on.
- **{password}**
  Specifies the shared secret from the MDR definition.

- **{mdr_name}**
  Specifies the mdr_name from the MDR definition.
- **{mdr_class}**
  Specifies the mdr_class from the MDR definition.
- **{class}**
  Specifies the class of the selected CI.
- **{family}**
  Specifies the family of the selected CI.
- **{path}**
  Specifies the path as described in the MDR definition.
- **{name}**
  Specifies the name of the selected CI.
- **{model}**
  Specifies the model of the selected CI
- **{manufacturer}**
  Specifies the manufacturer of the selected CI

Example: Use Parameters for URL Substitution

A CMDB user is looking at a Server CI named server1. The Server CI has a map to an internally developed application that is known as Comet. Comet uniquely identifies server1 as server:server1.

Comet is defined as an MDR with the following properties:

- Hostname: CometServer
- Port: 80
- Path: index.php
- Parameters: item={federated_asset_id}
- Launch_url: http://{hostname}:{port}/{path}?{parameters}

In CMDB, when the user clicks Attributes, Comet in the server1 CI, a web browser opens the following URL:

```
http://CometServer:80/index.php?item=server:server1
```

Federation Using GRLoader

When using GRLoader, the following XML tags must be populated in every CI in the XML document. These tags apply to every MDR family.

- <mdr_name>

- <mdr_class>
- <federated_asset_id>

> **Note:** CA Configuration Automation automatically provides mdr_name, mdr_class and federated_asset_id.

if the XML tags are missing, “launch in context” is not possible. This is because, the origin of the CI cannot be determined.

To identify the source of a CI, you can modify the XML before it is input into GRLoader. You can use a text editor to modify the XML and make a global change. You can also program this task.

For more information about MDR identification and GRLoader, see the GRLoader XML (see page 4306) topic.

Federate a CI

If CIs are loaded into CMDB before their corresponding MDR is defined, they are unfederated. Unfederated means that the CIs are not yet connected to an MDR and they do not yet support “launch in context”.

Follow these steps:

1. Define the required MDR.
2. Do one of the following tasks:
   - Manually map the CI.
   - Rerun the CA Configuration Automation report which created the CI, specifying Allow update of existing CIs on the report. For more information about CA Configuration Automation Reports, see the *CA Configuration Automation Product documentation*.
3. Rerun GRLoader, specifying the same input file that was used to create the CIs.
   The CMDB reconciliation engine merges the MDR information into the existing CIs.
4. Create an XML document that describes the CI and its MDR and run GRLoader in Update mode.
   The CMDB reconciliation engine merges the new information into the existing CI. The existing CI is federated.

Example: Specify CI Location

To locate the CI you want to update, verify that the reconciliation engine is provided with enough information. In the following example, end tags are removed and spaces added for readability.

```
<ci>
   <name>         server3
   <mac_address>
```

```
   <serial_number>
   <asset_num>
   <dns_name>
   <mdr_name>     mdr_one
   <mdr_class>    Cohesion
</ci>
```

Define Multiple MDRs to a CI Using GRLoader

You can define multiple MDRs to a CI by using GRLoader.

To define multiple MDRs to a single CI, the XML document can repeat the <ci> node. With each duplicated <ci> mode, specify a different mdr_name and mdr_class. In other words, each MDR can contribute its attributes independently of any other MDR that contributes data to the CI.

Example: Define Multiple MDRs to a CI

If MDR1 and MDR2 both contribute data to the server2 CI, the XML document looks something like the following example. In the example, end tags are removed and spaces added for readability.

```
<ci>
   <name>      server2
   <mdr_name>  mdr1
   <mdr_class> Cohesion
   <diskspace> 500 gb
   <disktype>  SCSI-3
</ci>
<ci>
   <name>     server2
   <mdr_name> mdr2
   <mdr_class>Service Assure
   <sla>
</ci>
```

CMDB reconciles the two previous CIs to the same CI and associates each MDR to that single CI.

Note: The CIs can be imported in one or two runs of GRloader.

Map Between MDR CIs and CMDB CIs

After you define a CI manually using the File, New Configuration Item... option, manually define the mapping between this CI and the CI in the federated MDR. Associate a CI with an MDR in the following ways:

- Editing the CI.
- Using the Federated CI Mapping node on the CMDB Administration tab.

Follow these steps:

1. To create a mapping by editing the CI, complete the following steps:

    a. Display the CI Detail page of the CI that you want to associate with an MDR.

    b. Click Edit.

    c. Display the Attributes tab.

    d. Click Add MDR.
    The CI is associated with the MDR.

2. To create a mapping using the Federated CI Mapping page, complete the following steps:

    a. Click the CMDB Administration tab.

    b. Open the Management Data Repository node.

    c. Select the Federated CI Mapping node.
    The Federated CI Mapping List appears.

    d. Click Create New.
    The Create New Federated CI Mapping For page appears.

    e. Associate the CI with the MDR by completing the Federated CI Mapping fields:

    - **CI Name**
      Specifies the name to use to identify the configuration item.

    - **Federated Asset ID**
      Specifies the string identifier that is used by the source MDR to identify this CI. The MDR software determines the identifier.

    - **MDR Name**
      Specifies the name that identifies the MDR (and its MDR button).

    - **Active**
      Denotes whether this mapping is active or not. Mappings cannot be deleted, only inactivated.

    f. Click Save.
    The mapping between this CI and the CI in the federated MDR is defined.

How To Configure MDRs for CMDBf Viewer

To use the CMDBf Viewer, set up your federated MDR providers to point to the CMDBf query service, as follows:

- External MDRs must provide a query service that can handle InstanceIdConstraint query.
- Button Name, MDR Name, and MDR Class are required to show the CMDBf Viewer button on the CI Detail page.
- MDR Class must be defined as **cmdbf**

- For CMDB, CMDBf Namespace must be set to **http://cmdb.ca.com/r1**. For other CMDBs and MDRs, see the appropriate documentation.
- Timeout is optional. Default is ten (10) seconds.
- To display a working Retrieve button on the Federated View, define CMDBf Endpoint, Userid, and Shared Secret.

Note: An existing CMDB system can be set up as a CMDBf provider by specifying an CMDBf Endpoint of "http://servername:port/axis/services/QueryPort" where:

- hostname is the computer where CMDB is installed (localhost or computer name).
- port is the port where CMDB is configured.

Launching the MDR Web Browser Interface

After a mapping between a CI and an MDR is created, a button is placed automatically on the Attributes tab. If multiple MDRs are associated with this CI, multiple buttons appear.

When you click an MDR button, a new page opens. The fully substituted MDR URL that is defined in the MDR definition appears on the page.

Example: Launch CA Cohesion

When a CI has been correctly associated with its MDR, a Cohesion button appears on the Attributes tab. If a button does not appear on the Attributes tab, review the mapping for the displayed CI. Verify that there is a mapping for this CI. Also verify that the target MDR has a URL that can be launched. Clicking the button to launch the MDR causes a new window to open. The window opens to the target URL to launch CA Cohesion.

CA Cohesion Integration

Consider the following items when integrating CA Configuration Automation with CMDB:

- Integrating Cohesion with CMDB

  Note: For information about Cohesion-CMDB integration, see the *CA Configuration Automation Implementation documentation*.

- Importing CIs from a Cohesion MDR

  For information about how to import CIs from a Cohesion MDR, see the help in the CA Configuration Automation Report Templates tab.

- Launch-in-Context for Cohesion MDRs
  For launch-in-context integration to work best with CA Configuration Automation, we recommend that you define the Cohesion MDR *before* running the Cohesion CMDB Report. You can define Cohesion MDR in the CMDB Administration tab.

  Note: CA Configuration Automation does not support a unique Federated asset ID for NIC or File System CIs. Therefore, Cohesion does not support MDR Launcher for NIC or File System CIs. As a result, a Cohesion-based NIC or a File System CI does not display an MDR launch button even when it was imported successfully.

Reconcile CI Ambiguities Using MDR

Reconciliation ensures that updates from multiple data sources that refer to the same business object only update a single CI. A single CI is updated even if the data sources possess different identifying information.

Ambiguity represents the possibility that a CI is not unique. CIs are *ambiguous* when they represent the same real business object. The CI transactions are ambiguous when they have more than one possible target CI.

Ambiguous CIs can lead to incorrect data in the CMDB, which negates the value of the CMDB. A negated value can lead to incorrect business actions.

Automatic CI reconciliation is a key CMDB advantage that saves significant time, when compared with manual data maintenance. The process of reconciling CIs uses several specific identifying attributes. However, automatic reconciliation can result in the following matches:

- False positive matches
  Existing CIs are updated instead of creating a CI.

- False negative matches
  New CIs are created instead of updating an existing CI. The set of CIs with similar identifying attributes are ambiguous, because they resemble the same real business object with similar identifying attributes.

CA Service Desk Manager supports the following reconciliation approaches:

- **MDR-Based Reconciliation (Passive)**
  Allow the CMDB to reconcile any ambiguous data based on the MDR-Based Reconciliation process.

- **Identify and Resolve ambiguous CIs (Reactive)**
  Identify and resolve ambiguous CIs through identification and management of existing CIs in the CMDB.

- **Review and modify inbound data using a transaction work area (Proactive)**
  Review and modify inbound data before loading into the CMDB using a transaction work area (TWA).

How to Identify and Resolve Ambiguous CIs

Contents

We recommend managing the ambiguity for a CI by reviewing each CI. In each case, the Configuration Administrator must detect when the ambiguity exists and must determine the optimal approach. CA SDM takes a broad approach to identify and manage ambiguous CIs that are already in the CMDB.

The ambiguity index is an operational measure of the potential nonuniqueness of a configuration item (CI) or a CI transaction item, which is based on its identifying attributes. The ambiguity index measures the probability of one or more CIs representing the same real business object. Or, it measures the probability that a CI transaction has more than one possible target CI.

Important! If you manually delete CIs with database queries, errors can occur for CIs ambiguity indexes. To avoid these errors, execute the cmdb_update_ambiguity utility and set the -full parameter to 1. This parameter ensures that you receive the accurate ambiguity indexes when you execute cmdb_update_ambiguity.bat or the shell script.

CI Ambiguity Example

Data from four different data sources is loaded into the CMDB. Each data source uses its own subset of identifying characteristics. Because of this inconsistency, more CIs exist in the CMDB than are desired.

Example: Ambiguous CIs

The following four CIs reside in the CMDB:

- Name(Server1) DNS Name(dns1) Serial Number(serial1)
- Name(Server1) DNS Name(dns1)

- Name(Server2) DNS Name(dns1) Serial Number(serial1)
- Name(Server3) MAC Address(mac1)

Due to shared identifying characteristics, the two instances of Server1 and Server2 are ambiguous with each other. Server3 is not ambiguous.

Every CI has an ambiguity index that is associated with it. The ambiguity index is approximately the number of existing CIs that match on any of the identifying attributes. The greater the index, the more CIs that match on the identifiers. Therefore, the greater the probability that CI data was entered inconsistently and that more CIs are incorrectly created. CIs with an ambiguity index of zero are unique across all identifiers and are therefore unambiguous.

The ambiguity index of each of the previous CIs is

- First Instance for Server1: Count of other CIs matching name + dnsname + serial number = 1+2+1=4
- Second Instance of Server1: Count of other CIs matching name + dnsname = 1+2 = 3
- Server2: Count of other CIs matching name + dnsname + serial number = 0 +2+1 = 3
- Server3; Count of other CIs matching name + mac address = 0+0 = 0

Follow these steps:

1. Identify ambiguous CIs (see page 2558).
   - Calculate the ambiguity index for all CIs.
   - Review the list of ambiguous CIs from the Scoreboard.
2. Determine if the identifying attributes for each CI are valid.
3. Resolve the ambiguous CI (see page 2563) with one of the following actions:
   - Modify the identifying attributes.
   - Exclude a CI from ambiguity management.
   - Reject a CI Update by inactivating the CI.
   - Supersede a CI.

Identify Ambiguous CIs

Investigate any CI with a nonzero ambiguity index to determine if it is unique or it was inadvertently created. Ambiguous CIs can be created because of incorrect reconciliation. CIs are not ambiguous by themselves, they are ambiguous with other CIs. A system can have many sets of ambiguous CIs, each set containing CIs with common values for the identifying attributes.

When you research the ambiguity of a CI, you also research the ambiguity of other CIs in the same set. When you resolve the ambiguity of a single CI, you reduce the ambiguity of other CIs in that set.

CA SDM has reconciliation management tools, which enable you to find ambiguous CIs. The tools also help you find the set of CIs of which the ambiguous CI is a member. You can research the underlying cause of the ambiguity and can resolve it.

When managing ambiguity, follow these steps:

1. Calculate the ambiguity index for all CIs.
2. To view the list of ambiguous CIs, use the scoreboard. The scoreboard lists all CIs that are ambiguous, in descending order of ambiguity.
3. Starting with the CI that has the highest level of ambiguity in the scoreboard, inspect all CIs in its ambiguity set. The reconciliation tab on CI detail form of a single CI lists all other CIs in the ambiguity set.
    a. Determine if all CIs in the set are legitimate or if an error was made in reconciliation. Review the identifying attributes. Determine if the CIs in the set are created correctly or are created due to a false negative reconciliation match.
    b. Determine which CIs in the set, if any, are false negatives.
    When you determine that a false negative reconciliation match has occurred, and more CIs are created, determine the valid CIs and the incorrectly-created CIs. Consider factors such as identifying attributes and attributes such as last update date, related problems, and issues.

Calculate the Ambiguity Index

Before you can begin managing ambiguity, update the ambiguity index for the existing CIs and CI Transactions. You update the ambiguity index for CIs and CI transactions by running the cmdb_update_ambiguity command.

Important! Run cmdb_update_ambiguity at least once to measure CI or CI transaction ambiguity. If you do not run the command, all ambiguity indexes are 0 (zero). An ambiguity index of zero implies no ambiguity.

You can run the utility before and during ambiguity management. Schedule the utility to run periodically, so the ambiguity indexes reflect the current state of your system.

Follow these steps:

1. Determine the necessary parameters to run the utility.
2. Run the utility.
3. Start the CA SDM Web Client and navigate to the Ambiguous CI or Ambiguous CI Transaction Lists.

cmdb_update_ambiguity Command

You can calculate CI and CI transaction ambiguity indexes by entering command syntax similar to the following command:

```
cmdb_update_ambiguity [parameters]  - m { ci | twa | all }
```

For command parameters, see cmdb_update_ambiguity Parameters (see page 2561).

By default, the CI scan is done from the last scan date. If "-full 1" is specified, a complete scan is performed.

Example: Calculate CI ambiguity on a Microsoft SQL Server database

The following command calculates the ambiguity index for all existing CIs and Transactions in the TWA:

```
cmdb_update_ambiguity  - m all  - d MSSQL  - u servicedesk  - p dbpassword -s
dbserver1
```

Example: Calculate CI ambiguity on an Oracle database

The following command calculates the ambiguity index for CIs and specifies database information.

```
cmdb_update_ambiguity  - m ci  - d Oracle  - u mdbadmin  - p dbpassword -s server1 -
port 1521  - SID orcl
```

Use a Configuration File

You can specify many cmdb_update_ambiguity parameters in a configuration file. You can use the configuration file to secure parameter settings in an encrypted form using operating system tools. The valid keywords and the corresponding command-line options are listed in the parameter table.

Note: If you specify a parameter both on the command line and in a configuration file, the command-line value overrides the configuration file value.

Example: Use a configuration file to specify the parameters for a Microsoft SQL Server database

The following command runs the configuration file ambiguity_mssql.cfg.

```
cmdb_update_ambiguity  - m all -c ambiguity_mssql.cfg
```

Configuration File Format

Configuration file options are specified as *keyword=value*. On Windows, the directory separator can be a double backslash (\\) or a single forward slash (/). The path name must not be enclosed in double quotation marks ("").

The valid keywords and the corresponding command-line options are listed in the parameter table.

Note: A hash mark (#) in column 1 starts a comment line.

Example: Microsoft SQL Server configuration settings

```
#Sample configuration file for Microsoft SQL Server
DBType=MSSQL
DBUser=servicedesk
DBPassword=dbpassword
DBHost=dbserver1
LogLocation=C:\\Program Files\\CA\\Service Desk Manager\\log
LogLevel=ERROR
SchemaName=dbo
```

Example: Oracle configuration settings

```
#Sample configuration file for Oracle
DBType=Oracle
DBUser=mdbadmin
DBPassword=dbpassword
DBHost=dbserver1
LogLocation=/tmp/ambiguity/log
LogLevel=INFO
DBPort=1521
DBSID=orcl
SchemaName=mdbadmin
```

cmdb_update_ambiguity Parameters

You can specify parameters on the command line or in a configuration file (some parameters are command-line only). On the command line, use quotation marks ("") to enclose any path name with spaces. In the configuration file, do not use quotation marks. If any parameter is specified on the command line and in the configuration file, the command-line value overrides the configuration file value.

The cmdb_update_ambiguity command takes the following parameters:

Option	Configuration File Keyword	Values	Notes
-m	(none)	twa, ci, all	(Required) Command line only twa = compute ambiguity on TWA only. ci = compute ambiguity for CIs only. all = compute ambiguity for CIs and TWA.
-d	DBType	MSSQL or Oracle	(Required. Windows only.) Database type. On Linux/UNIX, only Oracle is supported and this option is not needed.
-u	DBUser	<db user name>	

			(Required) Database user name. A user name with spaces must be enclosed in double quotation marks (for example: -u "sys as sysdba"). The quotation marks are not required in the configuration file.
-p	DBPassword	<db password>	(Required) Password for database user. A password with spaces must be enclosed in double quotation marks (for example: -p "secret code"). The quotation marks are not required in the configuration file.
-c	(none)	<configuration file>	(Optional) Command line only The full pathname of the configuration file. The pathname must be enclosed in double quotes if there is a space in the pathname.
-log	LogLocation	<directory to place log file>	(Optional) Log file directory. The Default is the NX_ROOT\log directory.
-level	LogLevel	INFO, ERROR, DEBUG	(Optional) Level of detail to write to the log file. Default value is ERROR.
-s	DBHost	<server name>	(Required) Database server host name. To use a Microsoft SQL Server named instance, specify *server**instance* on the command line, or *server**instance* in the configuration file.
-CI	CI	<CI uuid>	(Optional) Compute ambiguity for the specified CI and all CIs that are ambiguous with it.
-full	(none)	0,1	(Optional) Command line only Optimizes the performance of the scan by only considering those CIs updated since the last time the utility was run. If set to 1, forces a full scan of all CIs in the computation of the ambiguity index. The default is 0. This parameter does not apply to the calculation of transaction ambiguity. The utility always evaluates all transactions in the TWA.
-port	DBPort	<port number>	(Required. Oracle only) Oracle port number
-SID	DBSID	<SID name>	(Required. Oracle only) Oracle SID name
-h	(none)		(Optional) Prints help usage message.
-schema	SchemaName	<db schema name>	(Optional) Default is mdbadmin for Oracle; or dbo for Microsoft SQL Server.

Resolve Ambiguous CIs

After you identify ambiguous CIs and determine if their identifying attributes are valid, resolve the ambiguity among the CIs in the ambiguity set. Use one or more of the following ways:

- **Modify the identifying attributes**
  If the identifying attributes are not complete or invalid, set the CI identifying attributes so that the CI is unique. Use either the Web interface, GRLoader, or CMDBf.

  Note: When the MDR updates the CI, the MDR can undo the manual reconciliation changes.

- **Exclude a CI from ambiguity management**
  If the CIs identifying characteristics are correct and represent a known, valid ambiguity, remove the CI from the ambiguity management lists and the ambiguity calculation of other CIs. You can mark the CI as not ambiguous (exclude ambiguity).

- **Reject a CI Update by inactivating the CI**
  When you determine that the identifying attributes of a CI are incorrect and that updates using those attributes cause data corruption, you can inactivate the CI and prevent further updates. The user or MDR generating the information receives an error and the entire transaction is rejected.

- **Supersede a CI**
  Sometimes the updates to the CMDB are beyond the control of the administrator. Invalid identifying data must be in the system with valid nonidentifying attribute data. The incoming transaction attribute data can be transparently redirected to a superseding CI.

  Note: The transparent redirection of attribute data from one CI to another can cause confusion. This is because transaction data may not be stored in the same CI as the transactions identifying attributes would lead you to believe. Use this method with discretion, when the previous methods cannot be used.

Exclude CIs from Ambiguity Management

Sometimes you recognize that although a particular CI receives an ambiguity index greater than zero, it must be left as is. Any CI with its Exclude Ambiguity check box selected is not considered part of the ambiguity index or ambiguity management features.

Exclude Ambiguity for a CI

You can update the exclude ambiguity option for a CI from the web interface.

Follow these steps:

1. Select the CI that you want to remove from ambiguity management from the Ambiguous CI List page.
   The Configuration Item Detail page appears.

2. Click Edit.
   The Update Configuration Item page appears.

3. Select the Exclude Ambiguity check box on the Reconciliation tab, and click Save.
   The CI is excluded from the ambiguity index calculation and other ambiguity management features.

Exclude Ambiguity Using GRLoader

You can update the exclude ambiguity option for a CI by using GRLoader to set the not_ambiguous flag.

not_ambiguous values are as follows:

- **YES (1)**
  Removes the CI from ambiguity management. The CI is identified as unique regardless of the identifying attributes of other CIs. The ambiguity index of the CI remains zero.

- **NO (0) (default)**
  This CI is eligible for ambiguity management. The uniqueness of the CIs identifying attributes determines the ambiguity index of this CI. The identifying attributes of this CI are considered when evaluating the ambiguity index of other CIs.

Note: For more information about GR Loader, see the *CMDB Technical Reference* (see page 4168).

Reject Updates

When a CI is marked as Inactive, no updates can be performed on it. Set the CI to Inactive if you want CA CMDB to reject data for a given CI and you want the MDR to know of the rejection.

In this way, you can reject problematic data immediately and can reflect it back to the source. The MDR can correct the rejected input at the source.

To set a CI to Inactive in the web interface, edit the CI, set it to Inactive, and click Save. You also can set a CI to Inactive by using GRLoader or CMDBf web services. Inactivated CIs can also be reactivated.

Supersede Ambiguous CIs

You can supersede an ambiguous CI to redirect data to a specific target CI. You can display superseded CIs, which are Inactive and all web interface updates to them are ignored.

Note: Updates that are sent to superseded CIs by GRLoader or CMDBf web services are redirected to the superseding CI. However, updates to identifying attributes are ignored.

Follow these steps:

1. Select the CI that you want to be the focal (superseding) CI from the Ambiguous CI List page.
   The Configuration Item Detail page appears.

2. Click Edit.
   The Update Configuration Item page appears.

3. Click the Reconciliation tab.
   All CIs that are ambiguous with the focal CI display.
   Determine which CIs you want to supersede by the focal CI. Inspect each CI in the list by clicking each CI to launch its Configuration Item Detail page.

4. Select one or more ambiguous CIs that you want to supersede with the focal CI and click Supersede.
   The focal CI supersedes the selected CIs.

MDR-Based Reconciliation

This article contains the following topics:

MDR-based reconciliation is performed at the management data repository. This helps reduce the occurrence of multiple CIs that refer to the same object in the physical world.

MDR-based reconciliation treats the MDR as a trusted source that always uses the same federated asset ID when it communicates information about a single CI. All updates from a given MDR to a given federated asset ID always update the same CI, even when identifying attributes are changed.

MDR-based reconciliation, reconciliation management, and the Transaction Work Area (TWA) described in these sections help you take control of the reconciliation process. However, to use reconciliation management and the TWA successfully, first understand how CA SDM uses reconciliation attributes.

Important: If you reinstall or reinitialize any external data provider, inactivate and reactivate its MDR definition in the CMDB. If the MDR reuses its federated asset IDs, inadvertent CI data overlay can occur.

How MDR Reconciliation Matches CIs

MDR-based reconciliation uses the following process to identify the appropriate matching CI:

1. If the transaction specifies an ID, the CI is identified and reconciliation is complete.

2. If the transaction does not specify an ID, CA SDM checks whether federated identification attributes are specified and match a CI. If there is a match, the transaction reconciles to the matching CI.

3. If the transaction does not specify an ID or federated identifying attributes, the CI transaction uses the identification attributes (see page 2566).

How MDR Reconciliation Identifies CIs

MDR-based reconciliation uses the following precedence to identify a CI:

1. ID (if a transaction specifies an ID, reconciliation is successful)
2. Federated identification attributes
   - Federated asset ID
   - MDR name
   - MDR class
3. CI identifying attributes
   - Tenant (if multi-tenancy is installed)
   - Name
   - Serial number
   - MAC address
   - System name
   - Alternate asset ID
   - DNS name

Review and Modify Inbound Data Using Transaction Work Area (TWA)

You can stage CI and relationship transactions before execution, by copying data into the TWA staging area. Once in the staging area, you can manipulate CIs and relationships by using the web interface or native SQL.

You also can validate the CI transactions to prevent the creation of new CIs when you update existing CIs. In this approach, you view each transaction and the potential CIs that it can update. This helps you reconcile the transaction manually to the target CI. Likewise, relationship transactions can be validated to reference the correct CIs.

For more information, see How to Identify and Resolve Ambiguous CIs (see page 2557).

CI Transaction Ambiguity Example

Transaction data from different data sources is loaded into CMDB. Each data source uses its own subset of identifying characteristics and may not fully identify the target CIs for the transactions. Because of this inconsistency, more CI Transactions may exist in CMDB than are valid.

Example: Ambiguous CI Transactions

The following CI transaction resides in the TWA:

- Name(Server1) DNS Name(dns1), Serial Number(serial1)

The following CIs reside in CMDB:

- Name(Server2) DNS Name(dns1)
- Name(Server3) DNS Name(dns1), Serial Number(serial1)
- Name(Server4) MAC Address(mac1), Serial Number(serial1)

Due to shared identifying characteristics, Server1 transaction is ambiguous with Server2, Server3, and Server4 in CMDB.

Every CI Transaction has an ambiguity index that is associated with it. The ambiguity index is approximately the number of existing CIs that match on any of the identifying attributes, minus one, specified in the CI transaction. The greater the index, the greater the number of other CIs that match on the transaction identifiers. Therefore the greater the probability that CI data was entered inconsistently and the possibility that more CIs are incorrectly created. CI Transactions with an ambiguity index of zero have identifying attributes that are unique across all CIs. Or, they have a target CI specified and are therefore unambiguous.

Example: Calculate the Ambiguity Index

The following CI transactions reside in the TWA:

- Name(Server1) DNS Name(dns1), Serial Number(serial1)
- Name(Server2) DNS Name(dns1), Serial Number(serial1)

The following CIs reside in CMDB:

- Name(Server1) DNS Name(dns1), Serial Number(serial1)
- Name(Server2) DNS Name(dns1), Serial Number(serial1), Mac Address(mac1)

The first transaction (Server1) ambiguity is 0 because there is an exact match with the Server1 CIs identifying attributes. The only possible target CI to this transaction is Server1 CI.

The second transaction (Server2) is ambiguous with Server1 CI and Server2 CI.

The ambiguity index for Server2 transaction consists of the following components:

- Number of matching CIs with Name (Server2) = 1
- Number of matching CIs with DNS Name(dns1) = 2
- Number of matching CIs with Serial Number (serial1) = 2

Based on shared CI identifying characteristics, the ambiguity index for server2 transaction is (1-1) + (2-1) + (2-1) = 2.

CI Properties that Support MDR Federation

This article contains the following topics:

Configuration item properties (attributes) identify assets for MDR federation purposes.

Federated Asset ID

People are known to different organizations by different identifiers. You may have the following identifiers:

- A unique nickname to your close friends
- Driver license (unique ID associated with you)
- A national service ID (for example, a selective service card)
- A health insurance number
- A national tax identification number

Each of these unique identifiers refers to you. However, the identifier is only valid when used to describe you to the appropriate repository.

Similarly, a CI can have multiple identifiers to associate it with its source MDRs. Each CI is known to an MDR by only a single identifier. We call this identifier the *federated asset ID*. The process of associating a CI with one or more MDRs is *mapping the CI*.

Mapping occurs when CIs are loaded into the MDB in one of two ways:

- Defining the CI mapping using the Administration user interface
- Loading CIs using the GRLoader utility

MDR Name and Class

The MDR name identifies the MDR to CMDB when exporting data using XML and GRLoader. The MDR typically has its own naming convention for how it identifies itself: a combination of host server name plus an identifying instance name or number. Because only one MDR exists on a particular host, the MDR name is often set to the host server name. **Required for CMDBf Viewer.**

Note: The MDR Name for CA Asset Portfolio Management release 11.3.4 is APM and the MDR Name for CA APM r12.6 is ITAM. Both products are supported. However, we recommend that you verify product availability at CA Support Online (http://support.ca.com/) before implementing the products

The customer defines the MDR class to group MDRs.

Note: An MDR Class of CMDBf is required for CMDBf viewing.

Important! The MDR Name plus the MDR Class must be unique within your enterprise.

MDR Definition with CA Configuration Automation Installation

CA Configuration Automation MDRs have the following requirements:

- The mdr_name specified in the MDR definition on the CMDB server must match exactly the value of the attribute com.cendura.installation.name in the cendura.properties file on the target CA Configuration Automation server.
- CA Configuration Automation MDRs must have an MDR class of Cohesion.
- The MDR must specify the hostname and port number of the CA Configuration Automation server.

To run MDR Launcher, edit the following portion of the cendura.properties file:

```
# -- Configure One-Click Authentication --
com.cendura.security.oneclickauth.secret=shared_secret
com.cendura.security.oneclickauth.scheme=
com.cendura.security.oneclickauth.user=userid
```

Important! The secret that is specified in the cendura.properties file must match the *shared secret* in the MDR definition.

The MDR Launcher logs in as the *userid* specified in the properties file and inherits its security attributes. To use functionality such as Refresh for CI attributes, verify that this user has sufficient privileges. For more information about creating a user, setting security options, and modifying the properties file, see the *CA Configuration Automation Implementation documentation.*

CA Configuration Automation MDRs

This article contains the following topics:

- MDR Definition Administration (see page 2572)
- CA Configuration Automation Report (see page 2573)

CA Configuration Automation MDRs must be defined before importing data from a CA Configuration Automation server. A CA Configuration Automation MDR must specify an MDR Class of Cohesion.

Example: Cohesion1 MDR Definition

In the following Cohesion1 MDR definition, the XML specifies an MDR Name of cohesion_server and an MDR Class of Cohesion. These values are required for the CIs to be imported.

- **Button Name**
  Cohesion1
- **MDR Name**
  cohesion_server
- **MDR Class**
  Cohesion
- **Active?**
  Active
- **Owner**
  CMDBAdmin
- **Description**
  CA Configuration Automation server in Chicago
- **Hostname**
  cohesion_server
- **Port**
  8090
- **Path**
  CAisd/html/cmdb_cohesion.html
- **Parameters**
  hostname={hostname}+port={port}+family={family}+name={name}+secret={password}
  +federated_asset_id={federated_asset_id}
- **userid**
  cohesion_userid
- **Shared Secret**
  Chicago01
- **URL to launch in Context**
  http://cmdb_hostname:8080/{path}?{parameters}

In addition, because this is a Cendura server, the values that are listed previously must match the values in the cendura.properties file on that server. See the following example:

```
com.cendura.security.oneclickauth.secret=Chicago01
com.cendura.installation.name=cohesion_server
```

You can modify the URL syntax to handle special requirements.

How to Associate an MDR to a CI Manually

You can associate MDRs with a CI manually. Use the Federated CI Mapping facility in the CMDB Administration tab, in the MDR Management branch of the tree.

Before you associate a CI to an MDR, complete the following tasks:

1. Create the MDR definition (if it does not exist).
2. Create the CI definition (if it does not exist).
3. Identify the unique Federated Asset ID of the CI that you want to connect to the MDR. This ID is MDR-specific, so it is beyond the scope of this document.

Note: To identify Federated Asset ID, consult your MDR documentation.

CA Cohesion Automatic Import

You can import CIs directly from CA Configuration Automation. Run a CA Configuration Automation report specifying the host name, port, user ID, and password to a CMDB server. If the MDR is defined in CMDB, CA Configuration Automation automatically generates the XML. The XML includes CIs and relationships, with the information necessary to perform the MDR Launch on a CI. The report automatically imports the CIs into CMDB. For more information about exporting CIs from CA Configuration Automation, see the online help from the Reports, Report Templates tab.

CI to MDR Mapping

Because each MDR uses a federated_asset_id to identify a CI, one CI can be related to multiple MDRs. A federated_asset_id does not have to be unique across MDRs, but a federated_asset_id must be unique within an MDR. Each MDR must have a unique MDR class and MDR name.

Important: Whenever a CI or an MDR provider is made Inactive, all Federated CI Mappings that are associated with the CI or the MDR provider are also made Inactive.

After you create an MDR Data Provider definition, complete the following tasks:

1. Create a CI in the CMDB that references an MDR.
2. Verify that the MDR definition works.
   Because you can only launch from within the context of a CI, it is not possible to test directly from the MDR definition, which has no CI context.

You can view the Federated CI Mapping List in the Administration tab, in the Federated CI Mapping node.

To view the CI in a particular MDR context, click an MDR Launch button.

The target MDR is launched in the context of the CI that was opened.

Example: CI Mapping

1. Click the Administration tab.

2. Navigate to MDR Management, Federated CI Mapping.
   The Federated CI Mapping List appears.

3. Enter server1 in the CI Name field.
   The following columns show the values:

   - **Federated Asset ID**
     1000234
     1000235

   - **CI Name**
     server1
     server1

   - **MDR Provider**
     Cohesion1
     Cohesion2

   - **Active**
     Active
     Active

   The Cohesion1 MDR Provider and the Cohesion2 MDR Provider know the existence of server1. The example shows that they each have independently assigned the server a unique ID.

4. Click the CI Name server1.
   The server1 Configuration Item Detail page appears that includes launch buttons would be named Cohesion1 and Cohesion2.

5. Click either MDR Provider launch button.
   More details about the CI appear.

MDR Definition Administration

Administering the MDR definitions is a flexible process. You can modify the parameters in an MDR definition even when CIs reference it. For example, you can modify the button name, host name, user ID, and shared secret, after the MDR is defined and the CIs are loaded.

CA Configuration Automation Report

CA Configuration Automation provides a facility for scheduling recurring reports. Use this facility to simplify the process of keeping the CMDB synchronized with the data in the CA Configuration Automation MDR. Common errors such as an invalid password (due to password change or expiration) can prevent successful importing of data. You can choose to receive notification of any errors that occur during background data execution of the data import. Enable the Notification option in the CMDB Export report in CA Configuration Automation. You will receive an email when an import error occurs. If you run the Cohesion report in the background as a scheduled task, we recommend that you enable the Notification option. For information about scheduling execution of the CMDB Export report regularly, see the *CA Configuration Automation Product Documentation*.

How to Deploy CMDBf Web Services

After you install CA SDM, you can deploy CMDBf web services.

Follow these steps:

1. Verify that the web server is up and running.
2. Navigate to the CMDBHOME\sdk\websvc\CMDBF directory.
3. Run deploy_cmdbws.bat.
   The CMDBf web services are deployed and started. For more information about CMDBf web services deployment, see the Web Services Deployment (see page 4362) topic.

Using GRLoader

When using GRLoader to load a CI, populate the following fields in the XML for the MDR Launch to operate:

- <mdr_class>
- <mdr_name>
- <federated_asset_id>

The values that you provide for <mdr_name> and <mdr_class> in the XML must match the values in the MDR definition exactly.

Important! The MDR name and class must be defined using the Administration interface before importing the CIs that reference the MDR. If the MDR specified in the XML is not defined, the CI is not imported.

The GRLoader supports importing CIs and CI relationships from spreadsheets in the XLS and XLSX formats. To load CI data into CA SDM, format the source data into XML or Microsoft Excel spreadsheets. For more information about using GRLoader to load spreadsheet data, see the How to Prepare for Loading Spreadsheet Data (see page 4323) topic.

system_name Naming Convention

We recommend the following naming standards for software CIs and all MDRs. These naming standards facilitate the integration of MDRs with CA Configuration Automation and other MDRs. The standards are also helpful for reconciling CIs properly. CA Configuration Automation follows the same standards.

- **System_name**
  Identifies software CIs uniquely. When you define a relationship that involves a software CI, specify the same system_name as the one in that CI definition. If multiple instances of the same version of a software are installed on the same hostname, modify the system_name. Modifying the system_name enforces uniqueness. The total length of the system_name must not exceed 255 characters. If you ignore this restriction, data corruption can occur.
  System_name must be a unique identifier for this instance of the software on a single host.

Use the following syntax:

```
hostname | softwarename | version | business-application
```

- **pipe (|) character**
  Separates the various fields in the concatenation of the syntax to let the user use the search facility.

- ***hostname***
  Specifies the hostname that contains the software.

- ***softwarename***
  Specifies a common name for the software.

- ***version***
  Specifies the version number of the software if available.

- ***business-application***
  Specifies a unique identifier for this instance of the software on *hostname.* If the instance is associated with a business application or service, the name of that service is the qualifier. When you cannot determine *business-application*, you can use the installation directory to identify the software. If the total length of this field exceeds 255 characters, use ellipses (…) to shorten the total length of this field.

Examples: Use the UI Search Facility

You can use the UI search facility to search software CIs, as in the following examples:

Use case	Name	System_name
Find all software CIs on host	xxx	Xxx%

Use case	Name	System_name
Find all instances of software	yyy	yyy%
Find all instances of software	yyy version 123.0	yyy% %|%|123.0%

In the results list that the search returns, the user sees only the Name field.

```
mac_address     Null.  - Inappropriate for software
asset_num       Null   - Inappropriate for software
serial_number   Null   - Inappropriate for software
dns_name        Null   - Inappropriate for software
```

How to Update Metadata Files for CMDBf Mapping

This article contains the following topics:

Use CA CMDB metadata files to translate between MDR attribute names and CMDB attribute names. Using CMDB metadata files improves readability of attribute comparisons. For any MDR attribute without CMDB mapping, the Federated View displays the attribute name. The attribute name is sent by the MDR. Metadata can be defined for CMDBf data providers to do the following tasks:

- Display MDR attribute values using CMDB attribute names.
- Prevent MDR provider attributes from being displayed in Federated View.
- Define MDR provider attributes that do not have CMDB equivalents.

You define metadata using the cmdb_metadata_federation_viewer_site_attr.htmpl file. This file contains instructions on how to update the file. Metadata can apply to all CMDB families (common attributes) or family-specific attributes.

To map external MDR attribute names to CMDB labels, you update the respective cmdb_metadata_*extensiontable*.htmpl form. Use the following fields in the cmdbmetadata macro:

- mdr_attr - the name of the MDR attribute to be translated.
- mdr_name - the name of the MDR being translated. Regular expressions are supported.

Example: Attribute mapping

The code in this example defines metadata that equates the CMDB "phys_mem" attribute with the provider attribute "mdr_memory" for all providers named "myMdr" or starting with "MDR". In addition, "physical_memory" is equated to with "phys_mem" for all other providers.

```
<macro name=cmdbMetadata attr="phys_mem"  provider_attr="mdr_memory" provider_name="
myMdr">
<macro name=cmdbMetadata attr="phys_mem"  provider_attr="mdr_memory"
provider_name_regexp="MDR.*">
```

```
<macro name=cmdbMetadata attr="phys_mem" provider_attr="physical_memory"
provider_name_regexp=".*">
```

Example: Attribute hiding

The following statement hides the MDR provider "widget_cost" attribute for all providers named "myMdr".

<macro name=cmdbMetadata hide_provider_attr="YES" provider_attr="widget_cost" provider_name="myMdr">

Example: Setting an attribute label

The following statement defines an attribute name “ext_mem_capacity” using the label “External Memory Capacity” under the attributes category in the CMDBf Viewer.

```
<macro name=cmdbMetadata  attr="ext_mem_capacity" category="Attributes" heading="
External Memory Capacity" help="Total external memory">
```

How To Display MDR Attribute Values With CA CMDB Attribute Names

Metadata can create an association between MDR provider attributes and CMDB attributes. The association helps to display the attributes together to see differences and share labels. By default, MDR attributes that do not have a mapping are displayed as **Not in CMDB** in the viewer. cmdbMetadata macro arguments to equate a CMDB attribute with an MDR provider attribute include:

- attr - CMDB attribute name
- provider_attr - MDR provider attribute name
- provider_name - MDR provider name
- provider_name_regexp - MDR provider name regular expression

provider_name or provider_name_regexp are required.

Example: Associate MDR Attributes with CMDB Attribute Names

The following three metadata statements do these respective actions:

- Equate the CMDB "phys_mem" attribute with the provider attribute "mdr_memory" for all providers named "myMdr".
- Equate the CMDB "phys_mem" attribute with the provider attribute "mdr_memory" for all provider names starting with "MDR".
- Equate "physical_memory" with "phys_mem" for all other providers.

```
<macro name=cmdbMetadata attr="phys_mem"  provider_attr="mdr_memory" provider_name="
myMdr">
<macro name=cmdbMetadata attr="phys_mem"  provider_attr="mdr_memory"
provider_name_regexp="MDR.*">
```

```
<macro name=cmdbMetadata attr="phys_mem"  provider_attr="physical_memory"
provider_name_regexp=".*">
```

Hide MDR Provider Attributes

Some MDR provider attributes do not need to appear in the Federated View. You can hide metadata for a particular MDR provider. This option only applies for MDR provider attributes and does not apply for CMDB attributes.

cmdbMetadata macro arguments to hide a provider attribute include:

- hide_provider_attr - "YES" - hides the MDR provider attribute
- provider_attr - MDR provider attribute name
- provider_name - MDR provider name
- provider_name_regexp - MDR provider name regular expression

provider_name or provider_name_regexp are required.

Example: Hide an MDR-Only Attribute

To hide the MDR provider *widget_cost* attribute for all providers that are named *myMdr,* use the following metadata statement:

```
<macro name=cmdbMetadata  hide_provider_attr="YES" provider_attr="widget_cost"
provider_name="myMdr">
```

Define MDR Attributes Without CA CMDB Equivalents

You can define labels and help text for MDR provider attributes that do not correspond with any CMDB attributes. Attributes are labeled Not in Family in the Federated View.

cmdbMetadata macro arguments to define an MDR provider attribute include:

- attr - CMDB attribute name
- category - Category name where attribute is displayed
- heading - Heading label for attribute
- help - Brief description of the attribute

Example: Define an MDR-Only Attribute

The following statement defines an attribute name "ext_mem_capacity" using the label "External Memory Capacity" under the Attributes category in the Federated View .

```
<macro name=cmdbMetadata  attr="ext_mem_capacity" category="Attributes" heading="
External Memory Capacity" help="Total external memory">
```

Define CMDBf Data Provider Metadata

You can control how data is displayed in the Federated View.

To define metadata for CMDBf Viewer

1. To open the cmdb_metadata_federation_viewer_site_attr.htmpl file, use Web Screen Painter.
2. Determine which metadata changes are needed.

   Note: Sample templates are provided in the file.

3. Copy the appropriate template and substitute the required arguments according to the instructions in the file.
4. Save and publish the changes.

CMDB Management

Contents

Depending on your role, CMDB lets you manage configuration items and their relationships:

- The Configuration Administrator (CMDB Administrator) manages the tools in your CMDB, such as change verification. In addition to CI management, Configuration Administrator role includes administration of CI classes, CI families, and relationship types.
- The Configuration Manager plans and audits the type of information to store in the CMDB.
- The Configuration Analyst enters data into the CMDB by using approved methods and checks the accuracy of the data.
- The Change Manager helps ensure that users complete the following tasks:
  - Document the requests for change correctly.
  - Review the requests for change.
  - Execute the changes according to environment rules. The environment rules include priority, completeness, compliance, and signoffs.

Note: The Change Manager is not responsible for the CMDB, but servers as a major customer of the CMDB.

Create a CI from a Base Object

A CA CMDB installation can define CIs for *base objects*: Contacts, Locations, and Organizations. These CIs can be managed so, and they can establish relationships with other CIs as desired. For some customers, this approach supports the configuration management process better than employing base objects only as CI attributes.

Note: You cannot select a contact that is already represented by another CI in the Contact family.

The Scoreboard lets you create a configuration item from a base object.

Follow these steps:

1. Click File, New Configuration Item.
   The Create New Configuration Item page appears.

2. Complete the CI fields. Name and Class are required. Click Continue.

   Note: The common CI attributes Host Name, Serial Number, MAC Address, and DNS Name are not relevant to a CI for a base object.

   The Create New Configuration Item page appears.

3. Click the base object link to define the object that this CI represents.

4. Select the object. You can search for an existing object or click Create New to create an object. If you want to create an object, click Save to continue.
   The selected object appears at the top of the Configuration Item Detail page.

5. Click Save.
   The main attributes of the selected object appear on the Attributes tab of the Configuration Item Detail page.

Create a Base Object CI Using GRLoader

You can use GRLoader to create a base object CI from an existing base object.

Follow these steps:

1. Write XML that identifies the following parameters:

- CI name
- Family
- Class

2. Submit the XML.
   The base object is created and the GRLoader displays that one CI was read and inserted.

Example: Create a CI From an Existing Contact

The following example creates a CI from the existing contact **Gibbs, Keith**.

```
<GRLoader>
<ci>
    <name>Gibbs, Keith</name>
    <family>Contact</family>
    <class>Technical</class>
    <base_contact>Gibbs, Keith</base_contact>
</ci>
</GRLoader>
```

How to View a Federated CI

The Federated View page displays parallel CI attribute values from CMDB and CMDBf-registered MDRs. If no external MDRs are configured for CMDBf, only the CMDB attributes are displayed.

To update the fields from an MDR, click Retrieve.

Legend:

bold - Attribute value differences between CMDB and MDRs.

Not in Family - MDR-only attribute customized to display in a CMDB category.

Not in CMDB - Category for MDR-only attributes.

Note: To customize the way MDR attributes are displayed, see MDR documentation.

Note: To display federated CI attributes, the MDR class must be **cmdbf**.

Populating CMDB

This article contains the following topics:

Database Population

Populating the CMDB with the CIs and relationships in your IT infrastructure is a part of using the application efficiently. You can populate the CMDB with data manually by:

- Using the built-in Configuration Item Editor
- Using GRLoader
- Importing items from other asset management tools.

How GRLoader Populates the Database

T populate the database by loading CIs and relationships, complete the following tasks:

1. Convert input data containing information about CIs and their relationships to XML or in a spreadsheet.
2. The CA CMDB GRLoader program uses the XML data as input.
3. GRLoader loads the data into the database.For information about GRLoader parameters, see the GRLoader Command (see page 4289) topic.

Use GRLoader to Import the Data

Import data by using the GRLoader program that is provided with CA SDM. The program creates CIs based on the data in an XML file or a Microsoft Excel spreadsheet.

Follow these steps:

1. From the Start menu, select Run.
2. Enter **cmd**.
   A DOS command window appears.
   Enter the following command:

   ```
   Grloader -u <username> -p <password> -s http://<ca_sdm_servername>:8080
   -i <xml_document or spreadsheet>
   ```

   GRLoader creates CIs using the data in the XML file. If errors are found during this process, an error file is created. The error file lists the CIs that could not be imported and the reason. GRLoader import completes.
3. Start CA SDM and verify that the CI data has been correctly populated.
4. To verify that relationship data has been populated correctly, start the CMDB Visualizer.
   The data is imported and verified. For more information about GRLoader, see the General Resource Loader (see page 4289) topic.

Family and Class Assignments

Apply a classification scheme to each CI; this scheme involves assigning each CI the following attributes:

- Family -- A collection of configuration items having similar attributes
- Class -- A subset of configuration items within a family

You can create assignments in the following ways:

- Populate manufacturer data identifying family and class for each hardware asset.
- Include nonblank values for family and class in the respective columns in the input file.

GRLoader does not import an CI that cannot resolve family and class to an existing family and class.

How to Load CA APM Data

The primary input to the CA APM Loader program is a table or view that contains an extract of the CA APM import data. This data is contained in the CMDB_Export_Asset_Data database table or view. In some cases, the import data into the MDB is located in the same database as the target. However, in many circumstances, the import data resides in a different database, for example, when importing data across subsidiaries. In either case, create a view on the same database as the source data.

The CA APM data view does not contain the class and family attributes, and can come from a system with a different classification scheme. For example, if the source of the asset data is a different company, a different classification system can be in effect.

The CA_MODEL_DEF table contains a list of models, which are matched against the data in CMDB_Export_Asset_Data. If there is a match, the family and class from the model are assigned to the asset being imported. If there is no match, define a new model for the asset. Consider either copying entries from the source CA_MODEL_DEF table to the target MDB, or updating the CA_MODEL_DEF table with entries for all new hardware makes and model numbers.

CMDB Visualizer Overview

CA SDM lets you align your IT components (*configuration items*, or CIs) with your business services. CMDB defines *relationships* among CIs, as when a group of CIs work to provide a business service. CMDB Visualizer lets you see the entire picture of your CI relationships, and provides functions to manage the relationships. Working from a *focus CI*, you can use the Visualizer to display up to nine levels of related CIs.

(If you are using Advanced Availability configuration) If the visualizer makes a server request during the application server quiesce period, the following message is displayed:

You can hide the message box but the message is displayed on the top panel throughout the quiescing period. If the server quiescing is canceled, you receive a message about the cancellation.

```
This CMDB Visualizer server is scheduled to shut down for maintenance in xx:xx.
Please save your work and logout.
```

CA uses a provider/dependent model to define relationships among CIs. All CIs that contribute to a business service are *providers* to that business service (the *dependent*). In much the same way, providers can also be *dependents* that rely on other CIs. You can use Visualizer to perform the following provider/dependent analyses:

- **Browse**
  Displays unfiltered view of all CIs.
- **Impact Analysis**
  Starts with a focal CI (provider) and searches for its dependents.
- **Root Cause**
  Starts with a business service (dependent) and view all the CIs that are providers to that service.
- **Cause and Effect CIs**
  Combines impact analysis and root cause in one search.
- **Trace Relation**
  Displays all possible relationships that are based on levels. If you select only one CI, this filter displays the Browse view.
- **Shortest Path**
  Displays the shortest chain of relationships that are based on levels.

CMDB Visualizer lets you do the following actions:

- Visualize multiple levels of CIs from a configurable graphical view
- Monitor or cancel rendering progress
- Search using flexible criteria
- Filter based on CI families, relationship types, and other attributes
- Display CI relationships
- Trace a relationship between two CIs
- Visualize a dependency chain
- Invoke CMDB directly from Visualizer
- Display CI attributes and properties
- Save graph metadata
- Print the graph layout
- Find a specific CI on a displayed graph
- Create a CI (depending on role)

- Create new CI relationships (depending on role)
- Use the Scratchpad to store key CIs
- Display CI status
- Hide or reveal a CI in the Visualizer layout
- Role-based data security
- Launch external MDRs
- Obtain online help for Visualizer features

How To Use the Visualizer Interface

This article contains the following topics:

CA CMDB Visualizer provides a graphical interface with toolbars and a graphical canvas. You can click the button on the left side of the canvas to display the retractable Search pane.

Graphical Display Tasks

With the Visualizer graphical display, you can display the CIs and relationships that you select for analysis. You can also do the following tasks:

Note: Visualizer uses the space bar to select or confirm an operation. For example, if the focus is on a button, then instead of pressing Enter, press the space bar.

- Create, manage, and apply analysis filters.
- Change the graph layout and number of CI levels displayed.
- Select CIs for graphical viewing and right-click to provide various functions, including the ability to view and modify CI properties.
- Use the Toolbar icons to provide various functions.
- Zoom in to view areas of interest, or zoom out to see the larger context.

- Use Full Screen Mode display a larger work area.

> **Note:** When you enable Full Screen mode, you cannot use the keyboard functionality.

Search for CIs by Attributes

You can search for CI (and asset) attributes to locate and manage CIs.

> **Note:** If you only search for CIs, you can disable the Asset search. To disable the Asset search, clear the CA APM check box on the Visualizer administrative interface.

Follow these steps:

1. Open the retractable Search pane on the left side of the Visualizer graph.
2. Click the Search tab.
3. Expand the sets of search criteria that you want.
4. Complete one or more of the attribute fields on the search criteria areas.
   The search criteria is specified.

   > **Note:** Visualizer searches for both CIs and Assets by default. To restrict the search, change the CI or Asset general options.

5. Click Search.
   The Search Results tab displays all CIs/Assets that match your search criteria.

Primary

Primary fields focus your search that is based on the following basic CI attributes:

- CI Family
- CI Class
- CI Status
- Location
- Organization
- Department

- Asset
- CI

Network

Network fields search on the following common CI attributes for network addressing:

- IP Address
- DNS Name
- Host Name
- MAC Address

Asset

Asset fields search on the following basic CI/asset attributes:

- Manufacturer
- Model
- Serial Number
- Cost Center
- License
- Product Version

Maintenance

Maintenance fields provide searching on CI attributes for the following maintenance tasks:

- Service type
- Responsible Vendor
- Responsible Organization
- Maintenance Vendor
- Maintenance Organization
- Acquire Date
- Installation Date
- Expiration Date
- Warranty Start Date
- Warranty End Date

Filters and Layouts in Visualizer

This article contains the following topics:

Create a Filter

CA CMDB Visualizer provides built-in analysis filters, and you can create filters for your business needs.

Follow these steps:

1. Click the New Filter button.
   The Filter Wizard launches.

2. Name the filter and select one of the following filter types:

   - **Browse**
     Displays the unfiltered display of all related CIs.

   - **Impact Analysis**
     With the focal CI as provider, shows the CIs that are affected when any change occurs to the focal CI.

   - **Root Cause**
     With the focal CI as dependent, shows the CIs that could be the root cause for the focal CI to go down or can affect the focal CI's behavior.

   - **Cause and Effect CIs**
     Combination of Root Cause and Impact Analysis. From the focal CI, shows all the CIs that could be the root cause. Or shows the CIs that could be affected when a change occurs to the focal CI.

   - **Trace Relation**
     Displays all possible relationships among focal CIs, based on the Levels setting. If the graph has only one focal CI, applying this filter displays only the focal CI.

   - **Shortest Path**
     Displays the shortest chain of relationships among focal CIs, based on the Levels setting. If the graph has only one focal CI, applying this filter displays only the focal CI.

> **Note:** In addition to the predefined filters, any available administrator-defined and user-defined filters display.

3. Click Save & Finish.
   The filter is created.

Visualizer Filters

CA CMDB Visualizer provides built-in analysis filters, and you also can create filters.

Built-in filters include the following filters:

- **Browse**
  Displays the default unfiltered display.
- **Impact Analysis**
  With the focal CI as provider, shows all the CIs affected when any change occurs to the focal CI.
- **Root Cause**
  With the focal CI as dependent, shows all the CIs that could be the root cause for the focal CI to go down. Or, shows the CIs that can affect the focal CIs behavior.
- **Cause and Effect CIs**
  Combination of Root Cause and Impact Analysis. From the focal CI, shows all the CIs that could be the root cause. Or, shows the CIs that could be affected when a change occurs to the focal CI.
- **Trace Relation**
  Displays all possible relationships among focal CIs, based on the Levels setting. If the graph has only one focal CI, applying this filter displays only the focal CI.
- **Shortest Path**
  Displays the shortest chain of relationships among focal CIs, based on the Levels setting. If the graph has only one focal CI, applying this filter displays only the focal CI.

In addition to the built-in filters, any available administrator-defined and user-defined filters display.

Layout

The Layout drop-down list lets you switch your CI display between two different layout options, depending on your analysis needs. The following types of layouts are available:

- Hierarchical
- Circular

Hierarchical Layout

Use a hierarchical layout when you want to view related CIs that can be logically distant from the focal CI.

Circular Layout

You use a circular layout when you want to emphasize all relationships closest to a focal CI.

Change Levels

You can change the number of levels of CIs that are displayed relative to the focal CI. The maximum number of levels that are allowed is nine. The default value is two levels, which you can modify by using the Administration interface.

Follow these steps:

1. Click the Levels drop-down list.
   The numbered levels appear.

2. Select the number of levels that you want.
   The graph adjusts to reflect the new setting.

Working with CIs in Visualizer

This article contains the following topics:

Create CI

Use the Create CI button to launch CMDB to provide CI definition capability directly from Visualizer.

Note: This function is available to roles that have MODIFY permission for Configuration Items and VIEW permission or higher for Relationships.

Follow these steps:

1. Click Create New CI on the Visualizer toolbar.
   The CMDB Create New Configuration Item page launches in context.

2. Define the new CI and click Save.

The CI is created.

View CI Properties

The Properties button provides a CMDB launch in context capability to view and edit selected CI details. Other methods include the following options:

- Select CI on Search Results, right-click, and select Properties.

- Select CI on the graph, right-click, and select Properties.

Create Relation

Use the Create Relation button to launch CMDB to provide relationship definition capability directly from Visualizer.

Note: This function is available to roles that have MODIFY permission for Relationships and VIEW permission or higher for Configuration Items.

Follow these steps:

1. From the graph, select up to two CIs.
2. On the Visualizer graph, click Create Relation.
   The Create New Configuration Item Relationship page launches in context. If two CIs are selected, one is shown as Provider and the other one as Dependent.
3. Select the relationship type from the drop-down list.

   Note: Specify the Relationship Type to save the graph with the new relationship.
4. Click Save.
   The new relationship is saved and the Create Relationship page closes.

Set a Focal CI

You can set a focal CI to display relationships from its point of view.

Follow these steps:

1. Select a CI to serve as the focus of the analysis from Search or graph.
2. Make the focal CI in one of the following ways:
   - Select CI on Search Results and hit Enter.
   - Select CI on Search Results and click its Make Focal CI icon.
   - Select CI on Search Results, right-click, and select Make Focal CI.
   - Select CI on the graph, and click Make Focal CI on the toolbar.
   - Select CI on the graph, right-click, and select Make Focal CI.

   The graph is reorganized around the focal CI.

Scratchpad

You use the Visualizer Scratchpad like the Favorites or Bookmark feature of internet browsers. You can store some CIs in the Scratchpad for convenient use later. You can select one or more CIs from the Scratchpad to add them to the Visualizer graph. You also can use the Scratchpad to make a CI the focal CI.

Note: The Scratchpad is saved locally. If you launch the Visualizer from a different server later, a saved Scratchpad is not available.

The Scratchpad provides two different CI views: Tiles and Details.

Note: If you change a CI name or family in CMDB, refresh the Scratchpad to view the changes.

Hidden CI(s)

Use the Hidden CI(s) button to display the CIs that were hidden by using the Hide/Unhide commands. On the Hidden CI(s) list, you can select one or more CIs and can redisplay them. Perform one of the following actions:

Follow these steps:

- Click Unhide.
- Drag and drop the CIs on the graph canvas.
- Using the CI right-click menu to select Unhide.

Hidden CIs can display either the Tiles or Details view.

Show Configured Status

You use the Show Configured Status button to switch the CI status display. The status bar displays the current setting.

When Show Configured Status is on, each CI displays an icon on the graph to indicate its configured status. To define icons for each Configured Status, use the CI Status page in the Administrator interface.

Working with Graphs in Visualizer

This article contains the following topics:

Open Graph

Follow these steps:

1. Click Open Graph on the toolbar.
   The Open Graph list displays graphs with saved metadata.

2. From the list, complete one of the following actions:

   - Double-click a graph item.

   - Select a graph and click Open.

   The graph is rebuilt based on its saved metadata and its current CMDB data.

Follow these steps:

1. Click Open Graph on the toolbar.
   The Open Graph list displays graphs with saved metadata.

2. Select the graph from the Open Graph list.

3. Click Delete.
   The graph is deleted.

Invert Graph

By default, Visualizer displays Provider CIs at the top and Dependent CIs at the bottom, relative to the Focal CI.

Follow these steps:

1. Click the Invert Graph button to reverse this arrangement to a vertical axis.
   You can view the data from a different perspective.

Find CIs on the Graph

You can find specific CIs to display as nodes on the graphical display. Use the Find CIs button to open a new window over the graph to prompt for what string to match. The Find string is matched using graphical node attributes such as the CI name and family. Find shows the count of CIs which matched the users input criteria. The count is displayed in the bottom left corner.

Follow these steps:

1. Select the nodes to use from the Find CI results.

2. Click Select On Graph.
   The selected CIs display.

Show Graph for a Single CI

Follow these steps:

1. On the Visualizer graph, select a CI to serve as the focus of the analysis.
2. Right-click the CIs menu and select Make Focal CI.
   The selected CI becomes the *Focal CI* in the Visualizer. Its associated relations display, including the configured number of levels.

Add Multiple CIs to Graph

Follow these steps:

Make Focal CI, Add to Graph, or drag-and-drop CIs from the following sources:

- Search Results
- Scratchpad
- Saved graphs
- Hidden CI list

Note: The maximum number of CIs is ten (10).

Visualizer Procedures

This article contains the following topics:

The topic describes the Visualizer features that are available when the CA SDM server with Visualizer is running.

Note: (For Advanced availability configuration only) If the visualizer makes a server request during the application server quiesce period, the following message is displayed:

“This CMDB Visualizer server is scheduled to shut down for maintenance in xx:xx. Please save your work and logout.”.

You can hide the message box but the message is displayed on the top panel throughout the quiescing period. If the server quiescing is canceled, you receive a message about the cancellation.

Launch Visualizer in CI Context

Follow these steps:

1. In the CA SDM web interface, navigate to a CI List, or Search for the CIs to analyze.
   The CI List displays.

2. Click a CI of interest.
   The CI Detail page is displayed and the Visualizer button is available. If CA CMDB Visualizer was not installed, the Visualizer button is inactive.

3. Click Visualizer.
   Visualizer starts and the relationships for the focal CI display.

   Default: Cause and Effect CIs

Launch Visualizer with Applied Filter

Follow these steps:

1. Navigate to the CI List, or search for the CIs you want to analyze.
   The CI List displays.

2. Click a CI of interest.
   The Configuration Item Detail page displays.

3. On the Filters list, select a filter.

4. Click Visualizer.
   Visualizer starts and the graphical relationships for the focal CI display according to the selected filter. If CA CMDB Visualizer was not installed, the Visualizer button is inactive.

Trace Relation with Focal CIs

You can trace all relationships between the selected CI and any focal CIs on the graph.

Follow these steps:

1. Select a CI on the graph.

2. Right-click and select Trace Relations with Focal CIs.
   Any relationships are displayed.

> **Note:** If the selected CI is also the only focal CI, only that CI is displayed.

Launch MDRs

Follow these steps:

1. Right-click a CI on the Visualizer graphical display.
   A pop-up menu displays.

2. Select the Launch MDR option on the pop-up menu.
   All external data providers that are associated with the CI appear.

3. Select an application name and click Launch to start the associated application.
   Visualizer launches the external MDR application as it is defined in the CMDB.

> **Note:** Visualizer does not validate the external MDR applications credentials and URLs.

Hide/Display CIs

To promote clearer viewing, you can hide and then redisplay graphed CIs. Hidden CIs are available only for the current graph. When a new graph is generated, or when a Focal CI is set, the Hidden CIs List is cleared.

Follow these steps:

1. To select a CI, click it.

2. Right-click the CI and select Hide from the drop-down list.
   The graph updates so that the CI is hidden.

Follow these steps:

1. Click Hidden CIs on the toolbar or status bar.
   The Hidden CIs list displays.

2. Select one or more hidden CIs from the list and perform one of the following actions:

   - Click Unhide.
   - Drag to the graph canvas.
   - Right-click and select Unhide.

   The graph updates so that the CIs display.

View Change History for a CI

Follow these steps:

1. Select the CI you want to view.

2. Click Properties.
   CA CMDB is launched in context, displaying the CI Detail page.

3. Select the Versioning tab and click Show Log.
   The tab displays the details of the changes that were made to the CI.

Apply a Filter

Follow these steps:

1. Build the desired graphical display.

2. Click the Filter drop-down list.
   The Filter list is displayed.

3. Select a filter from the list.
   The filter is applied to the graph, which reorients to display the new perspective.

Use the Scratchpad

To view the Scratchpad, click the Scratchpad button on the Visualizer toolbar.

The Scratchpad displays.

Follow these steps:

1. Select one or more CIs on the Scratchpad.

2. Complete one of the following actions:

   - Click the Make Focal CI button on the Scratchpad toolbar.

   - Drag and drop one or more CIs from the Scratchpad to the graph.

   - Right-click on a CI and select Make Focal CI.

Follow these steps:

1. Select one or more CIs on the Scratchpad.

2. Complete one of the following actions:

   - Click the Add Focal CI button on the Scratchpad toolbar.

   - Right-click on the CI and select Add To Graph.

Follow these steps:

1. Select one or more CIs to delete.

2. Click the Delete button on the Scratchpad toolbar.
   The CI is deleted from Scratchpad.

To synchronize the Scratchpad to the Database, click Refresh. The Scratchpad removes all the CIs that were deleted from the database.

To save a CI on the Scratchpad, right-click the CI and select Add to Scratchpad.

The CI is added to the Scratchpad.

Visualizer Administration

Use the CMDB Visualizer administration interface to perform the following functions:

- Install and configure the Visualizer server.
- Modify the display of CI status and relationships.
- Create and manage administrative filters.
- Create and manage Visualizer CI graphics.
  You can use the Icon Configuration page to map family names to their respective icon images when you upgrade from CMDB Visualizer r11. To reset the family icon mapping, click Reconfigure. The icon image mapping file (\CMDBVisualizer\WEB-INF\classes\com\ca\cmdbvisualizer\config\clientsvgfamilyimagemap.properties) is recreated.

Note: These functions are only available to roles with administrator privileges.

How to Configure CMDB Visualizer

You can configure a CMDB Visualizer server as a primary or secondary server. The primary Visualizer server must reside on the same computer as the primary CA SDM server. All other Visualizer servers are treated as secondary servers. You cannot change a secondary Visualizer server to primary unless a CA SDM server on the same computer is changed to primary. The primary server address is required to reconfigure a secondary server.

You change some of the configuration values that were entered for the CMDB Visualizer during its initial configuration. To change some settings, you edit the properties files. If the CA SDM server has changed, you also most update the server name.

Visualizer configuration information is stored in the following file:

```
../CMDBVisualizer/WEB-INF/classes/com/ca/cmdbvisualizer/config/cmdbvisualizerconfig.properties
```

The following properties in the property file must be changed:

- USD_WEBSERVICE_URL

- PARENT_APPLICATION

To update entries for the web service URL and the Parent application URL, modify the following parameters:

```
USD_WEBSERVICE_URL=http://<cmdb-server-name>:<port no>/axis/services
/USD_R11_WebService>
PARENT_APPLICATION=http://<cmdb-server-name>:<port no>/CAisd/pdmweb.exe
```

This process must be repeated across all Visualizer installations.

You can update the timeout for SQL Queries in the SQL_QUERY_TIMEOUT property. For example, set SQL_QUERY_TIMEOUT = 30 sets the timeout as 30 seconds.

Managing CI Family Icons

CA CMDB Visualizer can represent CI families by using either SVG or JPEG graphics icons. By default, CA SDM provides SVG icons for CA-supplied CI families at installation. You can use either SVG or JPEG images for user-defined CI families.

You manage SVG and JPEG graphics using properties files in the following directory:

```
visualizer-install-dir\CMDBVisualizer\WEB-INF\classes\com\ca\cmdbvisualizer\config\
```

SVG graphics are defined as *key*=*value* pairs in the clientsvgfamilyimagemap.properties file.

- ***key***
  Specifies the family ID.

- ***value***
  Specifies the file name of the SVG graphic.

Example

400007=HARDWARE_MAINFRAME

> **Note:** SVG images cannot be previewed; they can only be viewed in the application.

You maintain JPEG graphics as *key*=*value* pairs in the serverjpegfamilyimagemap.properties file.

- ***key***
  Specifies the family ID.

- ***value***
  Specifies the file name of the JPEG graphic.

Example

400039=conx_32.jpg

Note: JPEG images reside in the following directory:

```
visualizer-install-dir\CMDBVisualizer\resource\
```

Important: When you create and maintain graphics in the .properties files, verify that no duplicate Family ID (key) occurs.

Visualizer displays an SVG or JPEG graphic for a CI Family that is based on the following priority:

- Family ID in the SVG.properties file
- Family ID in the JPEG.properties file
- JPEG image with key DEFAULT in the JPEG image map file

Example

DEFAULT=default_32.jpg

Built-In SVG Graphics

CA SDM supplies SVG graphics for the following families:

- CLUSTER
- CLUSTER_RESOURCE
- CLUSTER_RESOURCE_GROUP
- COMPUTER
- CONTACT
- DOCUMENT
- FACILITIES_AIR_CONDITIONING
- FACILITIES_FIRE_CONTROL
- FACILITIES_OTHER
- FACILITIES_UNINTERRUPTIBLE_POWER_SUPPLY
- HARDWARE
- HARDWARE_LOGICAL_PARTITION
- HARDWARE_MAINFRAME
- HARDWARE_MONITOR

- HARDWARE_OTHER
- HARDWARE_PRINTER
- HARDWARE_SERVER
- HARDWARE_STORAGE
- HARDWARE_VIRTUAL_MACHINE
- HARDWARE_WORKSTATION
- INVESTMENT_IDEA
- INVESTMENT_OTHER
- INVESTMENT_PROGRAM
- INVESTMENT_PROJECT
- LOCATION
- NETWORK_BRIDGE
- NETWORK_CONTROLLER
- NETWORK_HUB
- NETWORK_NETWORK_INTERFACE_CARD
- NETWORK_OTHER
- NETWORK_PORT
- NETWORK_ROUTER
- NETWORK_SWITCH
- ORGANIZATION
- OTHER
- PROJECT
- PROJECTS
- SAN_INTERFACE
- SAN_SWITCH
- SECURITY
- SERVICE

- SERVICE_LEVEL_AGREEMENT
- SOFTWARE
- SOFTWARE_APPLICATION
- SOFTWARE_BESPOKE
- SOFTWARE_COTS
- SOFTWARE_DATABASE
- SOFTWARE_IN_HOUSE
- SOFTWARE_OPERATING_SYSTEM
- TELECOM_CIRCUIT
- TELECOM_OTHER
- TELECOM_RADIO
- TELECOM_VOICE
- TELECOM_WIRELESS

How to Change the Icon of CI on the Visualizer

You can change the icon of a CI on the Visualizer. Complete the following:

Follow these steps:

1. Navigate to *$NX_ROOT\bopcfg\www\CATALINA_BASE_VIZ\webapps\CMDBVisualizer\WEB-INF\classes\com\ca\cmdbvisualizer\config* location.
2. Open the **clientsvgfamilyimagemap.properties** file and comment out the line (with a #) that corresponds to the family you would like to change the icon.
3. Navigate to *$NX_ROOT\bopcfg\www\CATALINA_BASE_VIZ\webapps\CMDBVisualizer\WEB-INF\classes\com\ca\cmdbvisualizer\config*.
4. Open the **serverjpegfamilyimagemap.properties** file and add the family class and image name (300002=new_hardware_server.jpg).
5. Create a resource subdirectory in *$NX_ROOT\bopcfg\www\CATALINA_BASE_VIZ\webapps\CMDBVisualizer* and place the image file mentioned in step 4 in the subdirectory.
6. Restart the CA Service Desk Manager service.
   You have successfully changed the icon of a CI on the Visualizer.

CMDB Data Maintenance

This article contains the following topics:

The tasks that you perform to maintain CMDB data require administrator privileges. The tasks include setting up the families, classes, and relationship types that are used to manage configuration items and relationship information.

CMDB Family/Class Structure

CMDB provides default configuration item families and the CI classes they contain.

The following Service Desk and CA APM base families do not have their own CA CMDB extension tables:

- Computer
- Contact (as base object)
- Hardware
- Location (as base object)
- Organization (as base object)
- Other
- Project
- Software

In CA CMDB, CIs in these base families receive CI Detail pages with some extraneous fields and without Attributes tab. Use the Change Family and Class capability of CA CMDB to convert these CIs to CA CMDB families. The advanced features include the ability to track family-specific attributes, versioning, snapshots, and baselines.

Change Family/Class of a Single CI

You can change the Family and Class for a single CI.

Follow these steps:

1. Select the CI that you want to change.
2. Click Edit.
   The Update Configuration Item page displays.
3. Change the Class value for the CI. Selecting the class also determines the family for the CI. You can enter a value directly or click the magnifying glass to select from a list of classes.

4. Click Save.
   The Family and Class of the single CI is changed.

Change CI Family/Class Using GRLoader

You can change the Family and Class for a CI by using GRLoader.

Follow these steps:

1. Create XML code to change the CI attribute.
2. Using GRLoader, open the CI you want to modify.
3. To change the CI attribute, run the XML through GRLoader.
   The Family and Class for a CI are changed.

Example: Set the Class of an Open CI to Document

The following example shows an XML fragment that sets the class of an open CI to *Document*.

```
<ci>
    <name>document number 1
    <class>Document
</ci>
```

Important! Do not attempt to update both the Family and Class attributes of a CI simultaneously. To change both, use two separate CI updates in two separate invocations of GRLoader.

Extending CMDB

This article contains the following topics:

CMDB is a highly flexible system that can be extended to include extra families, classes, and attributes according to your business needs. New attributes can be family-specific or *common* (applicable across all families). While CMDB provides predefined families with many classes and attributes based on industry standards, some business cases require one or more of the following activities:

- Extend one or more of the CI families by adding new attributes. For example, to add a GPS coordinate for every device on your office campus, you can define a gps_coordinate attribute to add to any family. If you only want to extend one family, use Web Screen Painter Schema Designer to define the new attributes in the existing extension table. In addition, whenever you add an attribute, you also must modify the Detail page, Attribute tab, and metadata forms that use the attribute. For more information, see Add Family Attributes (see page 2605).

- Extend all CI families by adding a common attribute. For more information, see Add Common Attributes (see page 2605).

- Add new classes to an existing family to support more classification detail in your system. For example, instead of the generic Server class, you can create a separate class for every model of server device. For more information, see Define a New CI Class (see page 2606).

- Add a new family by using an existing extension table and its attributes. A new family provides an alternative way of organizing or classifying CIs. For more information, see Define a New CI Family (see page 2607).

- If the existing class or family structure does not match your requirements, you can start over with a minimum set of attributes. To add a new family using a new extension table, define the new extension table and its attributes using Web Screen Painter Schema Designer. Also, create the forms that are required for display and update. For more information, see Constructing a New Attribute Framework (see page 2608).

Important: Extending CMDB requires specialized knowledge of CA SDM data structures and tables, and familiarity with Web Screen Painter (WSP). We recommend that you contact CA Services to help with this activity and also read and understand thoroughly the following sections before attempting to extend CMDB families and attributes.

Adding New CMDB Attributes

Adding a new CMDB attribute requires careful planning. CMDB already provides many attributes in its predefined families and classes, so determine whether they are sufficient for your needs before considering customization.

If you determine that a new attribute is necessary, we recommend proceeding conservatively by asking whether you must:

- add one or more new attributes to an existing family?
- add the new attribute(s) to more than one family?
- add a new common attribute, which applies across all families?

You can extend an existing family by adding new attributes. For example, if some devices on your office campus are assigned a GPS coordinate, you can add a gps_coordinate attribute to any applicable CI family. For more information, continue to Add Family Attributes (see page 2605).

After your attribute requirements are identified, if you determine that they require the use of new families and classes, see Adding a New CA CMDB Family or Class (see page).

Add Family Attributes

You can add a new attribute to one or more existing families by using the Web Screen Painter Schema Designer, which updates the database to include the new attribute and also updates the associated CA SDM tables and files. This method is preferred over updating the tables and file changes manually.

To add a new attribute to a family

1. Using Web Screen Painter Schema Designer, open the schema that corresponds to the family extension table.
2. Add the desired attribute to the extension table.
3. Publish the modified extension table.

Note: GRLoader and Versioning automatically pick up new attributes without further action. However, we also recommended that you enable logging. Logging is required for auditing purposes and Versioning enabled to record all snapshots.

To enable logging, verify that UI_INFO for the attribute is set to **AUDITLOG**.

After a new family attribute is created, it must be added to each display form so that users can see and update that attribute and to the metadata form specific to that extension table. For more information, go to Add Attributes to Forms (see page 2609).

In addition, Versioning requires metadata, including information about column headings and the related Standard CI attributes. You define new metadata for all new attributes that you create; for instructions, continue to Create Metadata (see page 2610).

Add Common Attributes

Common attributes are stored in the **ca_owned_resource** table in the **nr** object. This table provides the following customizable fields:

- smag_1
- smag_2
- smag_3
- smag_4
- smag_5
- smag_6

If you require less than seven modified attributes among all CI families, these fields provide a convenient solution.

As supplied, these custom fields do not display on any form. To allow CMDB users to view or update a smag_*n* field, use the Web Screen Painter (WSP) to add it to any display form. All logging and GRLoader functions are already enabled.

Note: For Web Screen Painter Schema Designer procedures, see How to Implement CA SDM and the Web Screen Painter online help.

Adding a New CMDB Family or Class

Adding a new CMDB family requires careful planning. CMDB provides many predefined families and classes, so determine whether these are sufficient for your needs before considering customization. If not, some new requirements can be met by one of the following actions:

- Defining a new class in an existing family
- Defining a new family that uses an existing extension table

If you determine that existing extension tables are insufficient for your needs, skip this section and continue to the section Constructing a New Attribute Framework (see page 2608) to create an extension table and the forms that it requires.

Define a New CI Class

You can add new classes to support higher levels of classification granularity. For example, instead of using any of the CMDB-provided classes in the Hardware.Server family, you can define more classes for different server devices.

Before you create a new configuration item class, determine whether a suitable class already exists in the Configuration Item Class List.

> **Note:** If you also require a new family to govern a new set of classes, skip this topic and proceed to Define a New CI Family (see page 2607). Then you can return and populate the new family with classes.

To define a CI class using the Administration interface

1. Navigate to the Configuration Item Class List.
2. Click Create New.
   The Create New Configuration Item Class page appears.
3. Enter a unique name for the new class.
4. Enter the appropriate family name in the Family field, or click the icon over the field to search for a family.
5. Verify that the Record Status field is set to Active.
6. Click Save.
   The new CI class is defined and ready for you to create new CIs.

Define a New CI Family

Before you create a configuration item family, determine whether a suitable family already exists in the Configuration Item Family List. If not, you can create new families as an alternative method of organizing or classifying CIs using existing attributes.

If the new family that you need cannot use an existing extension table (or the default table), complete all the additional preparations that are outlined in Constructing a New Attribute Framework (see page 2608). The new extension table can be used to define new families.

To define a CI family using the Administration interface

1. Navigate to the Configuration Item Family List.
2. Click Create New.
   The Create New Configuration Item Family page appears.
3. Enter a unique name for the new family.
4. Verify that the Record Status field is set to Active.
5. In the Extension Name field, select the extension table that identifies the type of family that you want to create. This may be a new extension table that you created recently.
   For example, if you are adding a family for an unspecified type of hardware, select ci_hardware_other. This type ensures that when you create configuration items whose classes use the new family, the appropriate attributes display on the Attributes tab. If you do not select a table name in the Extension Name field, the default table is used and only default attributes appear when you create a configuration item within the new family.

6. Type a description in the Description field.
   The description that you enter displays in the Configuration Item Family List for informational purposes.

7. Click Save.
   The configuration item family is defined.

Now that your new family is defined, you can add classes to it as described in Define a New CI Class (see page 2606).

Constructing a New Attribute Framework

If none of the existing class or family structures match your requirements, you can start over with a minimum set of new attributes. This requires construction of a new extension table and other supporting structures.

Before using the CMDB administration interface to define a new CI family that is based on a new extension table, use the Web Screen Painter Schema Designer to create the new extension table.

To use the new extension table, you must also create new HTMPL forms for:

- New CI Detail page
- New Attributes tab with its associated attributes
- New metadata form and metadata

CA CMDB supplies templates that you can use to build these HTMPL forms. The following sections provide more detailed information about what is required.

Note: For Web Screen Painter Schema Designer procedures, see How to Implement CA SDM and the Web Screen Painter online help.

To use the new framework in the CMDB user interface, define:

- One or more CI families that use the new extension table
- CI classes to classify your CIs by type

Create a New Extension Table

Before you can define a family that is based on a new extension table, update the database with the new table and also update the CMDB schema with information about that table.

To create an extension table

1. Using the Web Screen Painter Schema Designer, define the new extension table and extension name.

2. Save and publish the new extension table.

Note: WSP Schema Designer automatically creates the logging trigger in CMDB.

To create the CI Detail page, continue to the next section.

Create a CI Detail Page

A CI Detail page is required to support attribute display for CIs that are associated with a new extension table.

To create the CI detail page

1. Using the Web Screen Painter Schema Designer, click File, New, and create a form that is based on detail_extension.template.

2. Save this new form as **detail_***extension***.htmpl**, where *extension* is the name of the extension table.

3. Follow the instructions that are listed in the file, replacing the ***EXTENSION*** string with the name of the new extension table (defined previously).

4. Save the file with all changes.

The CI Detail page includes two attribute sections:

- Common attribute section named cmdb_detail.htmpl
- Family-specific section (the Attributes tab) named nr_cmdb_extension_tab.htmpl, where *extension* is the name of the new extension table.

Continue to the next section to Create the CI Attributes Tab (see page 2609).

Create a CI Attributes Tab

The Attributes tab displays the family-specific attributes for a CI.

To create the Attributes tab

1. Using the Web Screen Painter Visual Editor, click File, New, and create a form that is based on nr_cmdb_extension_tab.template.

2. Save this file as **nr_cmdb_***extension***_tab.htmpl**, where *extension* is the name of the new extension table.

3. Follow the instructions that are listed in the file, replacing the ***EXTENSION*** string with the name of the new extension table (defined previously).

4. Save and publish the file with all changes.

Continue to the next section to populate the Attributes tab.

Add Attributes to Forms

After Web Screen Painter Schema Designed has been used to create a new attribute in an extension table, that attribute must be added to any form that is used for display or update. For new family-specific attributes, the only form that must be changed is the Attributes tab that is named **nr_cmdb_***extension***_tab.htmpl**, where *extension* is the name of the extension table. This form must be edited to include any new attributes.

To edit an attribute form

1. Using Web Screen Painter Visual Editor, click File, Open to access the appropriate form.
2. Drag and drop the new attribute or attributes on the form.

   Note: CMDB-provided forms do not lend itself to editing using the Web Screen Painter Visual Editor, so use the Web Screen Painter text editor on the Source tab.

3. Save and publish the form.

If you have not yet created a metadata form, continue to the section Create a Metadata Form (see page 2610). To define metadata for a new attribute on the form, continue to the section Create Metadata (see page 2610).

Create a Metadata Form

A new extension table requires its own metadata form to define column headings and Standard CI information for Versioning.

To create the metadata form

1. Using the Web Screen Painter Visual Editor, click File, Open to access cmdb_metadata_extension.template.
2. Save the file as **cmdb_metadata_***extension***.htmpl**, where *extension* is the name of the new extension table.
3. Follow the instructions that are listed in the file, replacing the ***EXTENSION*** string with the name of the new extension table (defined previously).
4. Save and publish the form with all changes.

To populate the metadata form, continue to the next section.

Create Metadata

Metadata includes information about attribute column headings and Standard CI information that the Versioning feature requires.

Important: Metadata requires careful planning to ensure correct data in Snapshots, correct titles in Versioning, and successful Standard CI comparisons.

To create metadata

1. Using the Web Screen Painter Visual Editor, click File, Open to access **cmdb_metadata_** *extension*.**htmpl**, where *extension* is the name of the extension table.

2. Following the instructions that are listed in the form, copy and modify the indicated row for each attribute in the new extension table.

Note: The following attributes, although required, do not need metadata:

- ID
- Last_modified_by
- Etc (to be provided)

If you are adding metadata to an existing CMDB family, audit changes are displayed correctly on the Versioning tab. However, if you are defining metadata for a new extension table, you must have a new family and class for your attributes; for more information, see Adding a New CA CMDB Family or Class (see page).

The structures for your new extension table are now in place. To define a new family for your attributes, continue to Define a New CI Family (see page 2607).

Example

In this sample scenario, you create an **Automobile** family and a **Sedan** class in it for tracking inventory for manufacturing, shipping, rental transportation, or other purposes. You could also create many other automobile classes; this example is for demonstration purposes only.

Step 1 Create the New Extension Table

1. In Web Screen Painter Schema Designer, click Add Extension Table.

2. Enter a name for the new extension table. In this example, **vehicle**.
   The **zvehicle** extension table is created and its properties displayed.

Note: "z" is appended to the beginning of all new table names to distinguish them from application-provided tables.

3. In the Table Info tab, set the Function Group field to **inventory**. Other fields are populated with default values.

4. Add new columns and attribute information as desired.

5. Save and publish the new extension table.

Step 2 Create a New Family

To create a family

1. Navigate to the CI Family List.
2. Click Create New.
   The Create New Configuration Item Family page displays.
3. Enter a unique name for the new family. In this example, **Automobile**.
4. Verify that Record Status is set to Active.
5. Select the extension table name. In this example, **zvehicle**.
6. Click Save.
   The new CI family is created.

Step 3 Create a New Class

1. Navigate to the CI Class List.
2. Click Create New.
   The Create New Configuration Item Class page displays.
3. Enter a unique name for the new class. In this example, **Sedan**
4. Verify that Record Status is set to Active.
5. Select the Family. In this example, **Automobile**.
6. Click Save.
   The new CI class is created.

Step 4 Create the New CI Detail Form

To create the CI Detail form

1. In the Web Screen Painter Visual Editor, open the form detail_extension.template.
2. Save the template with the name **detail_zvehicle.htmpl**.
   The new form is saved under NX_ROOT\site\mods\wsp\project\web\analyst
3. In the new form, replace all instances of ***EXTENSION*** with **zvehicle**
4. Save and publish the new CI Detail form.

Step 5 Create the Attributes Tab

To create the Attributes tab form

1. In the Web Screen Painter Visual Editor, open the form nr_cmdb_extension_tab.template
2. Save the template with the name **nr_cmdb_zvehicle_tab.htmpl**
   The new form is saved under NX_ROOT\site\mods\wsp\project\web\analyst
3. In the new form, replace all instances of ***EXTENSION*** with **zvehicle**
4. Add attributes to the form as desired.
5. Save and publish the new Attributes tab form.

Step 6 Create the Metadata Form

To create the metadata form

1. In the Web Screen Painter Visual Editor, open the form cmdb_metadata_extension.template.
2. Save the template with the name **cmdb_metadata_zvehicle.htmpl**
   The new form is saved under NX_ROOT\site\mods\wsp\project\web\analyst
3. Replace all occurrences of ***EXTENSION*** with **zvehicle**
4. Using the heading and attribute placeholders, add metadata for all family-specific attributes.
5. Save and publish the new metadata form.

CMDB Visualizer

This article contains the following topics:

CA SDM lets you align your IT components (*configuration items*, or CIs) with your business services. CA CMDB defines *relationships* among CIs, as when a group of CIs work to provide a business service. CMDB Visualizer lets you see the entire picture of your CI relationships, and provides functions to manage the relationships. Working from a *focus CI*, you can use the Visualizer to display up to nine levels of related CIs.

Advanced Availability Configuration Only

Note: If the visualizer makes a server request during the application server quiesce period, the following message appears:

"This CMDB Visualizer server is scheduled to shut down for maintenance in xx:xx. Please save your work and logout.".

You can hide the message box but the message is displayed on the top panel throughout the quiescing period. If the server quiescing is canceled, you receive a message about the cancellation.

CA uses a provider/dependent model to define relationships among CIs. All CIs that contribute to a business service are *providers* to that business service (the *dependent*). In much the same way, providers can also be *dependents* that rely on other CIs. You can use Visualizer to perform the following provider/dependent analyses:

- **Browse**
  Displays an unfiltered view of all CIs.
- **Impact Analysis**
  Starts with a focal CI (provider) and searches for its dependents.
- **Root Cause**
  Starts with a business service (dependent) and view all the CIs that are providers to that service.
- **Cause and Effect CIs**
  Combines impact analysis and root cause in one search.
- **Trace Relation**
  Displays all possible relationships that are based on levels. If you select only one CI, this filter displays the Browse view.
- **Shortest Path**
  Displays the shortest chain of relationships that are based on levels.

CMDB Visualizer lets you do the following actions:

- Visualize multiple levels of CIs from a configurable graphical view.
- Monitor or cancel rendering progress.
- Search using flexible criteria.
- Filter based on CI families, relationship types, and other attributes.
- Display CI relationships.
- Trace a relationship between two CIs.
- Visualize a dependency chain.
- Invoke CA CMDB directly from Visualizer.
- Display CI attributes and properties.
- Save graph metadata.
- Print the graph layout.
- Find a specific CI on a displayed graph.
- Create a CI (depending on role).

- Create new CI relationships (depending on role).
- Use the Scratchpad to store key CIs.
- Display CI status.
- Hide or reveal a CI in the Visualizer layout.
- Role-based data security.
- Launch external MDRs.
- Obtain online help for Visualizer features.

Perform Root Cause Analysis

Using Visualizer with the CMDBf Viewer, you can perform a root cause analysis.

Follow these steps:

1. In Visualizer, locate a Service CI in a particular problem condition (for example, slow or unavailable).
2. Right-click the CI and select Make Focal CI.
3. Select a Root Cause filter using the following criteria:
   - Class Type: n/a
   - Dependent to Provider Relationship: All relationships to be displayed for the root-cause analysis.
4. Click View.
   In the resulting graph, all CIs that are related to the focal CI are displayed as specified in the filters. All paths between CIs include intermediary CIs to the default level.
5. Navigate to the CIs and inspect them for incidents, problems, or recent changes. These could be candidates for the root cause of the focal CI condition.
6. Launch CMDB in context for a particular CI.
7. Click CMDBf Viewer.
   The Federated View is displayed with the list of MDR providers for the CI.
8. To obtain the latest MDR attributes, click Retrieve.
   The MDR attributes are updated.

Visualizer Administration

The Visualizer administration interface can be used to edit CMDB Visualizer settings. These functions are only available to roles with administrator privileges.

The following tabs are disabled on the Visualizer running on secondary servers. These tabs are enabled on all the other CA SDM servers:

- **Visualizer Configuration Tab**
  Permits setting of the server and CI display information.
- **Relationship Style Tab**
  Defines relationship graphical characteristics.
- **CI Status Tab**
  Defines CI graphical characteristics.
- **Filters Tab**
  Creates, edits, and deletes filters for CI analysis.
- **Icon Configuration Tab**
  Maps a CI family to its respective icon image when CMDB Visualizer has been upgraded from r11.2 to Release 12.9. For more information about Visualizer definitions, see the Visualizer Administration (see page 2597) topic.

CA Business Service Insight Integration

When you integrate CA Business Service Insight and CA Service Desk Manager, the BSI Service tab displays Exceeds and Violations counts. The BSI Service by Metric and BSI Contract by Metric tabs display the Metric, Violation, Compliant, and Target attributes.

Note: These tabs only appear for CIs with Federated Asset mappings to the CA Business Service Insight MDR.

The integration provides the following reports:

- **Service Level Compliance**
  Displays information about CA Service Desk Manager Enterprise Service family CIs.
- **Modified Service Level by Metric vs. Target**
  Displays information about CA Service Desk Manager Enterprise Service family CIs.
- **Modified Service Level by Contract vs. Target**
  Displays information for CA Service Desk Manager Contract family CIs. Enter a valid CA Business Service Insight Contract Party and refresh the report.

Consider the following information to help you debug error messages:

- For an incorrect CA Business Service Insight MDR userID or SharedSecret, the error message displays Invalid username/org.name.
- For an incorrect CA Business Service Insight hostname, the error message displays BSI hostname is unknown.

- For an invalid Contract Party in the BSI Contract by Metric tab, the error message displays there is no metric data for the contract for the Reporting Period.
- If no CA Business Service Insight reports are associated with a particular Service or Contract, one of the following error messages is displayed:
  - For Services, there are no service details reports for federated service id.
  - For Contracts, there is no metric data for the contract for the Reporting Period.
- If CA Business Service Insight services are not available on the CA Business Service Insight computer, the error message displays that the CA Business Service Insight hostname is unknown.

Database Views

This article contains the following topics:

The CA SDM database is a repository for data entered and used to operate your service desk. CA SDM provides several database views and enables you to create customized reports of the database.

Basic Views

The basic views are based on CA SDM's tables. These views show data as long as the implementation makes use of Requests, Incidents, Problems, Change Orders, Issues, Assets, or Contacts / Groups.

Using the basic views, you can design and produce many reports, including:

- Detailed and summarized lists of open priority 1 requests sorted by request area.
- Detailed and summarized lists of change orders assigned to the level 1 group that have been open for more than 24 hours, sorted by priority.
- Counts of issues open for more than a specified number of days, sorted by priority, assigned group, or priority and assigned group.

The following basic views are provided:

View Name	Description
View_Contact_Full	All contacts, including their contact type, location, organizations, and service types
View_Contact_to_Environment	All contacts and their environment (assets)
View_Group	All the groups defined in the database
View_Group_To_Contact	All contacts (including managers) within their group assignments
View_Request	

View Name	Description
	All requests, including their service types, severities, urgencies, categories, assets, impact numbers, assignees by name, customers by name, groups, statuses, and priorities
View_Act_Log	The request activity log information, including activity type and analyst name
View_Request_to_Act_Log	All requests with their activity logs (this view joins View_Request and View_Act_Log)
View_Request_to_Properties	Requests and their properties (this may not include all requests, especially if no properties are assigned to them)
View_Change	All change orders, including their statuses, priorities, categories, organizations, affected end users by name, requesters by name, assignees by name, groups, service types, and impact numbers
View_Change_Act_Log	The change order activity log information
View_Change_to_Change_Act_Log	All change orders with their activity logs (this view joins View_Change and View_Change_Act_Log)
View_Change_to_Properties	Change orders and their properties (this may not include all change orders, especially if no properties are assigned to them)
View_Change_to_Change_WF	Change orders and their workflow tasks (this may not include all change orders, especially if no workflow tasks are assigned to them)
View_Change_to_Assets	Change orders and their assets (this may not include all change orders, especially if they have no assets)
View_Change_to_Requests	Change orders with basic information about attached requests (this view joins View_Change and the Call_Request table, which may not include all change orders -- especially if no requests are attached to them)
View_Issue	All issues, including their statuses, priorities, categories, organizations, affected end users by name, assignees by name, groups, service types, and so on
View_Issue_Act_Log	The issue activity log information
View_Issue_to_Issue_Act_Log	All issues with their activity logs (this view joins View_Issue and View_Issue_Act_Log)
View_Issue_to_Properties	Issues and their properties (this may not include all issues, especially if no properties are assigned to them)
View_Issue_to_Issue_WF	Issues and their workflow tasks (this may not include all issues, especially if no workflow tasks are assigned to them)
View_Issue_to_Assets	Issues and their assets (this may not include all issues, especially if they have no assets)

Advanced Views

The advanced views are based on CA SDM's audit_log table. Install the audit_ins and /or the audit_upd options in the Options Manager and restart the system before using these views.

Using the advanced views, you can report on the duration of a ticket (that is, request, change order, or issue) in a particular state. For example, you can report on the following:

- Show the length of time, between opening and assignment to L2 for requests opened since January 1, 2002
- Show the length of time, issues remained priority 3 before escalating to priority 2 for issues opened since January 1, 2002.

The following advanced views are provided, which are views of the audit_log table in the CA SDM database that specifically query for the status, priority, group, or assignee attributes:

View Name	Description
View_Audit_Status	All tickets sorted by the time in each status (does not include tickets that have no status)
View_Audit_Priority	All tickets sorted by the time in each priority
View_Audit_Group	All tickets sorted by the time in each group assignment (does not include tickets that have no group)
View_Audit_Assignee	All tickets sorted by the time in each individual assignment (does not include tickets that have no assignee)

Important! You must install audit logging options using the Options Manager, to view data in the advanced views. The descriptions for the Audit Options audit_ins and audit_upd in the Online Help provide more information.

Maintain Relationships

You can create and manage the relationships between configuration items.

To create a new relationship:

1. From the Administration tab, navigate to the CI Relationship List.
   The Configuration Item Relationship List page appears.
2. Click Create New.
   The Create New Configuration Item Relationship page appears.
3. Fill in the following fields:

- **Tenant (if multi-tenancy is installed)**
  The tenant level for this relationship.

- **Provider/Peer CI**
  The configuration item that provides the relationship. Enter the configuration item name directly into this field. To select the configuration item from a list, click the search icon.

- **Relationship Type**
  Use the Relationship Type Search and List to select relationship type.

- **Dependent/Peer CI**
  The dependent configuration item in this relationship. Enter the configuration item name directly into this field. To select the configuration item from a list, click the search icon. This field is required.

- **Symbol**
  (Optional) The unique identifier for this relationship. Assign a symbol that makes the relationship easily recognizable from the list.

- **Description**
  (Optional) A detailed description of the relationship. You can also use this field to describe the repositories that are assigned in the relationship.

- **Source Repository**
  (Optional) A detailed description of the relationship. You can also use this field to describe the repositories that are assigned in the relationship.

- **Cost**
  (Optional) The dollar value of the relationship between the configuration items.

4. Click Save.
   The relationship is created and assigned to the selected CIs.

CI Relationship Types

CA Service Desk Manager provides a list of predefined relationship types. Use these relationship types to describe a relationship or association between configuration items. How the relationship is expressed depends on which configuration item is the focus. For example, a provider *supports* a dependent configuration item, but the dependent *is supported by* the provider. These are different expressions of the same relationship. The relationship type label that you see depends on whether you are viewing a provider-to-dependent or a dependent-to-provider relationship. For information about the relationship types in CMDB, see the CI Relationships (see page 2489) topic.

Using Configuration Audit

The Configuration Audit node lets you perform the following actions:

- Manage Incidents that CACF (see page) created for rogue or improperly executed changes. For example, View which changes have failed verification and which changes require more investigation.

- Manage Changes Specifications (see page 2622).
  For example, view all Change Specifications that completed successfully or are pending verification.

- Manage open Change Orders (see page) with active Change Specifications.
  For example, view the changes orders that are still open with pending change specifications.

- View the Verification Log history (see page) that shows all verification activities that have occurred in the system.
  For example, view which MDR is responsible for rogue updates and the affected CIs.

Managing CACF Incidents

The Change Manager manages CACF incidents generated due to a rogue change or improperly executed Change Orders that require further attention.

CACF policies provide conditions under which Incidents are created, and can specify that Incidents close automatically after failed verification remediation.

Managing Change Orders

The Change Manager manages Change Orders with active specifications from this menu.

Verification Log

The Verification Log list lets you view all CACF change verification activity. CACF logs each attempted update to the CI, and if the update was allowed. This log helps you determine which policy allowed or disallowed a change to a CI.

For example, search for a log that specifies a specific CI where CACF detected a variance or unverifiable change. The results display information such as the previous and discovered value, the verify status, and associated Incident.

You access the verification log from the following locations:

- On the Administration tab, click CA CMDB, Configuration Audit, Verification Log.

- On the Scoreboard click CMDB, Configuration Audit, Rogue Inserts or Rogue Updates.

The Verification Log tab for the specific object shows detailed events only pertaining to the object in question. View the log for the following objects:

- Verification Policies

- Change Orders

- Change Specifications

- CIs

- Incidents

Note: Verification log entries highlighted in red indicate that the corresponding change specification is either Failed Verification or Manual Verification Active, and requires further attention by the user.

The Discovered Attribute History list displayed in the Change Specification form lists all attribute values for the currently selected managed attribute and CI that were recently discovered by an MDR, whetherthey were actually authorized or loaded into the CMDB.

Use this list to assist in defining the planned value for the change specification. In the list you can view the format, case sensitivity, and so on of the previously discovered values so that you can determine an appropriate planned value pattern.

Managing Change Specifications

This article contains the following topics:

The Change Manager manages change specifications in your CACF environment. Change Analysts create Change Specifications when they create Change Orders. The Change Analyst defines the change in terms of the specific CI and CI attribute being changed.

The Change Specifications list shows all verified and outstanding change specification verifications in your environment. The ability to modify a change specification depends on the status of the Change Order. By default, you can only modify change specifications in Change Orders with the RFC status. After CACF verifies this change, it considers all subsequent changes as rogue inserts or updates

If multiple discoveries occur during change specification verification, discovery data can invalidate a previously verified change. At the end of verification, the CI is in the state that all the change specifications desire. For example, a variance occurs for a CI with a change specification in the Verified state, but the status changes to Failed Verification.

A single CI can have many outstanding change specification verifications pending from many Change Orders. CACF evaluates each verification independently, and a single MDR update can update multiple pending change verifications.

The Final field on the Change Specification List indicates whether a change has been completed. The Change Order is eligible for to move to the next default state when all change specifications are final and the Promote Change Order After Verification option is enabled for the managed change state.

The following fields require explanation:

- **Verify Status**
  Specifies the status of the change specification, such as Verification Pending. For more information about change specification statuses, see Change Specification Statuses (see page 2627
  .

- **Change Order Status**
  Specifies the status of the Change Order.

- **Incident**
  Specifies the Incident that the verification policy creates optionally for an incorrectly implemented Change Order.
  If the Configuration Administrator specified the policy option to create Incidents, the Incident documents the expected and discovered values. If all discoveries result in failed verifications, the Incident receives log comments indicating that the incident represents multiple failures.

- **CI Name**
  Specifies the CI that you want to define the change specification.

  When you make several identical changes to a set of CIs, you can leave the CI Name field blank in the Change Specification. In this case, the Managed Attribute and Planned Value apply to all CIs attached to the Change Order. Change specifications for each CI are created when the Change Order moves to a status with Change Verification Active enabled for the managed change state.

- **Original Value**
  Specifies the value of the attribute at the time a user created change specification.
  The original value field shows the current attribute value for the CI when defining the change specification value for the first time.

- **Last Discovered Value**
  Specifies the last value that was discovered for the attribute during the implementation and verification active process. This field updates each time CACF discovers a new value for the attribute.

- **Last Verification Policy**
  Specifies the verification policy that was in effect during the last change verification for this change specification.

- **Verification Message**
  Shows the message associated with the last verification action such as the reason why a verification failed.

- **TWA**
  Link to the TWA record associated with this change specification and policy.

Create a Change Specification

Create a change specification for a Change Order. By default, you can only modify change specifications in the RFC state. The Configuration or Change Administrators can change the definition of the Change Order managed change state that allows modification of change specifications.

The Verification Log tab shows the change verification activity history for this change specification. The log shows details about the policy and actions that CACF takes when change verification was in effect for the change specification. Verification log entries highlighted in red indicate that the corresponding change specification is either Failed Verification or Manual Verification Active, and requires further attention by the user.

To help you set the planned value, the Discovered Attribute History tab lists all values that an MDR recently discovered, whether they were authorized or loaded into the CMDB. From this tab, you can see the format and case sensitivity of the values so that you can determine an appropriate planned value pattern.

The Change Specification History tab shows the audit history listing all previous modifications made to the change specification options with the time and the user that made the changes.

Follow these steps:

1. From a Change Order, click the Configuration Management tab and select the Change Specifications tab.

   You can also create change specifications from the Administration tab from CA CMDB, Configuration Audit, Change Specifications. You can also create them from a CI if you click the Related Tickets tab then select the Change Specifications tab.

   The Change Specifications List page appears.

2. Click Create New.
   The Create New Change Specification page appears.

3. Complete the following steps:

   a. Enter the Change Order number that requests the change (only required if created from a CI or the Administration tab).

   b. Enter the name of the CI associated with the Change Order.
   You can leave the CI name blank to imply that the change specification applies to all defined CIs (see page 2629) for the Change Order.

   c. Set the change specification as Active or Inactive.

   d. (Optional) Enter a description for the change specification.

e. Select the Managed Attribute for this change specification from the drop-down list.
Selecting Any Managed Attribute indicates that any managed attribute can be changed during the verification of the Change Order. In this case, multiple attributes can be updated, the planned value cannot be specified, and the planned change status is never updated.

f. Enter the planned value of the Managed Attribute.
Specify the expected value of the attribute after executing the change. After the Change Order moves into a verification state, and the CI updates through the web interface, GRLoader, or Web Services, CACF compares the planned value with the inbound data to determine a match.
You can embed special characters (see page 2626) in the planned value when the exact value is not known.

g. Select the appropriate verification state of the Change Specification from the drop-down list:

- Manual Verification will be required
  When CACF verifies the Change Order, manual verification will be required.
- Set after Change Verified
  Set the CI attribute to the planned value after verification completes. Use this option for setting CI attributes when the attribute is not discoverable.

  The set operation only occurs when the Change Order moves from a state with change verification active to a nonactive default state. For example, the set takes place when a Change Order moves from Verification in Progress to Closed. The set does not occur if the Change Order is canceled, demoted, or moved to another state.

- Use Discovered Value
  Copy the discovered value to the CI at verification time, used when the planned value is not known prior to verification.
- Verification Pending
  The change has not been verified and waits for a CI update (see page 2627).

4. Click Save.
   The change specification is saved.

Change Specification Considerations

Consider the following information about change specifications:

- The CI name can be left blank which implies the change specification applies to all CIs defined for the change order. This option is useful when all of the CIs for Change Order are using the same planned value. The change specification applies to all CIs that are attached to the Change Order (see page 2629) when the managed change state moves to a state with change verification active.

- You can create a Change Specification that requires manual verification. This action lets you verify managed attributes manually (see page 2629).
- Change Specification planned values for Lookup field managed attributes must be unique. For example, if you want to create a planned value for the Primary Contact (primary_contact), the contact specified in the planned value must be unique.
- You set case sensitivity only for comparisons made for change specification managed attribute planned values using the *Case Sensitive* option in the managed attribute. Specifying case-sensitive managed attributes do *not* affect the policy selection patterns.
- When the exact value is not known for the planned value, you can use wildcard (*), range (> or <) or negation (!) values (see page 2626).

Special Characters

You can embed special characters when you do not know the exact value. Use the asterisk wildcard character to match any number of characters. The pattern *must* match the discovered data in the same sequence, and spaces are significant.

For example, enter *10.*.*.** as the Planned Value to match any IP addresses that begins with *10.* and has two periods that follow any value between the periods.

For example, the inbound server_type value contains Windows 2003 (WIN32) 5.2.Service Pack 2 (Build 3790) Intel x86. To verify this value, specify a planned value of ** Service Pack 2 ** in the change specification.

A word at the beginning of the planned value indicates that the discovered value must start with that value. Similarly, an asterisk at the beginning of the planned value indicates that the discovered value can begin with any value and end with the value specified following the asterisk.

The following table provides examples about how to use the asterisk:

Planned Value	Discovered Value	Match or No Match
a	b	No Match
a	a	Match
a	aba	Match
a	bab	Match
a*	a	Match
a*	ab	Match
a*	ba	No Match
*a	a	Match
*a	ab	No Match
*a	ba	Match

A pattern that begins with an exclamation point results in the negation of the value. You can only use the exclamation point as the first character in the pattern. For example, you cannot use a pattern of 10.!*.*.*.

To compare numeric values contained within string values, use greater than (>) or less than (<) as the first character in the planned value. If there is a leading exclamation point, it must be the second character.

CACF ignores leading or trailing nonnumeric values in the discovered value and planned value patterns.

The following table provides examples about how to use the exclamation point, and the greater than and less than symbols:

Planned Value	Discovered Value	Match or No Match
>200	aaa 201 bbb	Match
>200GB	aaa 200 bbb	No Match
>200GB	300 GB	Match
!<200GB	200 Bytes	Match
!<200	200 Bits	Match

If you do not know the planned value in advance, but the value may change, you can set the status of the change specification to Use Discovered Value. This behavior requires discovery to update the CI before CACF considers the change specification as validated. You require this behavior for numeric fields and SRELs where an asterisk cannot be accepted as a planned value.

To help you with setting the planned value, the Discovered Attribute History tab lists all values that were recently discovered by an MDR, and whether were actually authorized, or loaded into the CMDB. This tab displays the format, case sensitivity, and other information about values so that you can determine an appropriate planned value pattern.

Change Specification Statuses

Change specifications use status to indicate the type of verification to perform and the current state of verification. The status values are also used in the verification log when recording change verification operations during the verification process.

- **Initial Statuses**
  Used when creating a Change Specification to specify the type of verification for CACF to perform. These statuses are non-final and the Change Order is not considered verified when change specifications are in either of these statuses.
  Verification Pending -- The change specification has not been verified, or the change is waiting for the CI update.
  Manual Verification will be required -- When the changes for a Change Order are verified, manual verification will be required.
  Use Discovered Value -- Copy the discovered value to the CI at verification time, and used when

the planned value is not known prior to verification.
Set After Change Executed -- Sets a CI attribute to the planned value after verification has completed. Use this status for setting CI attributes when the attribute is not discoverable. For example, set the CI Primary Contact to User1 after a change completes.

- **Final Statuses**
  Indicates a completed change specification and considered as final. When all change specifications enter either of these final states, the Change Orders are eligible for promotion to the next default state.
  Verified -- The change specification has been successfully verified.
  Was Manually Verified -- The change specification has been manually verified.
  Used Discovered Value -- The CI has been updated with the discovered value.
  Was Set To Planned Value -- The CI has been updated with the planned value after Change Order verification.
  Accepted Planned Value -- The CI has been updated with the planned value and overwritten during verification.
  Accepted Discovered Value -- The CI has been updated with the last discovered value and overwritten during verification.
  No Change -- The planned value matched the CI at verification time and no verification was required.
  Cancel -- The change specification was canceled (see page 2629) by the change manager.

- **Intervention Statuses**
  Indicates a change specification requires manual intervention for verification. CA SDM highlights these statuses in a red color on list forms. These statuses are not final and the Change Order is not considered verified when change specifications are in either of these statuses.
  Failed Verification -- Discovery found the value to be other than what was specified in the Change Order. The Change Analyst must determine if the change was correctly executed and the Change Order was incorrectly specified, or if the Change Order was correct and the change requires verification again. Depending on the definition of the Managed Change State and the current change order status, the Change Analyst can override, change, or cancel the failed change specification.
  Manual Verification Active -- Manual verification is required before the change specification can be marked final.

- **Action Override Statuses**
  Indicates an action to initiate during change verification. These statuses are not final and the Change Order is not considered verified when change specifications are in either of these statuses.
  Accept Planned Value -- Request to override the CI attribute with the planned value.
  Accept Discovered Value -- Request to override the CI attribute with the last discovered value.

- **Reporting Status**
  Indicates the result of policy operations that the verification log displays for logging purposes and not used by change specifications.
  Update Was Allowed -- A policy allowed a request to update a CI and did not match any change specifications.

Managing Failed Verifications

When a verification fails, the CMDB, Configuration Audit, Failed Verifications node in the scoreboard lists the number of failed verifications and change specifications that require manual intervention in a red color. The Change Specifications can also be viewed under the Change Specifications tab in the Change Order, CI or Administration tab with the verify status of "Failed Verification". When a verification fails, the Change Analyst can intervene or wait until the next discovery occurs.

If the managed change state allows the Show Change Specification Override Buttons action, the Change Analyst can open the change specification, review the data, and click one of the following options to close the verification by moving it to a final state:

- **Accept Discovered Value**
  The Analyst determines that the change specification is incorrect and that the discovery tool has discovered the correct value.

- **Accept Planned Value**
  The Analyst determines that the discovery tool is wrong or has not performed discovery, and to accept planned value, as if it was discovered correctly.

- **Cancel**
  This portion of the Change Order was not executed and this specification was canceled.

Managing Undiscoverable Attributes

When a Change Specification requires manual verification, the Configuration Analyst must manually verify the change. The CMDB, Configuration Audit, Manual Intervention node in the scoreboard shows the number of change specifications that require manual intervention in a red color. The Change Specifications can also be viewed under the Change Specifications tab in the Change Order, CI or Administration tab with the verify status of "Manual Verification Active."

If the managed change state allows the Show Change Specification Override Buttons action, the Change Analyst can open the change specification, review the data, and click one of the following options to close the verification by moving it to a final state:

- **Mark as Verified**
  Used when the attribute is not discoverable and manually verified.

- **Cancel**
  This portion of the change order was not executed and this specification was canceled.

Defining Bulk Changes

Creating identical changes to a large number of CIs, for example, when changing the location for a collection of CIs, with the following steps:

1. Create a Change Order.

2. Define a single change specification which describes the change and leave the CI name blank.

3. Attach all the CIs to the Change Order.

If you do not know the exact details of a change in advance of the implementation, for example, you acquire a new Server and you only know the CI Name, complete the following steps:

1. Create a Change Order.
2. Create a change specification that specifies Any Managed Attribute as the attribute name.
3. Leave the planned value empty, since it is unknown.
4. Move the ticket through the change management process.
5. When the Change Order is in a verification active state, and discovery runs, the inbound CI data loads into the CI (assuming that the policy allows it).
6. When all discoveries for the CI complete, the Change Manager must mark the change specification as verified manually.

Follow these steps when there are a large number of dissimilar changes to a large number of CIs. For example, when moving a collection of servers from one location to another, and also assigning each one a unique IP address.

1. Create a Change Order
2. Create a spreadsheet and list on each row the Change Order number, CI and, the new attribute values. Each row results in a distinct change specification.
3. Load the spreadsheet with GRLoader to create the required change specifications.
4. Promote the Change Order and its change specifications as usual.

For more information about using GRLoader, see CMDB Technical Reference (see page 4168)
.

Configuration Audit and Control Facility (CACF)

Configuration Audit and Control Facility (CACF) unifies three disciplines: Change Management, Configuration Management (CMDB), and Discovery Management. CACF verifies that changes are executed accurately and no unauthorized changes occur.

Change verification ensures that the CMDB reflects any changes accurately, and the Discovery Management tools verify the changes.

Change verification provides the following benefits:

- **Change Management**
  - Assurance that authorized changes execute correctly.

- Detection of incorrectly executed changes.
- Detection of unauthorized changes.
- Management reporting.
- Full auditing of all changes down the attribute level.
- Detection of overlapping or conflicting changes.

- **Configuration Management**
  - CMDB contains an accurate and current representation of all managed CIs.
  - Ability to view the future state of the CI with the proposed change specifications.
  - Full auditing of CIs.

CACF has two major sections: the CMDB administrative interface and the change management interface.

CACF Administration and Policy Definition

This article contains the following topics:

The CMDB Administrator defines CIs and attributes that are managed. The CMDB Administrator also defines the policy for updating those CIs and attributes. You administer the CACF components in the Configuration Control node in the CA CMDB section of the Administration tab. Define CACF change specifications from the Change Order, CI, Incident forms, or the Configuration Audit node on the Administration tab.

The administrator must consider allowing standard changes and whether to define the following items:

- Authoritative and trusted sources of data.
- CIs and the CI attributes that are under CACF management.

An incorrectly executed change or rogue change can occur (also referred to as a variance). In this case, CA SDM can respond in any of the following ways:

- accept the new value
- create an Incident
- copy the data to the TWA for later processing.

CA SDM can use any combination of these actions.

Important! The Configuration Administrator *must* establish a change verification strategy (see page 2658) for your environment. The default policy for CACF allows all changes to all CIs. This policy applies even if the change is rogue, or if the change does not match a change ticket.

You can implement change verification policies dynamically or scheduled in advance. You can define these policies as generic or highly specific. The change verification policy describes how CA SDM responds to the following events:

- **Updates from Unauthorized MDRs**
  Indicates that specific MDRs are authoritative for specific attributes. CI attribute updates from unauthorized MDRs can be selectively accepted or rejected.
  For example, define policies to prevent CA Application Configuration Manager from updating the IP address of a CI, even if a matching Change Order exists. Let updates to IP address only if the source MDR is Spectrum.

- **Rogue Changes**

Detects and manages updates to CIs when no corresponding Change Order exists. Specify a policy that manages rogue changes requesting inserts or updates of CI data. For example, you can define a policy that loads data into TWA and does not update the CI for the following conditions:

- A CI named similar to server* in New York changes

- The change does not have a matching Change Order

- **Incorrectly executed changes**
  Detects whenever a Change Order is not implemented (see page 2633) correctly.

Auditing facilities provide the Configuration Manager with capabilities to view changes to policies and CACF object definitions. CACF logs each attempted update to the CI, whether the update was allowed. This log helps you determine which policy allowed or disallowed a change to a CI.

The Configuration Administrator defines which Change Order statuses represent changes that can be edited, and which Change Order change states represent verification states. By default, you can edit change specifications for Change Orders in the *RFC* change state. In addition, you can edit when change verification occurs for a Change Order in the *Verification in Progress* state. Optionally, change tickets can be automatically promoted or closed when all associated change specifications execute successfully.

Important! Performance may be degraded if the Configuration Administrator enables the Create Incident option with more than one active verification policy.

Note: By default, CACF considers updates to attribute values to Change Orders with change verification active as non-rogue changes. The changes are effectively in the Verification in Progress status. The Configuration Administrator can modify this behavior (see page 2649).

How Change Analysts Define Change Specifications

The Change Management interface portion of change verification integrates into the change ticket order form. Change Analysts typically create change specifications when they create a Change Order. The Change Analyst defines the change in terms of the specific CI and CI attribute that they want to change.

The Change Analyst can describe the change specification using any of the following templates:

- Provide the exact CI, CI attribute, and value.
  For example, after the change has been implemented, the IP Address for server1 sets to 10.10.10.10.
- Provide the CI attribute and value, but omit the CI name.
  For example, after the change, all CIs attached to the Change Order upgrade to 8 GB of memory.
- Provide an attribute value to set when the attribute is not discoverable.
  For example: after the change, the CMDB reflects that all CIs are located in NY.
- Use the discovered value.
  For example, you do not know the new IP address in advance, but you know that the IP address will definitely change. Set the IP Address of the CI to whatever value the authoritative MDR discovers.

When the change order is approved, the change specifications are approved as part of the same approval process. The subsequent modifications to the specification can be prohibited and are fully audited.

Change Verification

Change verification ensures that Change Orders execute according to change specifications. A Change Order is verified when its state is Verification in Progress and when the CI is updated. Now, when data from any MDR or web client user imports into the CMDB, CACF compares the incoming attribute data with active change specifications. If the CI attribute data matches, CACF verifies the change. If the inbound data does not match the Change Order specifications, a corrective action can occur based on the policy.

The executed policies can perform any of the following actions:

- Reject a single attribute update from the transaction.
- Reject the entire transaction, including all attribute and value pairs.
- Load the entire transaction to the TWA for deferred processing after approval and verification of the transaction.
- Create an Incident that describes each variance.

Note: This action can trigger existing notification and automation. To prevent multiple incident creation, rogue change detection creates a single incident for all rogue changes to a single CI.

- Accept the transaction unconditionally when accepting data from authorized source MDRs.

For example, the CMDB Administrator can define a policy that creates an Incident when a change to a production server executes incorrectly. When imported data from an authorized MDR does not match a pending change specification, CACF creates an Incident. The policy can allow or reject a CI update by the nonmatching import data. In addition, the Change Manager may accept the newly discovered value, even if the value does not match the planned change specification exactly.

Note: If multiple discoveries occur during change specification verification, discovery data can invalidate a previously verified change. At the end of verification, the CI is in the state that all the change specifications want.

How Change Managers Use Change Specifications

The Change Manager can perform the following actions:

- View and modify the verification status of each change specification.
  For example, the Change Manager wants to know which change specifications are still pending for Change Order 12345. The change order is in *Pending Verification* status.

- Manage Incidents for rogue or improperly executed changes.
  For example, the Change Manager wants to see which changes have failed verification and which changes require more investigation.

- Manage the changes that require manual intervention.
  For example, a Change Order specifies that manual verification is required for a nondiscoverable change. The Change Analyst must complete the task.
  For example, the Change Manager investigates and determines that Change Order 12345 specifies ten different change specifications. Due to a typo, change specification number 9 was incorrect and can be canceled.

Auditing facilities provide the change capabilities to view the status of each update to the change specification and any overrides to the change specification. The scoreboard shows the status of the running system and any exceptional conditions that require intervention or investigation. CA Business Intelligence reports provide a longer term view of the efficiency of Configuration Manager policies to monitor the health of your environment.

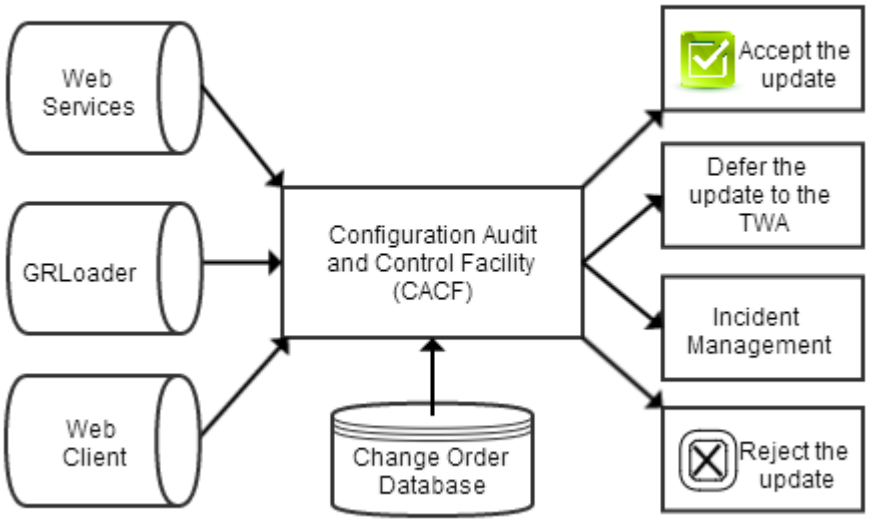
How Configuration Audit and Control Facility Works

This article contains the following topics:

CACF governs inbound CI data before loading the data into the CMDB. This verification ensures that each requested Change Order executes correctly, and detects and manages rogue changes automatically. The Configuration Administrator (CMDB Administrator) defines verification policies. The policies determine how CA SDM responds when any deviation or variance from the requested change occurs.

The following diagram shows how CACF works:

How Configuration Audit and Control Facility Works



1. Inbound CI data loads from Web Services, GRLoader, MDR, or the Web Interface to request an attribute update for a CI.

2. Based on the verification policies that your Configuration Administrator establishes, CACF completes one or more of the following actions:

   - CACF accepts the update and modifies the CI data in the CMDB.

   - CACF defers the update to the TWA for further processing.
     For example, your Change Manager handles transactions in the TWA.

   - CACF creates an Incident and lets you manage the ticket.
     For example, your Incident Management process requires managing the Incident for reporting purposes.

   - CACF rejects the update and the CI data is not changed in the database.

Verification Policy

First the Configuration Manager and the Change Manager agree on a change verification policy. Next, the decisions transcribe into a CA SDM change verification policy. A system can have many verification policies. When a CI update occurs, CACF selects a single verification policy for each updated attribute. The verification policy can update the CI, create a TWA entry, or create an Incident if a matching change specification exists.

Note: To monitor updates through the web client, specify the MDR Class Pattern as **Web Client** (case sensitive) in the policy. This pattern usage applies to English and localized versions of CA SDM when you want to monitor updates through the web client.

Important! Determining what policies you need in your environment requires significant thought into the goals of the organization and how you want to introduce those policies.

Verification Policy Selection

When an update occurs to a CI, CACF selects a policy for each updated attribute. This selection depends on the source of the update, the target CI, and whether matching change specification exists. When multiple policies match, CACF selects the single policy with the lowest sequence number to manage the attribute update.

Note: CACF can select multiple policies to manage a single transaction that updates multiple attributes. For example, updating a CI with a new description and new IP Address can trigger two different policies.

Each policy has four sections that CACF uses in policy selection:

- **Identification and Priority**
  Identifies a policy and specifies the order to evaluate the policy.
- **Change Order Alignment**
  Selects transactions that are based on how closely the attribute update matches an existing change specification.
- **Transaction Filter**
  Specifies the data sources to which this policy applies.
- **CI Filter**
  Specifies the CIs to which this policy applies.

A policy matches an attribute update when it passes each of these filters. If a policy does not match a transaction, CACF bypasses the policy. Next CACF evaluates other policies in the system. If CACF bypasses all policies, the default action lets the CI attribute update occur.

Verification Policy Filter Syntax

To help with establishing generic policies, the Change Order Alignment, Transaction Filter, and CI Filter accept an asterisk as a final pattern character as a wildcard. To indicate negation, use an exclamation point at the beginning of these filters.

Important! Policy pattern rules differ from change specification planned value rules. For policy filters, you cannot use embedded asterisks (*) or the greater than (>) and less than (<) special characters.

Policy filters are case-sensitive for verification policy selection patterns, such as CI Name or CI Class. The filters are case-sensitive even if you define those attributes as case insensitive.

Note: A blank "" (no value is specified in the field) policy filter matches only the blank value. A policy filter that uses an asterisk matches all values.

Consider the following information with the following example verification policies:

- Policy1 selects CIs name(prod*) attribute(IP Address) where a matching change specification exists.
- Policy2 selects CIs name(prod*) attribute(IP Address) where there is a rogue update.
- Policy3 selects CIs name(test*) attribute(Memory Installed) from mdr(Cohesion).
- Policy4 selects CIs name(“”) attribute(Memory Installed).

The following list describes the possible outcomes of these policies:

- When an update to CI(test2) attribute(Memory Installed) occurs, Policy3 manages the update. CACF ignores Policy1 and Policy2.
- When an update to CI(prod3) attribute(Memory Installed) occurs, and a matching change specification exists, Policy1 manages the update.
- When an update to CI(development4) attribute(IP Address) occurs, CACF updates the CI with the new IP address as no matching policy exists.
- When an update to CI(prod1) attribute(Disk Capacity) occurs, no policies for attribute(Disk Capacity) exist. CACF updates the CI with the new value. In this example, CACF does *not* manage the Disk Capacity attribute.

- Policy4 only matches CIs with blank names. Because blank CI names are invalid, the change is never executed.

Verification Policy Prioritization by Sequence Number

When multiple policies match an attribute update, CACF chooses the policy with the lowest sequence number. Consider the following policies and their sequence numbers.

- Policy name(Policy1) sequence(1000) CI(prod*)
- Policy name(Policy2) sequence(2000) CI(prod-NY*)

When an update to CI(prod1) occurs, Policy1 manages the transaction. When an update to CI(prod-NY-1) occurs, Policy1 still manages the transaction as it has a lower sequence number. In this example, Policy2 never takes effect.

We recommend that you change the sequence numbers so that the most specific policy has the lower sequence number. Refer to the following sample policies:

- Policy name(Policy1) sequence(2000) CI(prod*)
- Policy name(Policy2) sequence(1000) CI(prod-NY*)

When an update to CI(prod1) occurs, Policy1 manages the transaction. When an update to CI(prod-NY-1) occurs, Policy2 manages the transaction as it has a lower sequence number.

Change Order Alignment

Policies filter on how closely a CI attribute update matches a change specification. After a CI update, CACF searches for a change specification that matches both the CI and the attribute name. This search can verify the change specification. This Change Order Alignment can occur as follows:

- Change specifications exist for this attribute and CI.
- Change Orders exist for this CI, and those Change Orders do *not* contain change specifications.
- A rogue insert transaction occurs which indicates and new CI. A Change Order does *not* exist with this CI attached to it.
- A rogue update transaction occurs which indicates an existing CI. A Change Order does not exist with this CI attached to it.

Only Change Orders in a state where *change verification is active* are considered when looking for a matching Change Order. Closed, unapproved, unscheduled, or otherwise nonexecuted Change Orders are not considered when searching for a matching Change Order.

After CACF determines the Change Order alignment of a transaction, it performs a search for a corresponding policy. A policy can manage one or more Change Order alignment types:

- **Change Order with Specifications**
  Indicates that a Change Order with a change specification which specifies the updating CI and attribute name exists.

- **Change Orders Without Specifications**
  Indicates Change Orders that specify this updating CI, and those Change Orders do not have any change specifications.

- **Rogue Insert**
  Indicates an inserted CI, by definition, the CI does not have any matching Change Order in a verification state.

  Important! Policies which prevent rogue inserts must specify a managed attribute of *Name* or *All Managed Attribute. Name* specifies an active managed attribute.

  CACF always allows rogue inserts and updates when a transaction only has unmanaged attributes.

- **Rogue Update**
  Indicates an updated CI that has no matching Change Orders in a verification state.

Example Change Order Alignment Policies

The following example policies specify Change Order Alignments:

- Policy name(legacy) filters CI(*) attribute(Any Managed Attribute) alignment(Change Orders Without Specifications) action(Allow Attribute Update)

- Policy name(new) filters CI(*) attribute(Any Managed Attribute) alignment(Change Orders with Specifications) action(Allow Update Only if Matches Change Specification)

- Policy name(no-rogue) filters CI(*) attribute(Any Managed Attribute) alignment(rogue insert or rogue update) action(Always Cancel Entire Transaction, create Incident)

These examples provide the following functionality:

- Policy(legacy) allows CA SDM r12.6 change orders without change specifications to update the CI as they did before a CACF implementation.

- Policy(new) enforces change verification for all new change orders which have matching change specifications.

- Policy(no-rogue) prevents updates to CIs when no Change Orders exist in a Verification Active state.

Transaction Filter

Policies filter transactions that are based on the source of the transaction. The source includes the attribute name, MDR name, MDR class, and role (see page 2637) of the user that performs the update.

Note: If you want to filter users logged on through the web interface only, specify the keyword **Web Client** for the MDR class. The userid of the contact specifies the MDR name. This method of identifying users applies only to verification policies. The method does not appear in any other part of the product.

Example: Transaction Filters

The following example policies specify Transaction Filters:

- Policy name(root_access) filters ci(*) attribute(All Managed Attributes) role(Administrator) action (Allow Attribute Update)
- Policy name (cohesion_not_authorized) filters ci(*) attribute(IP Address) MDRclass(Cohesion) action(Keep Old Attribute Value)
- Policy name(john) filters ci(user1*) attribute(All Managed Attributes) MDRName(user1) MDRClass (Web Client) action(Allow Attribute Update)

These examples provide the following functionality:

- Policy(root_access) lets any user with Administrator access update any value. We recommend this type of policy to have a low sequence number.
- Policy(cohesion_not_authorized) prevents any MDR of MDR class(Cohesion) from updating the IP Address of the filtered CI. This example shows how to prevent an unauthorized MDR from updating data.
- Policy(user1) lets user1 update the CIs that the contact owns, but only when using the web client. This example shows how to provide specific users full control over their data.

CI Filter

Policy filters transactions on the characteristics of the updated CI. This selection criteria includes CI Name, class, priority, service type, and location.

Important! The CI filter is based on the attribute value in the CI before the update occurs. The filter is not based on the value in the inbound transaction data.

Example: CI Filter Policies

The following example policies specify CI Filters:

- Policy name(priority1) filters Service Type(priority1 resolution) action(Allow Update Only if Matches Change Specification, Create Incident)
- Policy name(prod-NY) filters ci(prod*) location(NY) attribute(All Managed Attributes) action(Allow Update Only if Matches Change Specification)
- Policy name(prod-not-NY) filters ci(prod*) location(!NY) attribute(All Managed Attributes) action (Allow Attribute Update)

These examples provide the following functionality:

- Policy(priority1) requires CIs with a service type of *priority1 resolution* to have a matching Change Order. This policy is a best practice because it helps control the most important CIs in the CMDB. This policy also requires verification for all changes under change management to have change specifications. It also requires the changes to be verified and completed.

- Policy(prod-NY) requires CIs in the NY location to have matching Change Orders. Using location to filter policies can help gradually implement change verification on a site by site basis.

- Policy(prod-not-NY) illustrates using the exclamation point in the location pattern to indicate CIs not located in NY.

Policy Actions

After CACF selects a policy, the action section of the policy determines the outcome of the attribute update. This section identifies the most important part of the verification policy because it affects the integrity of the CMDB. This section also affects the change management workflow, related notifications, and created Incidents.

A policy can have one of the following Update Behaviors:

- **Allow Update Only if Matches Change Specification**
  If the CI matches a change specification, conditionally applies the inbound attribute update to the CI. This update occurs when the Change Order is in a Verification Active state. Selecting this option enables change verification.

- **Allow Attribute Update**
  Unconditionally applies the inbound attribute update to the CI. This option effectively disables all change verification. Use this behavior for standard changes, when you have a trusted data source, authoritative, and you do not require a Change Order.

- **Always Cancel Entire Transaction**
  Cancels the update and any other attribute update in this transaction, even if a matching change specification exists. To prevent MDRs from updating CIs where they are not authorized to update, use this behavior. If any policy cancels a transaction, the entire transaction is canceled. The transaction is canceled even if other policies would have allowed the change to occur.
  For example, specify this behavior to stop an unauthorized MDR from inserting a CI. In addition, specify a common attribute name such as *Name*.

- **Keep Old Attribute Value**
  Cancels the single attribute update, but allows other attributes in the transaction to update if their policy allows it. Use this behavior when an MDR is unauthoritative at the attribute level.

A verification policy can specify that Incidents close automatically when failed verifications are remediated. The policy can specify that the inbound transaction data copies to the TWA. This type of policy is useful when data from an unauthorized MDR requires review before updating the CMDB.

To let the Configuration Manager identify that CACF policies that created the TWA record, the Change Order field in TWA is set to the name of the policy that created it. Writing data to TWA is independent of updating the CI in the CMDB, so a policy can update the CI, write to the TWA, or both.

Policy Scheduling

You can specify activation and deactivation dates on verification policies, which let the Configuration Administrator schedule unattended policy changes.

Multiple Policies

As you introduce more verification policies into your environment and more attributes are managed, organizing the policies becomes increasingly complex. More overlaps exist between the policies. For example, you have one policy for Server CIs and another policy for CIs in NY. Consider the appropriate policy for Server CIs in NY. Use the policy sequence number to force one policy to take precedence when multiple policies can potentially control a single attribute. As you manage more attributes, the possibility that more policies manage a single transaction can increase.

Consider the following information when you have multiple active policies for a single transaction:

- If any selected policy requests writing data to the TWA, data also writes to the TWA.
- If any selected policy requests to cancel the transaction, CACF cancels the entire transaction.

Important! Facilities that use the createAsset web service (including GRLoader and CMDBf) break the transaction into three separate transactions. The transactions include two inserts, and an update. Updates to ca_owned_resource can be allowed, while updates to the CI extension table are canceled. Updates to CI family-specific attributes in the extension table may not be detected as inserts, but rather as updates.

Example Multiple Policies

The following examples specify multiple policies:

- Policy name(IP Address) attribute(IP Address) action(Allow Attribute Update)
- Policy name(Memory Installed) attribute(Memory Installed) action(cancel transaction)
- Policy name(Disk Capacity) attribute(Disk Capacity) action(Keep Old Attribute Value)

These examples provide the following functionality:

- If a transaction only updates IP Address, the update is performed.
- If a transaction only updates Memory Installed, the update is not performed.
- If a transaction updates both IP Address and Memory Installed, the transaction is canceled in the web interface.
- If a transaction updates both IP Address and Disk Capacity in the web interface, IP Address is updated, but Disk Capacity is not updated.
- If a transaction updates both IP Address and Memory Installed in the web interface, neither attribute is updated.

Incident Consolidation

When a verification policy requests to create an Incident, CACF can reduce the number of open Incidents as follows:

- CACF creates only one open Incident for a single CI for rogue changes. More rogue changes update the single open Incident for rogue changes.
- CACF creates only one open Incident for each change specification verification failure. More verification failures for the change specification update the open Incident.

How to Define Policies for Change Verification

Contents

To begin using CACF in your CA SDM environment, complete the following recommended steps:

1. Review the Managed Change States in the CA SDM environment. Update the default Managed Change States or add states as necessary to suit your change management strategy. Change verification initiates when the status of a Change Order changes to a Change State that CACF manages. For example, Verification in Progress.

2. Identify the available CI Managed Attributes that you want CACF to manage for change verification.

   - For example, you want to manage changes to Memory Installed (phys_mem) so that the attribute *must* have a matching Change Order for the test* server. You also consider changes to IP Address (alarm_id) as normal and always allowed.

   - For example, you want to manage changes to Memory Installed (phys_mem), MAC Address (mac_address), and IP Address (alarm_id) so that the attribute must have a matching Change Order for prod*. You do not want MDR1 to update IP Address and prefer MDR2 to complete this update. When you have a problem, create an Incident. Closing the Change Order also closes the Incidents automatically.

3. Determine what CIs or subset of the CIs in your system that you want to monitor.
   For example, you want to control all servers name test* and prod*. In addition, you control what CIs based on CI Class and CI Location.

4. Determine what MDRs and sources of data that you want to monitor.
   For example, you want to restrict data from MDR1 for the IP Address attribute from updating any CIs.

5. Determine the appropriate verification policy to manage the following types of change:
   - CI changes that match change orders.
   - CI changes that match the attributes in a Change Order, but do not match the value.
   - CI changes that you consider as rogue updates.
   - CI changes that you consider as rogue inserts.

6. Determine the appropriate update behavior that CACF takes when it detects a variance for a policy:
   - Always allow the attribute update request.
   - Allow the attribute update only when a corresponding change specification is specified for the update.
   - Always cancel the entire transaction.
   - Keep the existing attribute value.
   - Write data to the TWA.
   - Create an Incident when CACF detects a variance.
   - Automatically close any Incidents after Change Order verification.

For more information about change verification planning and implementation, see Planning and Implementing Change Verification (see page 2670).

Change Verification Best Practices

Consider the following best practices when implementing change verification:

- Define a small number of policies.
- Avoid the use of negative logic (exclamation point in a policy pattern).
- A single CI update save must match a small number of policies.
- Organize the policies in a numerically tiered structure.
- Use Log Only Mode policies before you implement a change verification policy.
- Minimize overlapping policies, where multiple policies manage a single attribute being updated.
- Limit the number of Incidents that CACF creates.

- Implement archive and purge of CACF data.

Organizing Policies

You can use several strategies to track policies. We recommend that you use a multi-tier approach. To allow for future inserts, use increments of 100 between policy numbers.

Consider the following example tiers for this strategy:

- **Fundamental Policies**
  100,000-199,999
  - Allow Change Administrators to perform inserts.
  - Disallow the inserts by MDR Class(xxxx).
  - Exclude all test CIs from incident creation.
- **Temporary or Transient Policies**
  200,000-299,999: Bulk loads this week
- Application-Specific Policies
  - 301,000-301,999: Exceptions to the following general application-specific policies:
    For example, server1 in NY policies
  - 311,000-311,999: Policies that relate to Service Type priority1 resolution.
  - 320,000-320,999: Policies that relate to NY.
  - 331,000-331,999: Policies that relate to Lisle.
- Technology-Specific Policies
  - 410,000-410,999: Policies that are related to Servers.
  - 411,000-411,999: Policies that are related to Network.
- **Default Policies**
  You can use these policies if the previous policies do not apply to your environment.
  900,000-999,999: Default policies, such as all updates to managed attributes (Any Managed Attribute) must have a change specification.

Multi-Tenancy Considerations

Consider the following information when using CACF in a multi-tenancy environment:

- Managed attributes, verification policies, Change Orders, and change specifications are tenanted.
- Tenants up their hierarchy can view all CACF objects.
  For example, if a tenant creates a managed attribute, this action may block a tenant in the hierarchy from creating a duplicate managed attribute. The hierarchy requires unique policy sequence numbers.

- To determine the policy that manages a change to an attribute, consider only policies from the tenant hierarchy of the object (CI).
- A subtenant can create a policy that overrides the supertenant by assigning a lower sequence number to their local policy.
- CACF only considers policies at the tenant level and its parents in the hierarchy.
- CACF does not consider the tenant of that contact that performs the change.

Note: Verification policies are specific to your system and do not vary by user or role.

CACF Roles and Functional Access

The following table describes the default roles that CACF uses:

Role/Functional Access	Administration	CI	Incident/Problem/Request	Change Order
Administrator	Modify	Modify	Modify	Modify
Configuration Administrator	Modify	Modify	Modify	Modify
Configuration Analyst	View	Modify	Modify	Modify
Configuration Viewer	None	View	Modify	View
Change Manager	View	Modify	Modify	Modify
Service Desk Administrator	Modify	Modify	Modify	Modify
Service Desk Manager	View	Modify	Modify	Modify
System Administrator	Modify	Modify	View	View
Level 1 Analyst	View	View	Modify	View
Level 2 Analyst	View	Modify	Modify	Modify
Incident Manager	View	View	Modify	Modify
Problem Manager	View	View	Modify	Modify

- **Administration**
  Indicates creating, updating, and viewing CACF administration, policies, and attribute management.
- **CI**
  Indicates creating, updating, and viewing CI and relationship attribute data.
- **Incident/Problem/Request**
  Indicates modifying and viewing outstanding CACF issues, including rogue changes and incorrect change execution variances.
- **Change Orders**
  Indicates creating, updating, and viewing change specifications.

For example, the Change Manager role can view CACF policies and can manage attributes, but cannot update them.

Important! Update access to the Change Order and its status determine who can edit change specifications. For example, the Change Administrator provides this access to the Change Manager.

Example Change Specification in the Pending Verification Status

In this example, the Configuration Administrator established a verification policy for the Memory Installed (phys_mem) attribute to Allow Update Only if Matches Change Specification. CACF monitors a change specification for this attribute with the Verification Pending status. It sets the Change Specification to the Verified or Failed Verification status.

The following steps describe the lifecycle of this change specification:

1. A Change Order requests an update to the Memory Installed (phys_mem) attribute of a CI.
2. You create a change specification for the Memory Installed (phys_mem) Managed Attribute with a Planned Value of 4 GB with the initial status as Verification Pending.
3. The Change Order moves to a status with change verification active such as Verification in Progress.
4. The change specification waits for a discovery tool to discover CI details and export the values to the CMDB.
5. One of the following actions occurs after the discovery tool exports the value to the CMDB:
   - The value for Memory Installed matches the 4gb value that you specified in the change specification. CACF sets the status from Verification Pending to Verified. CACF closes the Change Order.
   - The value for Memory Installed does not match the value that you specified. CACF sets the status from Verification Pending to Failed Verification.

Example Change Specification in the Set After Change Verified Status

In this example, CACF updates the CMDB with the value that you want to use after the Change Order exits a managed change state with change verification active. For example, your environment uses Verification in Progress as the managed change state with change verification active enabled.

The following steps describe the lifecycle of this change specification:

1. A Change Order requests an update to the Serial Number (serial_number) attribute of a CI.
2. You create a change specification, specify Serial Number, and enter a planned value for an attribute.

3. You set the Change Order state to from RFC to Verification in Progress to Closed.

4. The CI attribute value is updated with the planned value after the Change Order exits a state with Change Verification Active (Verification In Progress). The value is updated to a state that does not have change verification active (Closed).

5. The change specification sets to Was Set to Planned Value to indicate that the set was completed successfully.

Accept the Planned Value

In this example, the Change Analyst researches the correct attribute value for a CI and accepts the planned value.

Follow these steps:

1. Open a Change Specification that an end user created in your environment.

2. To see the planned value for the CI attribute that the Change Analyst modified, view the detail page.

3. Research the attribute value for the CI.
   For example, your research indicates that the Change Analyst entered the correct value.

4. To update the CI with the corresponding planned value, click Accept Planned Value.
   CACF sets the state of the Change Specification to Accepted Planned Value.

Accept the Discovered Value

In this example, the Change Analyst determines that the CI is updated to a correct attribute value for a CI and accepts the discovered value.

Follow these steps:

1. Open a Change Specification that a Change Analyst created in your environment.

2. To see the planned value for the CI attribute that the Change Analyst specified, view the detail page.

3. Research the attribute value for the CI.
   For example, discovery indicates that the Change Analyst entered the incorrect value.

4. Click Accept Discovered Value.
   The CI updates with the discovered value. CACF sets the status of the change specification from Verification Pending to Accepted Discovered Value.

5. If you configured the managed state to enable the Promote Change Order After Verification option, CACF closes the Change Order. The closure happens after all change specifications are in a final state.

Manage Changes from an Unauthorized MDR

In this example, the Configuration Administrator established a verification policy to manage changes from an unauthorized MDR named MDR1. The policy rejects all updates to CIs from MDR1.

The following steps describe the lifecycle of this verification policy:

1. You create a Verification Policy with an MDR Name pattern of MDR1 and an Update Behavior of Always Cancel Entire Transaction.
2. Enable all Change Order alignment options.
3. Specify Any Managed Attribute and an asterisk (*) for all filters.
4. When the discovery tool (MDR1) runs and exports the data to the CMDB, the verification policy rejects all the updates.

Managed Attributes

Managed attributes indicate those eligible CI attributes for change verification by CACF. By default, this list contains *CI Name* and *Any Managed Attribute*. You add the CI attributes that you want managed as part of your change verification strategy. Define managed attributes as part of your change verification strategy in the Configuration Control, **Managed Attributes** node in the CA CMDB section of the Administration tab.

CACF does not consider unmanaged attributes (attributes not listed) for change verification. These unmanaged attributes update as usual.

Important! Change verification ignores unmanaged attributes and lets them update the CI, unless a verification policy specifies the Always Cancel Entire Transaction behavior.

Note: Case sensitivity in the managed attribute definition only applies when CACF compares the change specification planned value with the inbound CI transaction data. Case sensitivity does not apply to the selection patterns in the policy, which are always case-sensitive.

For a list of CI attribute names, see *CMDB Technical Reference (see page 4168)*.

Managed Change States

This article contains the following topics:

CACF uses managed change states to indicate which Change Order statuses CACF manages. CACF uses managed change states to control how or when to apply change verification for CI updates made to the system. You can customize these change states to suit the needs of your organization.

You configure managed change states on the Administration tab in the CA CMDB, Configuration Control, Managed Change States node.

The following list describes the Managed Change States options:

- **Change Specifications Editable**
  Specifies whether you can edit the change specifications for a Change Order. Typically, after a change request receives approval, you cannot change the request, and updates are restricted to performing a small set of override options in the *Verification in Progress* state.

- **Change Verification Active**
  Specifies whether changes discovered for a CI while the Change Order is in this status are considered for change verification. Change orders and their related change specifications are compared with any inbound transactions to verify that they were executed successfully.
  CACF monitors all CIs for any changes to their managed attribute values. As CACF verifies each attribute level change to the CI, CACF compares it against a list of change specifications that are in a *change verification active* state.
  After a change specification enters this state, any change specification without a specific CI undergoes expansion. This expansion occurs where new change specifications are created using the list of CIs attached to the Change Order.
  After a change specification exits this state, the list of change specifications with a verify status of *Set After Change Executed* complete. This action updates the CI with the planned values, as specified in each change specification.

- **Implementation State**
  Specifies whether the state represents a state when the changes are being executed or implemented on the CI. When a Change Order enters this transitional state, it is understood that the attribute values in the CI are volatile and may be updated as requested by the pending change specifications. CACF cannot consider these changes rogue changes, but it also cannot consider the changes for final verification. Typically, the change verification process should only compare the inbound attribute data after the Change Order executes completely.

- **Show Change Specification Override Buttons**
  Specifies whether the Change Analyst can control change specifications, and what level of control is given. In some implementations, the Change Analyst can edit change specifications as necessary, while in other implementations, the Change Analyst can override (see page 2657) or cancel (see page 2657) the change specification.

- **Promote Change Order after Verification**
  Specifies whether a Change Order promotes to the next default state automatically after CACF verifies all the change specifications.

Default Managed Change States

You can define Change Order states during which change specifications are created, overwritten, verified, or ignored.

The following list describes the default managed change state definitions that are provided by CA SDM as an example:

- **RFC**
  Define the Change Order specifications in this state, but are not considered during change verification. Changes to the CI detected while the Change Order is in this state are typically considered as rogue.

- **Approval in Progress**
  Change specifications in this state have the same characteristics as RFC and are editable and not considered for verification.
  After Change Order approval, the change specifications are approved as part of the same approval process. CACF prohibits more modifications to the specification and provides full auditing.

- **Implementation in Progress**
  Changes to CIs can occur, but are not considered rogue or used for verification. You may want to change the definition of this change state to let verification occur for Change Orders in this state.

- **Verification in Progress**
  Change specifications cannot be edited, but an analyst can override them. Change verification is active (see page 2654) in this state.

Change Specifications

A Change Order contains change specifications that define the specific CI changes that are requested for a CI. CACF uses these change specifications when the Change Order enters a verification state to validate and confirm that the actual changes to the CI completed correctly. Create change specifications from a Change Order, CI, or the Configuration Control, Change Specifications node the CA CMDB section of the Administration tab.

The change specification contains the following main sections:

- **Change Order Number**
  Specifies the Change Order that requests the change.

- **CI Name**
  Contains the name of the CI that you want to update.
  You can leave the CI Name field blank to imply that the change specification applies to all CIs defined for the Change Order. Use this option when all the CIs for a Change Order use the same managed attribute and planned value. The change specification applies to all CIs that are attached to the Change Order when the change order status moves to a managed change state with change verification active, referred to as expansion.

- **Attribute Name**
  Specifies the name of the managed attribute that you want to update.
  Selecting Any Managed Attribute indicates that any managed attribute can change during the verification of the Change Order. Because you can update multiple attributes in this case, you cannot specify the planned value.

- **Planned Value**
  Indicates the expected value of the attribute after executing the change. After the Change Order moves into a verification state, and the CI updates through the web interface, GRLoader, or Web Services, CACF compares the planned value with the inbound data to determine a match.
  Special characters (see page 2652) can be embedded in the planned value when the exact value is not known.

- **Status**
  Specifies the status of the change specification (see page 2656), such as Verification Pending.

If you do not know the planned value in advance, but the value may change, you can set the status of the change specification to Use Discovered Value. This behavior requires discovery to update the CI before CACF considers the change specification as validated. You require this behavior for numeric fields and SRELs where an asterisk cannot be accepted as a planned value.

To help you with setting the planned value, the Discovered Attribute History tab lists all values that were recently discovered by an MDR, and whether were actually authorized, or loaded into the CMDB. This tab displays the format, case sensitivity, and other information about values so that you can determine an appropriate planned value pattern.

Special Characters

You can embed special characters when you do not know the exact value. Use the asterisk wildcard character to match any number of characters. The pattern *must* match the discovered data in the same sequence, and spaces are significant.

For example, enter *10.*.*.** as the Planned Value to match any IP addresses that begins with *10.* and has two periods that follow any value between the periods.

For example, the inbound server_type value contains Windows 2003 (WIN32) 5.2.Service Pack 2 (Build 3790) Intel x86. To verify this value, specify a planned value of ** Service Pack 2 ** in the change specification.

A word at the beginning of the planned value indicates that the discovered value must start with that value. Similarly, an asterisk at the beginning of the planned value indicates that the discovered value can begin with any value and end with the value specified following the asterisk.

The following table provides examples about how to use the asterisk:

Planned Value	Discovered Value	Match or No Match
a	b	No Match
a	a	Match
a	aba	Match
a	bab	Match
a*	a	Match

a*	ab	Match
a*	ba	No Match
*a	a	Match
*a	ab	No Match
*a	ba	Match

A pattern that begins with an exclamation point results in the negation of the value. You can only use the exclamation point as the first character in the pattern. For example, you cannot use a pattern of 10.!*.*.*.

To compare numeric values that are contained within string values, use greater than (>) or less than (<) as the first character in the planned value. If there is a leading exclamation point, it must be the second character.

Important! CACF ignores leading or trailing nonnumeric values in the discovered value and planned value patterns.

The following table provides examples about how to use the exclamation point, and the greater than and less than symbols:

Planned Value	Discovered Value	Match or No Match
>200	aaa 201 bbb	Match
>200GB	aaa 200 bbb	No Match
>200GB	300 GB	Match
!<200GB	200 Bytes	Match
!<200	200 Bits	Match

If you do not know the planned value in advance, but the value may change, you can set the status of the change specification to Use Discovered Value. This behavior requires discovery to update the CI before CACF considers the change specification as validated. You require this behavior for numeric fields and SRELs where an asterisk cannot be accepted as a planned value.

To help you with setting the planned value, the Discovered Attribute History tab lists all values that an MDR recently discovered, and whether they were authorized, or loaded into the CMDB. This tab displays the format, case sensitivity, and other information about values so that you can determine an appropriate planned value pattern.

Defining Bulk Load

Managing new CIs without first creating a Change Order that requires defining those CIs presents an issue within CMDB environments. Consider the following information when you define a large number of CIs

- Define a special bulk loading policy that allows rogue insert to complete successfully, restricted by userid, MDR, or role.

- Define a special bulk loading policy that reroutes all new CIs to the TWA for verification and later processing. This action also requires the previous special bulk loading policy.

Defining Bulk Changes

Creating identical changes to a large number of CIs, for example, when changing the location for a collection of CIs, with the following steps:

1. Create a Change Order.

2. Define a single change specification which describes the change and leave the CI name blank.

3. Attach all the CIs to the Change Order.

If you do not know the exact details of a change in advance of the implementation, for example, you acquire a new Server and you only know the CI Name, complete the following steps:

1. Create a Change Order.

2. Create a change specification that specifies Any Managed Attribute as the attribute name.

3. Leave the planned value empty, since it is unknown.

4. Move the ticket through the change management process.

5. When the Change Order is in a verification active state, and discovery runs, the inbound CI data loads into the CI (assuming that the policy allows it).

6. When all discoveries for the CI complete, the Change Manager must mark the change specification as verified manually.

Follow these steps when there are many dissimilar changes to many CIs. For example, when moving a collection of servers from one location to another, and also assigning each one a unique IP address.

1. Create a Change Order

2. Create a spreadsheet and list on each row the Change Order number, CI and, the new attribute values. Each row results in a distinct change specification.

3. To create the required change specifications, load the spreadsheet with GRLoader.

4. Promote the Change Order and its change specifications as usual.
   For more information about using GRLoader, see the General Resource Loader (see page 4289) topic.

How Change Verification Occurs

When a user requests a save to a CI, CA SDM searches for applicable change specifications as it searches for all matches. The following information describes an applicable change specification:

- The CI in the change specification is the same as the one that is being saved.
- The Change Order is in a managed change state that is defined with Change Verification Active.
- The attribute in the change specification is the same as the attribute being updated.
- The change specification is active.
- If there are no managed attributes being updated or policy in effect, the save proceeds uninhibited.

If the inbound data values match a change specification exactly, CACF considers the change specification as validated. Depending on the policy, verification closes any Incident that change verification created.

Verification takes place when information from web clients, web services, or GRLoader update the CI. At this time, the Change Order and all underlying change specifications are undergoing verification. After all verification for a Change Order complete, the Change Order can optionally promote to the next Change Order state automatically.

If the inbound data values do not match the values in the change specification, it is considered an incorrectly implemented or failed change. Incidents are created or appended to, depending on the policy.

For example, CA SDM does not find applicable change specifications, but Change Orders exist in a *change verification active* state. These Change Orders specify the target CI and have no change specifications. CACF manages this change by policies which handle *Change Orders without Specifications*.

- If there are no applicable change specifications or Change Orders without specifications, the save operation is considered rogue.
- After all attributes have been processed, any policy that requested the inbound data to write to the TWA triggers.

Managing Change Specifications

After a change is executed or implemented, the Change Order enters a change state that is managed by CACF. The change state is set to *change verification active*. When the Change Order is in this state, CACF reviews all related CI activity. CACF reports the status of each change specification to the scoreboard.

The Change Manager uses the scoreboard to verify that the required changes are correctly executed and to perform any manual verification that is required.

After all verification for a Change Order are complete, the Change Order may optionally be promoted to the next Change Order state (typically closed). In this state all change specifications are automatically marked inactive.

Change Specification Statuses

Change specifications use status to indicate the type of verification to perform and the current state of verification. The status values are also used in the verification log when recording change verification operations during the verification process.

- **Initial Statuses**
  Used when creating a Change Specification to specify the type of verification for CACF to perform. These statuses are not final. The Change Order is not considered verified when change specifications are in either of these statuses.
  Verification Pending -- The change specification has not been verified, or the change is waiting for the CI update.
  Manual Verification will be required -- When the changes for a Change Order are verified, manual verification is required.
  Use Discovered Value -- Copy the discovered value to the CI at verification time, and used when the planned value is not known before verification.
  Set After Change Executed -- Sets a CI attribute to the planned value after verification has completed. Use this status for setting CI attributes when the attribute is not discoverable. For example, set the CI Primary Contact to User1 after a change completes.

- **Final Statuses**
  Indicates a completed change specification and considered as final. When all change specifications enter either of these final states, they are eligible for promotion to the next default state.
  Verified -- The change specification has been successfully verified.
  Was Manually Verified -- The change specification has been manually verified.
  Used Discovered Value -- The CI has been updated with the discovered value.
  Was Set To Planned Value -- The CI has been updated with the planned value after Change Order verification.
  Accepted Planned Value -- The CI has been updated with the planned value and overwritten during verification.
  Accepted Discovered Value -- The CI has been updated with the last discovered value and overwritten during verification.
  No Change -- The planned value matched the CI at verification time and no verification was required.
  Cancel -- The change manager canceled the change specification.

- **Intervention Statuses**
  Indicates that a change specification requires manual intervention for verification. CA SDM highlights these statuses in a red color on list forms. These statuses are not final. The Change Order is not considered verified when change specifications are in either of these statuses.
  Failed Verification -- Discovery found the value to be other than what was specified in the Change Order. The Change Analyst must determine if the change was correctly executed and the Change Order was incorrectly specified. Or, if the Change Order was correct and the change requires verification again. Depending on the definition of the Managed Change State and the current change order status, the Change Analyst can override, change, or cancel the failed change specification.
  Manual Verification Active -- Manual verification is required before the change specification can be marked final.

- **Action Override Statuses**
  Indicates an action to initiate during change verification. These statuses are not final. The Change Order is not considered verified when change specifications are in either of these statuses.
  Accept Planned Value -- Request to override the CI attribute with the planned value.
  Accept Discovered Value -- Request to override the CI attribute with the last discovered value.

- **Reporting Status**
  Indicates the result of policy operations that the verification log displays for logging purposes and not used by change specifications.
  Update Was Allowed -- A policy allowed a request to update a CI and did not match any change specifications.

Managing Failed Verifications

When a verification fails, the CMDB, Configuration Audit, Failed Verifications node in the scoreboard lists the number of failed verifications. The scoreboard also lists the number of change specifications that require manual intervention in red. The Change Specifications can also be viewed under the Change Specifications tab in the Change Order, CI, or Administration tab. Failed verifications have the verify status of "Failed Verification". When a verification fails, the Change Analyst can intervene or wait until the next discovery occurs.

If the managed change state allows the Show Change Specification Override Buttons action, the Change Analyst can open the change specification and review the data. The Change Analyst can click one of the following options to close the verification by moving it to a final state:

- **Accept Discovered Value**
  The Analyst determines that the change specification is incorrect and that the discovery tool has discovered the correct value.

- **Accept Planned Value**
  The Analyst determines that the discovery tool is wrong or has not performed discovery. The Analyst decides to accept planned value, as if it was discovered correctly.

- **Cancel**
  This portion of the Change Order was not executed and this specification was canceled.

Managing Undiscoverable Attributes

When a Change Specification requires manual verification, the Configuration Analyst must manually verify the change. The CMDB, Configuration Audit, Manual Intervention node in the scoreboard shows the number of change specifications that require manual intervention in red. The Change Specifications can also be viewed under the Change Specifications tab in the Change Order, CI, or Administration tab with the verify status of "Manual Verification Active."

If the managed change state allows the Show Change Specification Override Buttons action, the Change Analyst can open the change specification and review the data. The Change Analyst can click one of the following options to close the verification by moving it to a final state:

- **Mark as Verified**
  Used when the attribute is cannot be discovered and manually verified.

- **Cancel**
  This portion of the change order was not executed and this specification was canceled.

How to Archive and Purge Audit Data

We recommend that you archive and purge obsolete Verification Log entries, CACF audit history, and CI audit history as part of database maintenance.

Important! The CACF reports typically present monthly reports with a yearly summary. The default archive purge time for the archive purge rules for the log, CACF audit history, and CI audit history tables is 30 days. Use the same value in the archive and purge rules for verification log entries, Incidents, and Change Orders. Using the same value ensures data consistency. You can probably change the 30-day default to something more in keeping with your reporting requirements.

To archive and purge audit data, complete the following actions:

1. To archive and purge inactive Incidents older than *nn* days, use the current incident rule.
   CA SDM archives and purges verification log entries only after archiving and purging associated Incidents. If you associate a Change order with an Incident, CA SDM does not verify whether the Change Order is active.

2. To archive and purge inactive Change Orders older than *nn* days, use the current Change Order rule.
   CA SDM archives and purges verification log entries and change specifications only after archiving and purging associated Change Orders. If you associated an Incident with a Change Order, CA SDM does not archive and purge the Change Order.

3. Use the Rogue Change Verification Log rule for rogue changes that did not create an Incident. To archive and purge verification log entries older than *nn* days, use this rule. By definition, rogue changes are not associated with Change Orders.

4. Use the CMDB Audit rule to archive information that is shown in the Change Specification History, Verification Policy History, Managed Change State History, and Managed Attribute History tabs. These tabs are shown in the respective Change Specifications, Verification Policy, Managed Change State, and Managed Attributes detail forms. CA SDM stores this information in the ci_audit table.

Implement a Change Verification Strategy

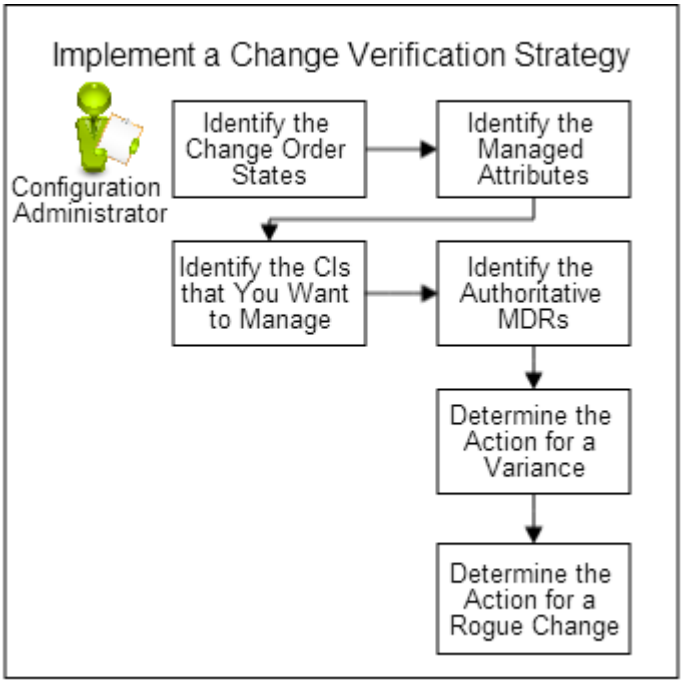
This article contains the following topics:

- Determine the Action for a Variance (see page 2662)
- Determine the Action for a Rogue Change (see page 2662)

The Configuration Administrator determines how aggressively to implement the change verification strategy for your CMDB environment. You identify areas of your Change Management process that require a change verification strategy. These areas include attributes under change control, the Change Order states that indicate that change verification are active, when you can modify change specification, and authoritative MDRs.

For example, you only want to allow updates to the IP Address attribute from MDR1. You also determine the appropriate actions when CACF detects a variance and rogue change.

The following diagram explains how a Configuration Administrator implements a change verification strategy:



1. Identify the Change Order States (see page 2660).
2. Identify the Managed Attributes (see page 2660).
3. Identify the CIs that You Want to Manage (see page 2661).
4. Identify the Authoritative MDRs (see page 2661).
5. Determine the Action for a Variance (see page 2662).
6. Determine the Action for a Rogue Change (see page 2662).

Identify the Change Order States

The Configuration Administrator identifies the Change Order states for when change verification is in effect. The verification happens after a change is executed. Change states help you determine specific conditions, such as if you can edit change specifications in a particular state. For example, you want to review the RFC change state for Change Orders that request updates to CIs.

Follow these steps:

1. On the Administration tab, click CA CMDB, Configuration Control, Managed Change States.
2. To view the change state details or create a Change Order state that has not been already defined, click RFC.

   Note: By default, the RFC Change Order state lets you only edit change specifications. The Implementation in progress state does not let you edit change specifications. The Verification in progress state enables change verification and displays override buttons for the Change Manager or other authorized user.

3. Specify the CACF options and behavior for when a Change Order enters this state.
4. Click Save.

Identify the Managed Attributes

Identify which CI attributes you want to manage for the change verification strategy. For example, you want to manage the IP Address (alarm_id) attribute with change verification.

Follow these steps:

1. On the Administration tab, click CA CMDB, Configuration Control, Managed Attributes.
2. Click Create New.
3. Complete the following steps:
   a. Enter **alarm_id** as the Attribute Name.
   b. Enter **IP Address** as the Attribute Label.
   c. Select an Initial Verify Status from the drop-down list.
      Default: Verification Pending
   d. (Optional) If you want to enforce case sensitivity for change specification planned value comparisons, select the Case Sensitive option.
      Default: Disabled
   e. Click Save.

Identify the CIs that You Want to Manage

Identify the CIs that you want to manage with a verification policy. For example, you want to manage the IP Address (alarm_id) for all high priority CIs with names beginning with NY_Server.

Follow these steps:

1. On the Administration tab, click CA CMDB, Configuration Control, Verification Policies.
2. Click Create New.
3. Complete the following steps:
    a. Enter a sequence, such as **100**.
    b. Enter **NY Server IP Addresses** as the Policy Name.
    c. Select the appropriate Change Order Alignment options.
    For example, you want the verification policy for all options except Change Orders Without Specifications.
4. To specify the transaction and CI filters, complete the following steps:
    a. Select IP Address from the Managed Attribute drop-down list.
    b. Enter a Role Pattern or leave the asterisk to apply to all roles.
    c. Enter **NY** as the Location Pattern.
    d. Enter **NY_Server*** as the CI Name Pattern.
    For example, this filter verifies CIs named NY_Server1, NY_Server2.
5. Select *Allow Update Only if Matches Change Specification* from the Update Behavior drop-down list.
6. (Optional) Use Log Only Mode if you want to experiment with the policy. Also use this mode to view the results only in the standard log, and not affect the active CMDB environment.
7. Click Save.

Identify the Authoritative MDRs

Identify the authoritative MDRs in your CMDB environment. For example, you want to allow updates to CIs from CA Configuration Automation that you identified as MDR1. You consider updates from Web Services that you identified as MDR2 as unauthoritative. You want to send those requests to the TWA.

Follow these steps:

1. Open the NY Server IP Addresses policy, click Edit.

2. Enter **MDR1** as the MDR Name Pattern.
   Note: If you want to exclude an MDR named MDR2, but you want to allow MDR1, MDR3, and so on, enter **!MDR2** as the pattern.

3. Create a separate verification policy, such as MDR2 NY Server.

4. Enter the same information as in the previous policy except the following fields:

   a. Enter **MDR2** as the MDR Name Pattern.

   b. Select *Always Cancel the Entire Transaction* as the Update Behavior.

   c. Select Always from the Write Data to the TWA drop-down list.

5. Click Save.

Determine the Action for a Variance

Determine the action for a variance. For example, a change to a CI does not match the values that are specified in the Change Order. You want the verification policy to create an Incident for the variance.

Follow these steps:

1. Open the MDR2 NY Server policy that you created and click Edit.

2. Select Yes from the Create Incident drop-down list and assign a template.

3. Click Save.

4. An end user creates a Change Order with a change specification to update a CI from MDR2.

5. CACF creates an Incident if MDR2 requests a CI update with a value that does not match the planned value.

Determine the Action for a Rogue Change

Determine the action for a rogue change. For example, CACF detects a change to a CI that does not have any change specifications from any active Change Orders. The Configuration Administrator wants to reject these types of requests.

Follow these steps:

1. Create a verification policy and enter **Rogue NY Server** as the name.

2. Complete the appropriate pattern fields.

3. Verify that only Rogue Insert and Rogue Update are selected as the Change Order Alignment options.

4. Select *Allow Update Only If Matches Change Specification* from the Update Behavior drop-down list.

5. Select Yes from the Create Incident drop-down list and assign a template.

6. Click Save.

Change Verification Notification Messages

The CI detail form displays a notification message when a change is completed. The message indicates whether a change performed in the web interface was successful or unsuccessful. If a change does not complete successfully, a warning message displays with the policy, attribute, and corresponding action. For example, if a user attempts to update a CI but the change was not saved. The reason could be the policy rejected the change when the user attempted to update the CI.

The Verification Log tab also shows details corresponding to the message for future reference.

The notification message indicates the following information:

- Which policy was in effect and corresponding policy action
- Whether a rogue update was detected and if the changes do not match any change orders pending verification
- Whether an Incident was created, updated, or closed, and the corresponding reference number

Examples for Implementing Change Verification

This article contains the following topics:

For Implementing Change verification, consider the following examples:

Example Upgrade Laptops in Your Organization

In this example, an Asset Manager wants to upgrade all laptops from Windows XP to Windows 7 in your organization. The Configuration Administrator creates a verification policy for the Product Version attribute. The verification policy is to filter all laptops with the Windows XP operating system. The Configuration Administrator creates a Managed Attribute definition with the *Use Discovered Value* status, reviews Managed States, and creates a verification policy. CA SDM receives updates to the CMDB from CA Configuration Automation from laptops that require an operating system update. The Asset Management team completes the upgrades.

Follow these steps:

1. Create the following managed attribute:
   - Enter **product_version** as the Attribute Name.
   - Enter **Product Version** as the Attribute Label.
   - Select Use Discovered Value from the Initial Status drop-down list.
   - Enter a label and description for details about the managed attribute.
2. Create the following verification policy:
   - Enter a sequence that you base on other policies in your organization.
     For example, you enter **101**.
   - Enter **Windows* XP*** as the CI Name Pattern.
   - Enter **Workstation** as the Class Pattern.
   - (Optional) Enter a Location Pattern if you want to associate the policy with a specific office in your organization.
   - Select Allow Update Only if Matches Change Specification from the Update Behavior drop-down list.
   - Select Yes from the Create Incident drop-down list.
3. Create a Change Order and change specifications that specify Windows 7 for the Product Version managed attribute for each of the laptop CIs.
4. Move the Change Order to Implementation in Progress status and wait for your Asset Management team to start the upgrades.
5. When the implementations complete, move the Change Order to Verification in Progress.
   CA Configuration Automation discovers laptop information and imports the data in the CMDB.
6. View the open CACF Incidents list for any variances that CACF detected.
7. Select one of the Incidents and review the details about the laptop that CA Configuration Automation discovered.
8. Click Create Change Order and associate the CI with the ticket. Specify change specifications for Product Version for the outstanding changes.
   Wait until discovery verifies that all remaining changes completed.
9. Repeat Steps 6-8 as necessary for any new Incidents that CACF creates.

Example Lock Down Nonverified Change Orders

In this example, the Configuration Administrator wants to only allow a CI update for a matching Change Order. Only CIs in the Server class that is located in NY update for verified Change Orders. Any variance creates an Incident.

Follow these steps:

1. Create a verification policy.
2. Complete the following steps:
    a. Enter a sequence number.
    b. Select Any Managed Attribute as the Managed Attribute.
    c. Enter **NY** as the Location Pattern.
    d. Enter **Server** as the Class Pattern.
    e. Select Allow Update Only if Matches Change Specification as the Update Behavior.
    f. Select Yes from the Create Incident drop-down list.
3. Save the policy.

Example Allow a CI Update If No Matching Change Order Exists

In this example, the Configuration Administrator allows updates for all CIs named test*, even if no matching Change Order exists. This policy accepts updates from all users in an administrative role.

Follow these steps:

1. Create a verification policy.
2. Complete the following steps:
    a. Enter a sequence number.
    b. Select Any Managed Attribute as the Managed Attribute.
    c. Enter **test*** as the CI Name Pattern.
    d. Enter **Administrator*** as the Role Pattern.
    e. Select Allow Attribute Update as the Update Behavior.
3. Save the policy.
4. A user with an administrative role creates a change specification for a CI named test5. The CI updates successfully.

Example Defer All Updates from CA Configuration Automation to the TWA

In this example, the Configuration Administrator wants to defer all CI updates from CA Configuration Automation to the TWA. This policy does not update the CI in CMDB. It writes the data for all rogue changes to the TWA for further evaluation instead.

Follow these steps:

1. Create a verification policy.
2. Complete the following steps:
    a. Enter a sequence number.
    b. Select Any Managed Attribute as the Managed Attribute.
    c. Select Rogue Insert and Rogue Update as the Change Order Alignment.
    d. Enter **CCA** as the MDR Class Pattern.
    e. Select Always Cancel Entire Transaction as the Update Behavior.
    f. Select Always for the Write Data to TWA option.
3. Save the policy.

Example Only Log the Policy Results as a Test

In this example, the Configuration Administrator wants to test a new policy before implementing it in your CMDB environment. The Log Only option lets CACF write the potential CI impacts of the policy to the standard log file.

Follow these steps:

1. Create a verification policy.
2. Complete the information for the alignment, filters, and action.
3. Select the Log Only Mode option.
4. Save the policy.
5. To simulate executing the policy, view the standard log file after you perform CI updates that match the policy specifications and filter criteria.

Example Reject a CI Update

In this example, the Configuration Administrator rejects updates from an MDR named Cohesion for the IP Address (alarm_id) attribute only. This policy does not update the IP address of the CI in CMDB, while it may update other attributes. CACF writes all attributes to the TWA for further evaluation.

Follow these steps:

1. Add IP Address (alarm_id) to the managed attributes list.
2. Create a verification policy.
3. Complete the following steps:
    a. Enter a sequence number.
    b. Select IP Address as the Managed Attribute.
    c. Select Rogue Insert and Rogue Update as the Change Order Alignment.
    d. Enter **Cohesion** as the MDR Pattern.
    e. Select Keep Old Attribute Value as the Update Behavior.
    f. Select Always for the Write Data to TWA option.
4. Save the policy.

Example Allow Change Orders Created Without Specifications

In this example, the Configuration Administrator wants to trust Change Orders that users created without specifications. This policy assumes that the CI text describes all changes accurately and lets the CI update.

Follow these steps:

1. Create a verification policy.
2. Complete the following steps:
    a. Enter a sequence number.
    b. Select Any Managed Attribute as the Managed Attribute.
    c. Select Change Orders Without Specifications as the alignment.
    d. Select Allow Attribute Update as the Update Behavior.
3. Save the policy.

Example Do Not Allow Change Orders Created Without Specifications

In this example, the Configuration Administrator does *not* want to trust Change Orders that users created without specifications. This policy ignores Change Orders without specifications and creates Incidents.

Follow these steps:

1. Create a verification policy.
2. Complete the following steps:

a. Enter a sequence number.

b. Select Any Managed Attribute as the Managed Attribute.

c. Select Change Orders Without Specifications as the alignment.

d. Select Always Cancel Entire Transaction as the Update Behavior.

e. Select Yes from the Create Incident drop-down list and select an Incident template.

3. Save the policy.

Example Allow Rogue Inserts from Selected Sources

In this example, the Configuration Administrator wants to allow new CIs from selected sources. The z /OS MDRs can create CIs without requiring a Change Order.

Follow these steps:

1. Create a verification policy.
2. Complete the following steps:

   a. Enter a sequence number.

   b. Select Any Managed Attribute as the Managed Attribute.

   c. Select Rogue Insert as the alignment.

   d. Enter **z/OS** as the MDR Class Pattern.

   e. Select Allow Attribute Update as the Update Behavior.

3. Save the policy.

Example Allow a Rogue Update for a Nonproduction CI

In this example, the Configuration Administrator allows updates to the IP Address attribute from the Spectrum MDR, but the name cannot begin with *PROD*.

Follow these steps:

1. Create a verification policy.
2. Complete the following steps:

   a. Enter a sequence number.

   b. Select IP Address (alarm_id) as the Managed Attribute.

   c. Select Rogue Update as the alignment.

   d. Enter **!PROD*** as the CI Name Pattern.

e. Enter **Spectrum** as the MDR Class Pattern.

f. Select Allow Attribute Update as the Update Behavior.

3. Save the policy.

Example Allow Rogue Updates Only From a Specific Location

In this example, server CIs in your New York office require repair. The vendor that repairs your servers also resides in New York. The Asset Manager requires that your organization ships all defective servers to New York. The Configuration Administrator wants to allow rogue updates to the CIs when the hardware arrives in New York. The Configuration Administrator creates a verification policy for the Maintenance Vendor attribute. This policy lets a Service Desk Analyst in New York verify that the vendor receives the servers.

Follow these steps:

1. Create the following managed attribute:
   - Enter **vendor_repair** as the Attribute Name.
   - Select verification pending from the Initial Status drop-down list.
   - Enter **Maintenance** as the label and description for details about the managed attribute.
2. Create the following managed change status:
   - Enter **Vendor Hold** as the Change Order Status.
   - Enable the Change Verification Active option.
3. Create the following verification policy:
   - Select Rogue Insert and Rogue Update as the change order alignments.
   - Enter a sequence number for the policy.
     For example, you enter **201**.
   - Enter **server*** as the CI Name Pattern.
   - Enter **Server** as the Class Pattern.
   - Enter **New York** as the Location Pattern.
   - Select Allow Attribute Update from the Update Behavior drop-down list.
4. The Service Desk Analyst creates a Change Order and change specifications for the server CIs and specifies New York for the location.
5. The Service Desk Analyst sets the Change Order Status to Vendor-Hold.

6. The Service Desk Analyst updates the location for the server CIs as New York.
   For example, defective servers from the Chicago office ship to New York. The Service Desk Analyst verifies that the servers arrived in New York.

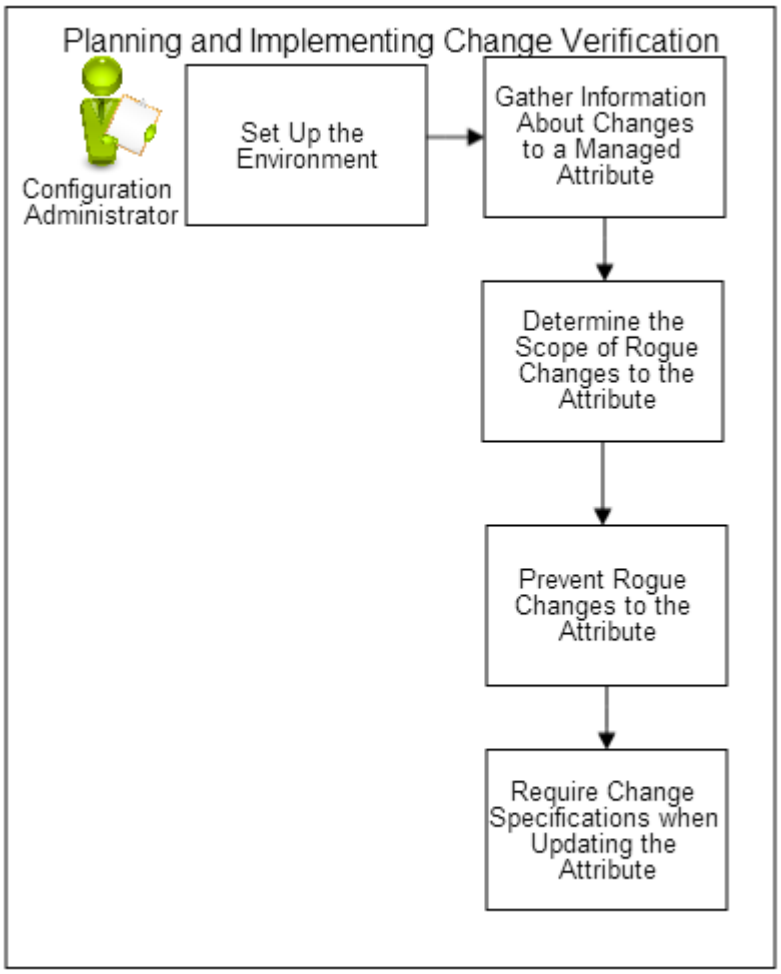
7. The Service Desk Analyst enters the vendor information in the CI.
   The Change Order closes after all the CI locations are set to New York and all the change specifications are verified.

Planning and Implementing Change Verification

The Configuration Manager wants to implement change verification so that the CMDB contains correct data. The Change Manager wants to ensure that changes execute correctly. The Change Manager wants to track the number of rogue changes that occur and their data sources. Both managers agree implementing change verification provides significant value to the organization. The Change Manager wants to ensure that changes do not harm the production environment.

The Configuration Manager and the Change Manager agree to a conservative-phased implementation. The Configuration Administrator implements policies for specific locations and specific CIs in those locations. This scenario describes example phases about completing the verification policy implementation to a broader audience for your organization.

The following diagram shows how a Configuration Administrator completes the example phases to implement change verification:



Follow these steps:

1. Set Up the Environment (see page 2671).
2. Gather Information About Changes to a Managed Attribute (see page 2672).
3. Determine the Scope of Rogue Changes to the Attribute (see page 2673).
4. Prevent Rogue Changes to the Attribute (see page 2674).
5. Require Change Specifications when Updating the Attribute (see page 2675).

Set Up the Environment

You set up the environment so that Configuration Administrators can always update CIs. The Configuration Administrator can create and update CIs in the CMDB as needed, without specifying a change order. The Configuration Administrator is trusted to provide correct CI data.

Follow these steps:

1. Create a verification policy that is named **Policy0.1** with the following information:
   - Enter **1** as the sequence.
   - Enter **Allow Administrator to Always Update CIs** as the description.
   - Select all Change Order Alignment options.
   - Enter **Configuration Administrator** as the Role Pattern.
   - Enter **Web Client** as the MDR Class Pattern.
   - Enter an asterisk (*****) as the CI Name and Class, and all other patterns.
   - Select Any Managed Attribute for the Managed Attribute.
2. Select Allow Attribute Update as the Update Behavior action.
3. Click Save.
   The policy is enabled to only allow Configuration Administrators to update CIs always.

Gather Information about Changes to a Managed Attribute

You want to gather information about changes to a specific CI-managed attribute. The change information helps you identify the CIs that are being updated, the source of the changes, and the specified values. This information helps when defining a verification strategy for the attribute and corresponding CIs. For example, you want to understand the scope of all changes to IP Address (alarm_id) and log this to the CA SDM standard log (stdlog). Gathering this information can take several weeks, depending on the number of changes to attributes that occur in your organization.

1. Define IP Address (alarm_id) as a Managed Attribute.
2. Define Implementation in Progress and Verification in Progress as Managed Change States in your environment. Enable Change Verification Active in both states.
3. Create a verification policy that is named Policy1.1with the following information:
   - Enter **3000** as the Sequence.
   - Enter **Log All Changes to IP Address** as the description.
   - Select all Change Order Alignment options.
   - Enter an asterisk as the CI Name and Class and all other patterns.
   - Enable Log Only Mode.
4. Click Save.
5. After a few weeks, review the stdlogs to view the sources of the updates.
   For example, the log displays rogue CI updates and updates with matching Change Orders.

6. You determine that users located in NY have been updating the IP Address of CIs without creating Change Orders.

7. After you complete your analysis, inactivate Policy1.1 by editing the policy and setting Active? to Inactive.

Determine the Scope of Rogue Changes to the Attribute

You want to determine the scope of rogue changes to the IP Address attribute. Knowing the scope of rogue changes helps you understand the impact of rogue changes on your organization. For example, based on your previous analysis using the Log Only option, you want to create Incidents whenever a change occurs to IP Address to CIs that begin with "test" located in NY without a Change Order. To ignore new Incidents that this process creates, communicate with Change Managers in your organization.

Follow these steps:

1. Complete the following initial implementation actions:

   - Define Implementation in Progress as a managed change state and enable the Implementation State option.
   - Define Verification in Progress as a managed changes state and disable the Promote Change Order After Verification option.
   - Define IP Address (alarm_id) as a Managed Attribute if not already defined.

2. Create a verification policy that is named Policy2.1 with the following information:

   - Enter 3001 as the Sequence.
   - Enter a description about this policy. For example, you enter **Rogue inserts and rogue updates cause Incidents to be created. All other changes are not impeded**.
   - Select Rogue Inserts and Rogue Updates as the alignments.
   - Select IP Address from the Managed Attribute drop-down list.
   - Enter **test*** as the CI Name and **NY** as the Location and an asterisk for all other Patterns.
   - Select Allow Attribute Update, Yes to Create Incident, and an Incident Template from the actions.

3. Click Save.
   After you complete this phase, CACF creates Incidents for all computers in NY. You discover the following information after reviewing the Incidents:

   - Several MDRs report different IP addresses for the same CI.
   - Some MDRs are authoritative, other MDRs are not authoritative.
   - Some CIs cannot be managed based on Location, Family, Name, Service Type, and so on.

4. The Change Manager meets with other IT Managers to review the CMDB, CI detail forms, verification logs, and filtering by attribute name to see the rogue data.

5. Your organization decides to update the CI filter in Policy 2.1 to manage Priority 1 Servers only.

Prevent Rogue Changes to the Attribute

You want to prevent rogue changes to the IP Address attribute to ensure CMDB data integrity. You want to require a Change Order for the update. The Change Order must specify the CI. However, a change specification is not required for the IP Address for the change to occur. Change verification occurs at the CI/Change Order level but not at the attribute level. For example, prevent any rogue updates to and use Incident creation to track the users that request these changes.

Follow these steps:

1. Set Policy1.1 and Policy2.1 to Inactive to disable these policies so that they are not in effect.

2. Create Policy 3.1 with the following information:

   - Enter **3100** as the Sequence.
   - Enter **Prevent rogue changes without any Change Order** as the description.
   - Select Rogue Update as the alignment.
   - Enter **test*** as the CI Name and **NY** as the Location and Any Managed Attribute. Enter an asterisk for all other patterns.
   - Select the Always Cancel Entire Transaction action.

3. Click Save.

4. Create Policy3.2 with the following information:

   - Enter **3200** as the Sequence.
   - Enter **Require a Change Order for IP address changes** as the description.
   - Select Change Orders Without Specifications as the alignment.
   - Enter **test*** as the CI Name and **NY** as the Location and an asterisk for all other patterns.
   - Select IP Address from the Managed Attribute drop-down list.
   - Select Allow Attribute Update as the action.

5. Click Save.
   This policy eliminates rogue changes, because Change Orders must accompany the change. With this policy, the Configuration Manager prevents data that is not defined in the Change

Order being updated. For example, requesting a change to increase Memory Installed while changing the IP Address simultaneously, would not be considered a rogue change because there is a Change Order. They also would like the Change Orders to be automatically verified and promoted and determine they want verification at the attribute level.

Require Change Specifications when Updating the Attribute

Your Configuration Manager may be concerned that the CMDB is updated multiple times although changes are not specified in the Change Order. For example, a user changes the value of Memory Installed (phys_mem) and IP Address (ip_address) simultaneously. In the previous phase, CACF does not consider this request as a rogue change because a Change Order exists.

The Configuration Manager wants to enforce change verification at the attribute level. The Configuration Administrator creates a policy with the following requirements:

- Use change specifications when updating IP Address.
- If no rogue update is attempted, create an Incident.

Follow these steps:

1. The Configuration Manager contacts Change Analysts that changes to IP Address must contain a change specification.
2. Set Policy3.1 and Policy3.2 to Inactive to disable these policies so they are not in effect.
3. Create Policy4.1 with the following information:
   - Enter **4000** as the Sequence.
   - Enter **Require Change Specifications for IP Address changes** as the description.
   - Select Rogue Insert, Rogue Update, and Change Orders Without Specifications as the alignment.
   - Enter **test*** as the CI name and **NY** as the Location, and an asterisk for all other patterns.
   - Select IP Address from the Managed Attribute drop-down list.
   - Select Always Cancel Entire Transaction as the action.
4. Click Save.
5. Create Policy4.2 with the following information:
   - Enter **4100** as the Sequence.
   - Enter **Require Change Specifications for IP Address changes** as the description.
   - Select Change Orders With Specifications as the alignment.
   - Enter **test*** as the CI Name and **NY** as the Location pattern.

- Select IP Address from the Managed Attribute drop-down list.
- Select Allow Update only if Matches Change Specification as the action.

6. Click Save.

You have successfully completed the appropriate example phases to implement change verification in your environment. You can expand the change verification strategy to include more attributes, CIs, MDRs, and tenants.

Verify a CI Attribute Value Update Manually

The Configuration Administrator determines that your CA SDM environment requires a verification policy for the Memory Installed (phys_mem) attribute. The Configuration Administrator creates a Managed Attribute definition with the *Manual Verification will be required* status. This status is appropriate because CA SDM does not have an MDR to discover the value. The Configuration Administrator reviews the managed states and creates a verification policy. The Change Manager views a Change Order that requests an update to the Memory Installed value of a CI. This change request requires manual verification.

Follow these steps:

1. Create a Managed Attribute definition (see page 2676).
2. Review the Managed Change states in your environment (see page 2677).
3. Create a Verification Policy for the Managed Attribute (see page 2677).
4. Review the Change Specifications list (see page 2678).
5. Accept the Planned Value (see page 2679).

Create a Managed Attribute Definition

The Configuration Administrator creates a Managed Attribute definition for the Memory Installed (phys_mem) attribute.

Follow these steps:

1. On the Administration tab, click CA CMDB, Configuration Control, Managed Attributes.
2. Click Create New.
3. Enter **phys_mem** as the attribute name.
4. Enter **Memory Installed** as the Attribute Label.
5. Select *Manual Verification will be required* from the Initial Verify Status drop-down list.
6. (Optional) Select the Case Sensitive option to enforce case sensitivity for change specification planned value comparisons.
   Default: Disabled

7. Click Save.
   The Managed Attribute is saved.

Review the Managed Change States in Your Environment

The Configuration Administrator reviews the Managed Change States in the CA SDM environment. Change verification initiates when the status of a Change Order changes to a Change State that CACF manages. For example, Verification in Progress.

> **Note:** The Configuration Administrator can modify which state in the Change Order lifecycle initiates change verification. The administrator can also modify which states allow you to modify change specifications when implementation starts.

Follow these steps:

1. On the Administration tab, click CA CMDB, Configuration Control, Managed Change States.
2. Click Implementation in Progress to open the managed status detail page.
3. Review the details about the managed status.
   For example, you make the Implementation in Progress status allow editing change specifications, and also enable Change Verification Active. This example indicates an active change verification process. It also indicates that you can edit values when the Change Order sets to the Implementation in Progress status.

Create a Verification Policy for the Managed Attribute

The Verification Policy specifies the CACF action when an MDR discovers an attribute value. The MDR attempts to update the CMDB with that data.

Follow these steps:

1. On the Administration tab, click CA CMDB, Configuration Control, Verification Policies.
2. Click Create New to open the detail page.
3. Enter **1000** as the policy Sequence.

   > **Note:** You can enter a higher or lower number, which is based on other verification policy priorities in your environment.

4. Enter a Policy Name, such as **RAM Management** and a brief description of the policy.
5. Select Rogue Insert and Rogue Updates under Change Order Alignment.

6. You can configure the policy to prevent a specific MDR from updating the Memory Installed (phys_mem) attribute.
   Complete the following tasks:

   - Select Memory Installed as the Managed Attribute.
   - Enter a Role Pattern or use an asterisk to apply to all roles.
   - Enter a CI Name Pattern or use an asterisk to apply to all CIs.
   - Enter a Class Pattern or use an asterisk to apply to all classes.
   - Select Keep Old Attribute Value as the Update Behavior.

   - **Note:** To allow updates to this attribute from a web interface user, enter Web Client as the MDR Name Pattern.

7. Click Save.

Review the Change Specifications List

A Change Order with an RFC status wants to change the value of the Memory Installed (phys_mem) attribute in a CI named server1. The Change Manager sets the verification status of the Change Specification to *Manual Verification will be required*. The Change Manager can view the Change Specification in CA SDM.

Follow these steps:

1. The Change Manager moves the Change Order from RFC to Verification in Progress.
   All the change specifications with Manual Verification become Manual Verification Active.

2. From the Change Order, select the Change Specifications tab from the Configuration Management tab.
   The tab highlights all change specifications in red to indicate that manual verification is required.

   Note: You can also view change specifications from the Administration tab when you click CA CMDB, Configuration Audit, Change Specifications. Additionally, view change specifications from a CI after you select the Change Specifications tab from the Related Tickets tab.

3. Search for change specifications with *requires manual verification* as the Verify Status.
   For example, change specifications of Change Order 21 contain this status.

4. Research the appropriate value for the Memory Installed attribute for the server1 CI.

Note: Change specifications that failed verification also display in red to help show change specifications that require further attention.

Accept the Planned Value

The Change Manager researches the correct attribute value for the CI and makes the appropriate decision on the change request.

Follow these steps:

1. Open the Change Specification to view the detail page.
2. You research the specific Memory Installed (phys_mem) attribute for CI and confirm the planned value.
3. Verify that the Change Order of the Change Specification is in Verification in Progress State.
4. Click Accept Planned Value.
   The Verify Status changes to Accepted Planned Value.

Note: After you click Accept Planned Value, the CI updates with the Planned Value automatically.

MDR Management

This article contains the following topics:

The MDR Launcher is an open integration tool that lets you view data in a management data repository (MDR) from a CMDB web page. MDR Launcher lets you obtain additional details about a CI and to gain control over it (if the MDR supports such control).

Manage Federated CI Mappings

A single CI can be associated to multiple MDRs, with each MDR having a federated_asset_id that identifies the CI. While it is not necessary for the federated_asset_id to be unique among MDRs, a federated_asset_id must be unique within each MDR.

Each MDR is identified uniquely by its combination of MDR class and MDR name.

To view the CI in a particular MDR context, click Launch. The target MDR is launched in the context of the CI that was open.

View an MDR Location for a CI

You can display the MDR location for a CI.

- **CI Name**
  Identifies the configuration item.
- **Federated Asset ID**
  Specifies the string that the source MDR uses to identify this CI. The MDR software typically determines this identifier. CMDBf Viewer uses the UUID.
- **MDR Name**
  Identifies the MDR.
- **Active**
  Denotes whether this mapping is active or not. You can inactivate mappings but not delete them.

Create MDRs

Before you can associate a CI with an MDR, define the MDR to CA SDM.

Follow these steps:

1. Click Create New on the MDR List.
2. Enter the definition (see page)for the new MDR.
3. Click Save.

Note: When you associate a CI with an MDR, the Add MDR button does not appear until the CI is first saved and then edited.

MDR Defintion

You can create, view, and edit an MDR definition. The MDR Definition page provides the following settings:

- **Tenant**
  Identifies the tenant owner of this MDR (if multi-tenancy is installed).
- **Button Name**
  Defines the MDR button label that appears on the CI Detail page. This name is unique for each MDR. Required for “launch in context” and for CMDBf Viewer.

- **MDR Name**
  Specifies the data that is sent in the mdr_name field in XML. While this string can be anything that the MDR chooses to send to CMDB, typically it is the hostname of the source. This name together with the mdr_class create a unique name for the MDR. Note: CA APM MDRs must specify an MDR name of APM and MDR class of GLOBAL. Required for “launch in context", CMDBf Viewer and GRLoader.

- **MDR Class**
  Specifies the data that is sent in the mdr_class field in the XML. While this name can be anything, it must together with the mdr_name field create a unique identifier for the MDR. Global MDRs are defined with an MDR Class of “GLOBAL”. Note: Cohesion MDRs must specify an MDR class of COHESION, which automatically sets the Path, Parameters and "URL to be Launched" fields to the required Cohesion launch-in-context values. CA APM MDRs must specify an MDR class of "GLOBAL", which automatically sets the Path, Parameters and "URL to be Launched" fields to the required CA APM launch-in-context values. Required for CMDBf Viewer. CMDBf Endpoint sets to "cmdbf" for all federated MDRs.

- **Active**
  Denotes this MDR definition as active or inactive. Inactive MDR definitions are logically deleted, but they can be made active again by using the Search utility.

- **Owner**
  Denotes the contact responsible for this MDR.

- **Description**
  Specifies text field.

- **Hostname**
  Specifies the host name, DNS name or IP address of the host, which contains the web server which hosts the web page that is launched. Required for “launch in context”.

- **Port**
  Specifies the TCP/IP port used by the MDR web server to serve up web pages. Port 8080 is the default. Required for “launch in context”.

- **Path**
  Specifies the portion of the URL that precedes the question mark (?) character. This information can be obtained from the MDR documentation. For mdr_class of Cohesion, the value is set automatically to CAisd/html/cmdb_cohesion.html and cannot be changed. For mdr_name of UAPM and mdr_class of GLOBAL, the value is set automatically to apm/frmObject.aspx and cannot be changed.

- **Parameters**
  Specifies the portion of the URL that follows the question mark (?) character. This information can be obtained from the MDR documentation. For mdr_class of Cohesion, the value is set automatically to hostname={hostname}+port={port}+family={family}+name={name}+secret={password}+federated_asset_id={federated_asset_id} and cannot be changed. For mdr_name of UAPM and mdr_class of GLOBAL, the value is set automatically to ObjectID={cmdb_asset_id} &obj=11&FUNCTION=1&WinID=OBFRASSET{cmdb_asset_id}&WinContainerID= and cannot be changed.

- **Userid**
  Specifies the user ID to logon to the MDR (if necessary). This value is substituted into the URL wherever {userid} is found.

- **Shared Secret**
  Specifies information that is shared between CMDB and the MDR. This value is substituted into the URL wherever {password} is found. For Cohesion MDRs, the value must match the value of the “com.cendura.security.oneclickauth.secret”. Required for CMDBf Viewer.

- **CMDBf Namespace**
  Specifies the MDR namespace that is passed to the query by CMDBf Viewer. If you use CMDB as an MDR provider, the value is "http://cmdb.ca.com/r1". For external MDRs, consult the MDR documentation. Required if MDR Class is cmdbf.

- **CMDBf Timeout**
  (Optional) Specifies time limit for CMDBf endpoint query. Default is ten (10) seconds. Only applies when MDR Class is cmdbf.

- **URL to be Launched**
  Default value of *http:///{hostname}:{port}/{path}?{parameters}*. For some MDRs, it can be overridden if necessary to accommodate MDR-specific requirements. Required for "launch in context".
  For mdr_name of UAPM and mdr_class of GLOBAL, the value is *http:///{hostname}:{port}/{path}?{parameters}*
  For mdr_class of Cohesion the default value is: *http://cmdb_hostname:cmdb_port/{path}?{parameters}*

  where
  cmdb_hostname is the host name, DNS name or IP address of the CMDB web server. Defaults to the current hostname that is currently accessing the CMDB web server.cmdb_port is the TCP/IP port of the CMDB web server. Defaults to the current port number used to access the CMDB web server.If you have enabled SSL support for Cohesion, set the URL to:*http://hostname:port/{path}?{parameters}+https=yes*

- **CMDBf Endpoint**

  Specifies the MDR Query Service endpoint for CMDBf Viewer. Required if MDR Class is cmdbf.

Using the Configuration Control

Contents

Under the Configuration Control node in the Administration tab, view and manage CACF Managed Attributes, Managed Changes States, and Verification Policies. Change verification governs inbound CI data before loading the data into the CMDB. This verification ensures that each requested Change Order executes correctly, and detects and manages rogue changes automatically. Change verification lets you perform the following tasks:

- **Authoritative MDR Updates**
  Specifies that MDRs can only update authoritative attributes at the attribute level.
- **Rogue Change Detection**
  Detects and manages updates to CIs when no corresponding Change Order exists.
- **Change Verification**
  Provides automated verification that Change Orders executed correctly.

Change verification policies can be implemented dynamically or scheduled in advance. They can be generic or highly specific.

Managed Attributes

The managed attributes indicate those eligible CI attributes for change verification by CACF. By default, this list contains *CI name* and *Any Managed Attribute*. You add the CI attributes that you want managed as part of your change verification strategy. For more information about establishing a change verification strategy, see the Implement a Change Verification Strategy topic.

CACF does not consider unmanaged attributes (attributes not listed) for change verification. These unmanaged attributes update as usual. Selecting Any Managed Attribute as the Attribute Name in a verification policy or change specification applies to all managed attributes.

Case sensitivity in the managed attribute definition only applies when CACF compares the change specification planned value with the inbound CI transaction data. Case sensitivity does not apply to the selection patterns in the policy, which are always case-sensitive.

By default, CACF manages the CI *Name* attribute to enable rogue insert rejection. If you inactivate *Name* from the managed attributes list, executing a transaction that inserts a CI but does not update any managed attributes is considered an unmanaged change. So, inactivating may cause CACF verification policies to ignore rogue inserts.

For a list of CI attribute names, see the *CA CMDB Technical Reference Guide*.

Create a Managed Attribute

Add managed attributes to use change verification in your environment. For example, the Configuration Administrator wants to enable change verification for a specific CI attribute and requires to define change specifications when updating a CI.

The Managed Attribute History tab shows the audit history. The audit history lists all previous modifications to the managed attribute options with the time and user that changed.

Follow these steps:

1. On the Administration tab, click [set the cmdb value at the book level], Configuration Control, Managed Attributes.
   The Managed Attribute List page appears.

2. Click Create New.
   The Create New Managed Attribute page appears.

3. Enter a valid CI attribute name. For information about attribute names, see the *CA CMDB Technical Reference Guide*. You can also use grloader -sc xxxxx (where xxxx indicates the class name) to list attribute names for a particular class.

4. Enter an attribute label.

5. Select the default Initial Status from the drop-down list of the verification criterion. When you select a managed attribute when creating a change specification, this status is used as the initial default value.

   - **Manual Verification will be required**
     Indicates that this verification requires a Configuration Administrator to verify that the change completed successfully.

   - **Set After Change Executed**
     Indicates that the planned value from the change specification sets in the CI after CACF verifies and completes the Change Order. This set operation only occurs when the Change Order moves from a state with change verification active to nonactive. For example, the set takes place when a Change Order moves from Verification in Progress to Closed. The set does not occur if the Change Order is canceled, demoted, or moved to another state.

   - **Use Discovered Value**
     Indicates that the Configuration Administrator uses the discovered value regardless of the planned value in the change specification. The original value in the verification criterion remains unchanged, but updates the CI attribute with the new value.

   - **Verification Pending**
     Indicates a pending verification.

6. Set the managed attribute as Active or Inactive to remove the attribute from being considered by CACF.

7. Enter a description for the managed attribute.

8. Enable the Ignore Case option if you want the comparisons between the discovered and planned values to remain case insensitive.

9. Click Save.
   The managed attribute is saved.

Managed Change States

CACF uses managed change states to indicate which Change Order statuses CACF manages. CACF uses managed change states to control how or when to apply change verification for CI updates. You can customize these change states to suit the needs of your organization.

The Change Order statuses represent changes that can be edited. Similarly, Change Order change states represent verification states. By default, you can edit change specifications for a Change Order in the RFC change state. The change verification occurs for a Change Order in the Verification in Progress state. Optionally, change tickets can be automatically promoted or closed when all associated change specifications execute successfully.

The following list describes the Managed Change States options:

- **Change Specifications Editable**
  Specifies whether you can edit the change specifications for a Change Order. Typically, after a change request receives approval, you cannot change the request. The updates are restricted to performing a small set of override options in the *Verification in Progress* state.

- **Change Verification Active**
  Specifies whether changes discovered for a CI while the Change Order is in this status are considered for change verification. Change orders and their related change specifications are compared with any inbound transactions to verify that they were executed successfully.
  CACF monitors all CIs for any changes to their managed attribute values. As CACF verifies each attribute level change to the CI, CACF compares it against a list of change specifications which are in a *change verification active* state.
  After a change specification enters this state, any change specification without a specific CI undergoes expansion. This expansion occurs where new change specifications are created using the list of CIs attached to the Change Order.
  After a change specification exits this state, the change specifications with a verify status of *Set After Change Verified* execute. This action updates the CI with the planned values, as specified in each change specification.

- **Implementation State**
  Specifies whether the state represents a state when the changes are being executed or implemented on the CI. When a Change Order enters this transitional state, assume that the attribute values in the CI are volatile. CACF cannot consider these changes rogue changes, but it also cannot consider the changes for final verification. Typically, the change verification process only compares the inbound attribute data after the Change Order executes completely.

- **Show Change Specification Override Buttons**
  Specifies whether the Change Analyst can control change specifications, and what level of control is given. In some implementations, the Change Analyst can edit change specifications as necessary. In other implementations, the Change Analyst can override or cancel the change specification.

- **Promote Change Order after Verification**
  Specifies whether a Change Order promotes to the next default state automatically after CACF verifies all the change specifications.

Create a Managed Change State

Create a managed change state for your change verification environment. For example, the Change Administrator wants to create the Approval In Progress state and set the verification to active.

The Managed Change State History tab shows the audit history that lists all previous modifications to the managed change state options. The tab also shows any previous values and the users that specified them.

Follow these steps:

1. On the Administration tab, click CA CMDB, Configuration Control, Managed Change States.
   The Managed Change States List page appears.

2. Click Create New.
   The Create New Managed Change State page appears.

3. Enter a Change Order status, such as **Approval in Progress**.
   You can also click Change Order Status to search for a status.

4. Select the option to set the change state as Active or Inactive.

5. (Optional) Select any of the following change states:

   - **Change Verification Active**
     Enables change verification for this change state.

   - **Implementation State**
     Indicates that the Change Order is in an implementation phase.
     Use this option to prevent unwanted Incident creation for incomplete Change Orders. For example, CACF detects a rogue change where the change matches the CI and attribute names of a change specification. The verification policy states to only update if the change matches. You can reject this change because the Change Order is verified after fully implemented and moved to a verification state.

     You cannot use a managed change state as both as an active change verification and an implementation state.

   - **Change Specifications Editable**
     Indicates that you can edit change specifications in this state.

   - **Show Change Specification Override Buttons**
     Displays the override buttons when a change verification is active. However, editing such as Accept Discovered Value, Accept Planned Value, Mark As Verified, and Cancel is not allowed.

   - **Promote Change Order After Verification**
     Promotes the Change Order to the next state automatically after change specifications move to a verified or final state.

> Promotion only occurs when the Change Order is in a state with change verification active.

6. Click Save.
   The managed change state is created and saved.

Verification Policies

Verification policies specify the action that CACF takes when an MDR discovers an attribute value, and the MDR attempts to update the CMDB with that data. A variance occurs when the inbound data does not match the desired state information, as described in the change specification. A policy search executes to locate a policy that matches both the change order alignment and change specifications. Policies process in an ascending, sequential number order. By default, a compatibility policy lets all updates occur providing the behavior observed in previous releases of CA Service Desk Manager.

The change verification policy describes how CA Service Desk Manager responds to the following events:

- **Updates from Unauthorized MDRs**
  Specifies that specific MDRs are authoritative for specific attributes. CI attribute updates from unauthorized MDRs can be selectively accepted or rejected.
  For example, define policies to prevent CA Configuration Automation from updating the IP address of a CI, even if a matching Change Order exists. Allow updates to the IP address to occur only if the source MDR is Spectrum.

- **Rogue Changes**

Detects and manages updates to CIs when no corresponding Change Order exists. Specify a policy that manages rogue changes that request inserts or updates of CI data. For example, you can define a policy that loads data into TWA and does not update the CI for the following conditions:

- - A CI named similar to server* in New York changes
  - The change does not have a matching Change Order

- **Incorrectly executed changes**
  Detects whenever a Change Order is not implemented correctly.

The policy specifies any of the following actions with the discovered data inbound to the CMDB:

1. Accept the data into the CMDB even though a variance exists.
2. Reject the inbound attribute data.
3. Reject the entire inbound transaction.
4. Write the inbound data to the TWA.
5. Create an Incident.

6. Write to the standard log.

The Configuration and Change Administrators *must* establish a change verification strategy for your environment. The default policy allows all changes to all CIs, even if the change is rogue, or the change does not match a change ticket. For more information about implementing a strategy see the Implement a Change Verification Strategy topic.

Create a Verification Policy

The Configuration Administrator creates verification policies for change verification. For example, the policy can reject specific attributes and values from a transaction. Or, it can record the transaction to the TWA for deferred processing. For authorized source MDRs, the policy can accept the transaction unconditionally.

The Verification Policy History tab shows the audit history that displays all previous modifications that are made to the policy. The Verification Log tab shows all the CACF events that are associated with the policy. The Verification Log tab lists all events that have occurred for the policy. The log shows details on the affected change specifications, managed attributes, and actions when the policy was effect.

For example, the log displays the modified managed attribute and the policy history shows the category values that you specified in the policy. Verification log entries in red indicate that the change specification is either Failed Verification or Manual Verification Active and require further attention by the user.

Follow these steps:

1. Click Create New.
   The Create New Verification Policy page appears.

2. Complete the Policy Description:

   a. **Sequence**
   (Unique) Specifies the numbered order to process the policy.
   Note: CACF processes policies in ascending order.

3. On the Policy Settings tab, select the appropriate Change Order alignment:

   a. **Change Orders With Specifications**
   Active if a Change Order with selection criteria matches the inbound CI and the attribute. The inbound transaction data may not match the specified change specifications. If an exact match exists between the planned value and the inbound data, the policy determines whether to close any Incidents that change verification creates automatically.

   b. **Change Orders Without Specifications**
   Active for Change Orders that do not have any change specifications defined. Indicates that CACF cannot verify the variance for the inbound CI attribute data for Change Orders that do not have change specifications.

c. **Rogue Insert**
Indicates that the variance is found without a matching CI or change ticket.

d. **Rogue Update**
Indicates that the variance is found with a matching CI, but without a matching change ticket that updates the changed attribute.

4. Select a Managed Attribute.

5. Select Any Managed Attributes if the policy applies to all managed attributes.

6. Enter the appropriate patterns such as Role Pattern, MDR Name Pattern, MDR Class Pattern, CI Name Pattern, Class pattern, Location Pattern. Consider the following rules:

   - When you specify patterns, the MDR Name Pattern, MDR Class Patterns, and role patterns refer to the source of the data update. The other filters refer to the CI that a user updated.
   - Specify an exact string match for the inbound attribute value.
     For example, enter **COHESION** to return all string matching *COHESION*.
   - Specify an exact string matched suffixed with a wildcard (*) for the inbound attribute value. CACF only allows one asterisk at the end of the string.
     For example, enter **spectrum*** to match the string *spectrum*, and any string that starts with *spectrum*.
   - Specify the negative of an exact string match by prefixing the string with an exclamation point.
     For example, enter **!COHESION** to match any string that does not start with COHESION.
   - The MDR Name of Web Client indicates that the web interface created the source data.

   Note: Policy filters do not support embedded wildcards, such as spec*rum.

7. (Optional) Select a Priority level from the drop-down list to match the CI priority.

8. (Optional) Select a Service Type from the drop-down list to match the CI Service Type.

9. Select the appropriate Update Behavior from the drop-down list:

   a. **Allow Attribute Update**
   Updates to CI attribute values are always allowed.
   Use this value when you require no attribute verification, such as when you require logging and auditing.

   b. **Allow Update Only if Matches Change Specification**
   Updates the CI attribute value only if it matches the planned value of the change specification. Otherwise, CACF rejects the update, and the change specification status sets to Failed.
   Use this selection when you enable Change Order verification.

c. **Always Cancel Entire Transaction**
Cancels this update and all other updated attributes during this transaction. If any matching policy cancels the entire transaction, the transaction is canceled, even if other policies allow the change.
This value only triggers when an update occurs to a managed attribute.

d. **Keep Old Attribute Value**
Value rejects the inbound data.
This value is similar to canceling the entire transaction, but it only rejects a single attribute.

10. Select the appropriate Action:

a. **Write Data to TWA**
Select Always or Never. If you select Always, the incoming data is written to the TWA for later processing.

b. **Create Incident**
Select Yes or No to create Incidents that is based on this verification policy. If you select Yes, CACF creates an Incident for failed verification or a rogue update.

c. **Incident Template**
(Optional) Select an existing template to use if CACF creates an Incident.

d. **Close Incident after Verification**
Automatically closes any associated Incidents with this verification policy. The criteria for closing are that the data matches the Change Order and all change specifications are in a final state.

e. **Log Only Mode**
Adds a warning message to the stdlog whenever this policy would take effect.
Note: Any higher sequenced policy governs the transaction, as if this mode policy did not exist.

11. Specify the Activation and Deactivation dates when this policy is in effect, and click Save.
The verification policy is saved.

Knowledge Management

This section contains the following articles:

Knowledge Management Overview

This article contains the following topics:

Knowledge management refers to the concept of finding, organizing, and publishing knowledge. Knowledge management captures information quickly and efficiently and then delivers this information to a user or group. The information that is captured and made available for retrieval is referred to as a knowledge base.

Users access a knowledge base by using a search engine. Knowledge Management lets you create and manage content that resides in a knowledge base. You set category and document permissions to use groups or roles. Knowledge Management helps you provide customers with solutions to complex issues. Effective knowledge management quickly delivers solutions to customers through a process that is user-friendly and easy to navigate.

To manage knowledge effectively, you take the following actions:

- Create a meaningful hierarchy of content.
- Identify the gaps in existing knowledge.
- Perform the updates and maintenance to help ensure relevance of content.
- Measure the value of available content.

Key Features

Some of the key features of Knowledge Management are as follows:

- **Document Preferences**
  Users can define preferences that help them work with documents. For example, users can set preferences for the contents that display on the Knowledge Document List page. To view the Preferences Settings page:

  - Select Preferences from the View menu.
  - Click Edit on the Preferences Detail window.

- **Natural Language Search**
  Natural Language Search (NLS) lets the analyst specify a natural language string, such as "How do I install a network printer?" to query the knowledge base for solutions. NLS instantly pinpoints candidate solutions, ranking them in order of relevance. As NLS learns from every solution that is captured, it continuously and automatically refines the knowledge base.

- **Knowledge Categories**
  Knowledge categories allow the analyst to manage the content in the knowledge base. They provide a mechanism for building and editing knowledge underlying the retrieval tools. Knowledge categories also include the ability to assign ownership of a particular knowledge solution to an expert. Hence, they ensure that the solution for a given problem is kept current and accurate.

- **Knowledge Tree Designer**
  The Knowledge Tree Designer (see page) tool helps the analyst develop and deploy business policies and intelligence by mapping any reasoning process into a knowledge tree structure.

- **HTML Editor**
  The HTML Editor (see page 2740) lets the analyst define the layout and static content of a knowledge document template. The template defines the layout and content of the Resolution section of a knowledge document. In a knowledge tree document, it defines the layout and content of a node.

- **Knowledge Report Card**

  The Knowledge Report Card (see page 2819) provides feedback to analysts, knowledge engineers, knowledge managers, supervisors, category owners, and system administrators about which knowledge documents are most effective. You can use the report card to improve the processes of creating knowledge documents and providing the best support to customers.

- **Multi-Tenancy**
  Multi-Tenancy allows analysts to create and modify knowledge documents and knowledge categories publically, or for specific tenants. A tenant dropdown appears in the search filter, and the search can include or exclude Public data.

Types of Knowledge Documents

Knowledge documents can be of two types:

- Knowledge document
- Knowledge tree document

Knowledge Document

Knowledge documents are placed into categories that some organizations assign to owners. Under the Top category in the Knowledge Tree, many sub categories can exist. These sub categories can in turn have many sub categories.

A knowledge document contains the following components:

- **Template**
  Specifies the content and format of documents that are displayed in the defined user view. The following templates are available by default:
  - Knowledge Documents
  - Knowledge Tree Documents
  - Quick Editing
- **Document Fields**
  Provides a consistent structure to the content in a knowledge document. For example, the Title and Summary make the content easy to scan when viewed in a list of items. The Resolution field stores the body of the solution, in rich text, tables, graphical images, and much more. These fields and their associated attributes define properties such as categorization, ownership, permission, modification date, and a range of other metadata that can help with management and retrieval.

Links to Other Forms

Allows knowledge documents to link to other forms of knowledge, which is stored either within or outside of Knowledge Management, including unstructured content such as a text file. You can also add action content (a live URL) so that the user viewing the document can perform certain actions. For example, you can insert a link into the Resolution field, which creates a ticket or performs some other action.

Knowledge Tree Documents

A knowledge document and knowledge tree document share much of the same descriptive data (such as Title, Summary, Modify Date). However, a knowledge tree document prompts the user with a series of questions with a list of multiple choice answers. By responding to the questions, they are directed to the correct answer or to the information they require. This interaction is governed by a decision tree, which is designed by the creator of the Knowledge Tree document.

Knowledge Tree Documents is well-suited to the following situations:

- Common incidents that need decision-based diagnosis/process guidance.
- Highly structured content.
- Relatively unchanging content.

Knowledge Management Roles and Functions

Knowledge Management is designed for a wide variety of users, from administrators and knowledge managers, who manage the product. It is also for customers, and employees, who use the system to find solutions to their problems. Although one person can fill multiple roles, the following roles are the basic user roles in Knowledge Management:

- **Customer --** An external end user who performs basic self-service tasks.
- **Employee --** An internal end user who performs basic self-service tasks.
- **Knowledge Analyst --** A user that is responsible for one or more steps within the knowledge management process. This user interacts with service desk analysts to create and maintain a quality solution base.
- **Knowledge Manager --** A supervisor for the Knowledge Analyst. This role handles knowledge document reassignments and escalations, and manages day-to-day administrative aspects of the solution. For example, creating the category structure, defining the approval process, managing noise words, special terms, synonyms, and other settings and options that are more dynamic in nature than what the Knowledge Management Administrator controls.
- **Administrator --** The administrator who has access to all the functionality in CA SDM and Knowledge Management. This role is typically used when implementing CA SDM to help ensure that all users and roles are set up properly. This role is also applicable for a CA SDM environment that has a single person performing all administration tasks.
- **Knowledge Management Administrator --** An administrator who is responsible for configuring and monitoring the knowledge management process. This role includes creating the category structure, defining the approval process, and configuring default search and security settings.

Each role has a different level of access in the CA SDM environment. These levels help define the tasks that each role performs.

Knowledge Documents Lifecycle

Knowledge documents provide you with information about knowledge that is stored in the knowledge base. Creating quality knowledge requires input from several individuals. Each individual is responsible for performing specific tasks throughout various stages in the lifecycle of a knowledge document.

Knowledge documents reside in the knowledge base and are managed as part of the following ongoing process:

1. Identify content to include in the knowledge base.
2. Create a knowledge document.
   Knowledge documents are placed into categories that some organizations assign to owners. If the Incident/Request Area in CA SDM matches the knowledge categories in Knowledge Management, the category is automatically selected for the knowledge submission.

> **Note**: When a document is created or updated, it is placed in an owner Inbox. Until the items are published, the items in the Inbox do not appear as resolutions and are not added to the knowledge base.

3. Revise the document.
   After a document arrives in the inbox, users can modify the documents according to their assigned roles.
   All users with full (read/write) permission to the document can modify the document. The current owner has full permissions to the document, but not necessarily have explicit write permissions. Users can create versions or can roll back to a previous version when a problem with the document is found.

4. Submit the document.
   In addition to submission from the customer or employee self-service interface, knowledge can also be submitted from CA SDM. This option lets the analyst submit a new resolution from an existing ticket. This option also provides a link between a problem and its resolution, and can help other users with similar problems to find a resolution.

5. Publish the document.
   After a document has passed through the complete approval process cycle, it can be published. A document that has been published becomes part of the viewable knowledge base on the start date, which is the current date by default. The document is only viewable by groups that have been granted access rights to read it. A user with full permissions can edit a published document.

Evaluate and decide whether to perform the following tasks:

- **Unpublish the document --** When a knowledge document is published, the user is not permitted to modify the document unless it is unpublished first. During this time, the knowledge document is offline and unavailable to users. The owner of the document, a knowledge manager, or a system administrator can unpublish the document using the Rework button and the Unpublish check box. Unpublishing a document returns it to draft status. An administrative user can then select the next step in the workflow process.

- **Create a Rework Version --** Users with full editing permissions can create a rework-draft version of a published document while it remains online and available for viewing and searches. A rework version create a copy of the document. This document replaces the original document in the knowledge base after it is verified and republished.

- **Retire the document --** The owner of the document, a knowledge manager, or a system administrator can retire the document from the knowledge base.

You can define the tasks and the roles that perform each of these tasks to meet the approval process structure that exists in your organization.

Note: You can track knowledge activities from the Event Log tab on contact detail pages. For example, the event log records the actions that an user performed on the document and provides a link to the document.

Knowledge Management User Interfaces

The following user interfaces help you manage knowledge:

- **Self-Service --** In the self-service interface, customers and employees using CA SDM can access knowledge documents and can submit knowledge for further consideration. Customers can search, browse, or use bookmarks to locate and view knowledge documents.

- **Knowledge Documents --** The knowledge documents interface is accessed from the Knowledge Documents node on the CA SDM Scoreboard. All users of the system can view their Inbox and follow-up comments using this interface. The *administrator* manages their unassigned/unindexed documents, automated document lifecycle policies, and user forums.

- **Knowledge Management --** The knowledge management interface is accessed from the Knowledge tab in CA SDM. The *knowledge analyst* or *knowledge manager* can find, organize, and publish knowledge using this interface.. They can also filter the documents that are displayed using advanced options, and sort the results by relevance, modified date and much more.

- **Knowledge Administration --** The knowledge administration interface is accessed from the Knowledge node on the CA SDM Administration tab. The *administrator, knowledge manager, or knowledge management administrator* can set system options using this interface. Settings can help conform the functionality and use of Knowledge Management.

Knowledge Management Configuration and Management Functions

You can perform the following configuration and management functions in Knowledge Management:

- Create "action content" (a live action URL) that you can insert into the Resolution field of a document.

- Set up the approval process and define the knowledge document lifecycle process.

- Set up automated policies that automate certain tasks in the knowledge document approval process.

- Set up document options that are related to comments, submitting knowledge, templates, and document settings.

- Create the templates that control how a document displays information.

- Manage the default Knowledge Management search engine and configure noise words, special terms, and synonyms that are used to perform keyword and natural language searches.

- Create "recommended documents" that display in the self-service interface when users search for knowledge solutions.

- Manage the knowledge category structure to make document access easier.

- Set up the Knowledge Report Card and general system settings.

- Define the surveys that collect and analyze the customer feedback about knowledge document performance.

- Manage integration of Knowledge Management into CA SDM, including the field mapping and request and issue search configuration.

Web Services

Knowledge can be accessed through SOAP web services. Various methods are available, permitting the search, retrieval, creation, and updating of documents, and a range of other operations.

Note: For more information about SOAP web services, see Web Services Management (see page 1855).

Knowledge Base Monitoring

You can monitor the efficiency of the knowledge base using the following reporting tools. These tools let you view statistics on the usefulness of your documents and their effectiveness in solving problems.

- **Knowledge Report Card**
  Lists statistics for documents you have created. Each user has an individual Knowledge Report Card.

- **Web-Based Reports**
  Displays metrics that describe how knowledge is meeting user needs. Some of the most commonly used features include:

  - Listing the most frequently accessed documents.

  - Displaying user searches that did not return any results.

Getting Started with Knowledge Management

Effective knowledge management consists of more than the development of a large knowledge base. Knowledge management also involves the implementation of processes and procedures for maintaining relevant and accurate content.

To set up a knowledge base, do the following tasks:

1. Analyze how you plan to use the knowledge base and the scope of it.

2. Consider who the customers are and what information they are likely to need.

3. Develop a strategic plan that identifies the potential issues that can result in the need for customer support. The problems that you identify can guide you in determining what content must reside in your knowledge base.

4. Execute the development of your knowledge base. Create, organize, maintain, and secure this data. You can perform all these functions by using Knowledge Management.

Import Sample Knowledge Data

Sample Knowledge data from Knowledge Broker and Knowledge Accelerators is provided for your use. You can import the sample data to view example knowledge articles on How-to, knowledge broker, and so on.

Note: The sample files are not localized. Importing sample data does not work on localized environments.

For the advanced availability configuration, run ImportSampleData.bat or ImportSampleData.sh from the background server.

Windows

1. Go to $NX_ROOT\samples\data and unzip SampleData.zip into the same directory.
2. From the command window, go to $NX_ROOT/bin and run ImportSampleData.bat.

UNIX

1. Run the command tar -xvf SampleData.tar from $NX_ROOT/samples/data.
2. From the command window, go to $NX_ROOT/bin and run ImportSampleData.sh.

Setting Up the Knowledge Management System

This section includes the following articles:

Configure Knowledge Management Settings

Contents

You can configure certain role-specific and document-specific settings when you are setting up your knowledge management system. You can also change these settings later to suit your requirements.

How to Manage Role Privileges and Document Visibility

You can set up Knowledge Management security permissions by managing role privileges for users in your environment. Use these permissions to define the information that users can access in a knowledge document, when they view or create knowledge. You can also define how users are authenticated when they log in to the system.

Follow these steps:

1. From the Administration tab, select Security and Role Management, Role Management, Role List.
   The Role List page appears.

2. Select the role that you want. For example, Knowledge Manager.
   The Role Detail and Update Role pages display the following tabs:

   - **Knowledge Management**
     Specifies the Knowledge Management privileges for the role.

   - **KT Document Visibility**
     Specifies which document statuses the role is allowed to view, such as draft, retired, and published.

3. Complete the tab pages and save changes.
   Security and role privileges are defined.

Note: For more information about setting up security and defining roles, see Managing Roles (see page 1166).

Configure General Settings

You can set the default information to display on the Knowledge tab at logon. You can specify the format in which categories display in the Knowledge Categories pane on the Administration tab, and the number of documents to list in the Top Solutions list on the Knowledge Management home page.

Follow these steps:

1. Select **Knowledge, System, General Settings** on the **Administration** tab.
   The **General Settings** page opens.

2. Complete the following fields as appropriate:

   - **Search Tool Opening Screen**
     Specifies the information that is displayed by default on the **Knowledge** tab. You can select one of the following options:

     - **Open with FAQ / Search**
       Displays the **Category, Knowledge Search**, and **Knowledge Document List** panes.

- **Open with Knowledge Tree Document ID**

- Displays the knowledge tree with the document ID specified in the field provided. You can return to the knowledge tree document itself, and then to the **Category**, **Knowledge Search**, and **Knowledge Document List** panes. **Default:** Open with FAQ /Search

- **Category Viewing**
  Specifies the format in which document categories display in the **Knowledge Categories** pane on the **Administration** tab. You can select one of the following options:

  - **Display categories in tree view**
    Presents the categories in a hierarchical tree structure in the **Knowledge Categories** pane. Categories expand to reveal associated subcategories. In this manner, you can view all the categories in the tree simultaneously.

  - **Display categories in list view**
    Presents the categories in a list format in the **Knowledge Categories** pane. When you select a category, its subcategories display in a list. You can view only the current level of categories or subcategories at one time. Use the **Up One Level** link to return to the previous category level.

  Note: If you have more than 250 categories under the top category, or under any category, use the **Display Categories in List View** option and not the tree view.

- **Top Solutions**
  Specifies the number of documents to list in the **Top Solutions** list on the CA SDM home page.
  Default: 10

  Path for EBR Index Files

  Defines the location for storing EBR index files. CA SDM creates EBR index files when you save and publish any knowledge document. Depending on your configuration type, consider the following points while defining the EBR index file path:

  - Conventional: If you are upgrading from the CA SDM Release 12.9 from r11.2 or r12.X, you may choose not to use UNC shared path. If you have not created a UNC path, CA SDM uses the default path to store EBR index files. If you are using a UNC shared drive, manually copy the ebr/ebr_ADM folders from the default location ($NX_ROOT/site/) to the UNC shared path.

  - Advanced availability: If you are upgrading to the advanced availability configuration from CA SDM r11.2 or r12.X, you must create the UNC shared path and use it to store EBR index files. The UNC credentials are not required for the default path. After you create the UNC path, manually copy the ebr/ebr_ADM folders from the default location ($NX_ROOT/site/) to the UNC shared path.

    Important!EBR Index Files path & **KEIT Files path** must refer to the same UNC credentials and the path must reside on a same server to support this.

Default: $NX_ROOT/site/ebr

- **Path For Knowledge Import/Export Files**

Defines the location for storing KEIT import/export packages during an import/export operation. Depending on your configuration type, consider the following points while defining KEIT file path:

- Conventional: If you are upgrading to CA SDM Release 12.9 from r11.2 or r12.X, you may chose not to use UNC shared path. If you have not created a UNC path, CA SDM uses the default path to store the KEIT files. If you are using a UNC shared drive, manually copy the Import/Export package folders from the default location ($NX_ROOT/site/keit) to the UNC shared path.

- Advanced availability: If you are upgrading to the advanced availability configuration from CA SDM r11.2 or r12.X, you must create the UNC shared path and use it to store the KEIT files. The UNC credentials are not required for the default path. After you create the UNC path, manually copy the Import/Export package folders from the default location ($NX_ROOT/site/keit) to the UNC shared path.

  Important!EBR Index Files path & **KEIT Files path** must refer to the same UNC credentials and the path must reside on a same server to support this.

Default: $NX_ROOT/site/keit

- **UNC Credentials**

You can use this option to create UNC credentials to access the network shared drive to access EBR indexing files and import/export packages. Use the **UNC Credentials** link to create the UNC credentials.

Note: UNC paths and UNC credentials are required in case of the advanced availability configuration. Restart the CA SDM service when you change any of the UNC details (UNC paths or UNC credentials).

- **Document Indexing Notifications**

Sets a user to receive email notifications about status or when errors occur with document indexing. The user must have an email address in the ca_contacts table to receive these email notifications. Use the Notification Page for the assignee contact record for setting notification methods.

Important! You must set an **Assignee** to receive document indexing notifications in the **Document Indexing Notifications** section. A valid email address must be defined in the **Notification** tab of this contact to enable email notifications.

3. Click Save.
   General settings are configured.

Note: When migrating from an older CA SDM release to the advanced availability configuration, manually copy the import/export packages to UNC shared location (specified in **Path For Knowledge Import/Export Files** field). For EBR index files, you can manually move the EBR/ebr_ADM folders to the UNC shared location or execute the pdm_k_reindex command path.

Specify Document Settings

As a system administrator, you can specify settings that are related to comments, submitting knowledge, and viewing knowledge tree documents.

Follow these steps:

1. On the Administration tab, select Knowledge, Documents, Document Settings.
   The Document Settings page appears.

2. Complete the following fields:

   - **Knowledge Tree Document Viewing**
     Specifies the viewing mode in which knowledge tree documents open. Select Open in Tree Mode (default) to open the knowledge tree directly or Open in Document Mode to open the document in document view. If you open in Document Mode, click Display to show the knowledge tree.

   - **Comments**
     Specifies if users can submit comments for documents and view document comments. Select one of the following options:

     - **Allow comment submission and comment viewing (default)**
       Displays a Comment field at the bottom of an open document so users can submit comments for the document. Users can view comments that are already associated with the open document.

     - **Allow comment submission but not comment viewing**
       Displays a Comment field on the right of an open document so users can submit comments for the document. Users cannot view comments that are already associated with the open document.

     - **Allow neither comment submission nor comment viewing**
       Disallows the users from submitting or viewing comments. The Comment field does not display in an open document.

3. **Submit Knowledge**
   Defines the repository for user-submitted documents. The product populates the list with the names of repositories that are defined on the Attachment Library pane.
   Consider the following information:

- When an analyst creates a document in a category that has an owner and assigns the document to the category owner:
  Category owner becomes the assignee and owner of that document.
  Category owner must receive a document assigned notification.

- When an analyst creates a document in a category that has no owner and assigns the document to the category owner:
  No one becomes the assignee or owner of that document.
  Submit KD notification must send as defined in the administration.

- When an analyst creates a document and does assign the document to the category owner:
  That user becomes the assignee and owner.
  A notification does not send.

- When an employee or customer creates new documents, CA SDM takes the action as stated in the first two points.

4. **Maximum Resolution Size**
   Defines the maximum size (in characters) that the Resolution field in a document can contain.
   Limits: The maximum characters allowed is 256000.
   Default: 32768.

5. **Duplicate Document Avoidance**
   Forces a search for similar documents when the user creates a knowledge document.

6. **Notification before Expiration**
   Defines the number of days before the document expires and a notification is sent.
   Default: 7

   Note: This value only applies to documents that have been updated or created in CA SDM. If you migrate documents from CA SDM r11.2, and the expiration dates are set before the migration, this option applies only when you update the document after the migration.

7. Click Save.

   The changes apply when you open a knowledge document or a knowledge tree document.

Setting Up Self-Service Knowledge Options

Customers and employees using CA SDM have access to knowledge documents through the self-service interface. Customers can search, browse, or use bookmarks to locate and view knowledge documents. Giving the customers access to knowledge documents and services permits customers to find answers themselves and reduces the pressure on resources.

In the self-service user interface, employees, and customers can view the following knowledge solution options:

- **Search for Knowledge Solutions**
  Employees and customers can enter keywords and phrases in a search field that retrieves a list of knowledge solutions. You can configure this option in the following location: Administration, Knowledge, Search, Search Settings.

- **View Top Solutions**
  Employees and customers can display a list of top solutions in the self-service interface. The following Administrator setting: Administration, Knowledge, System, General Settings, Top Solutions -- Number of Documents to Display, determines the number of documents to display.

- **Prompt for Knowledge Survey**
  The users are prompted for a knowledge survey after they have read the document. The survey has a series of questions. One of these questions lets the customer indicate through a prompt whether they feel that their problem has been solved. You can configure this option in the following location: Administration, Knowledge, Solution Survey, Survey Settings.

- **Suggest Knowledge**
  Employees and customers can, where permitted, view a list of knowledge suggestions when they create a ticket in the self-service interface. You can configure this option in the following location: Administration, Knowledge, Service Desk Integration, Suggest Knowledge.

Define Document Preferences

You can define preferences that help you work with information in Knowledge Management. The Preferences Settings window opens when you do either of the following actions:

- Select Preferences from the View menu
- Click Edit on the Preferences Detail window

In General Settings, the following fields require explanation:

- **Avoid Popups**
  Specifies whether to reduce the number of new browser windows opened by displaying new forms in the main browser window whenever possible.

  - Select the check box to minimize the number of new browser windows opened.
  - Clear the check box to open new browser windows according to the properties set in the form definition.

  Default: Cleared.

  Note: If this option is selected, the Back to List button can be used to navigate from detail forms back to the previously displayed list window. The Back to List button appears in the upper right-hand side of the window.

- **Keep Log Reader Window**
  Specifies whether to keep the Log Reader window open when you select the Close All Popups command from the Window menu and after you log off of Knowledge Management. This setting has no effect when the Log Reader window is not open.

- Select the check box to keep the Log Reader window open.
- Clear the check box to close the Log Reader window when you select the Close All Popups command or log off of Knowledge Management.

Default: Selected.

- **Preserve Popup Size**
  Specifies whether to open new popup windows with the same dimensions as the most recently resized popup window.
  - Select the check box to use the new dimensions for new popup windows.
  - Clear the check box to open new popup windows with default dimensions.

  Default: Selected.

  Note: If you select Preserve Popup Size, maximizing a popup window will cause subsequent windows to cover any other open window. However, new popup windows appear slightly off the screen, to the right and down. As there is a 10 pixel (left and top) offset for popups, they do not completely overlay the currently displayed window. We recommended that you do not maximize popup windows when using the Preserve Popup Size option.

- **Using Screen Reader**
  Selecting this preference modifies behavior for optimal use with a screen reader for blind and limited vision users. Log off and log back in again after changing this preference. From the Help menu, select Screen Reader Usage for an overview of using CA SDM with a screen reader.

In Knowledge Search Document Settings, the following fields require explanation:

- **Attributes to be shown in list**
  Displays two lists with which you can define the properties that display for each document in the Knowledge Document List pane on the Knowledge Categories pane of the Administration tab.

  Note: Choosing the attributes different from the Preference default can impact performance. If you believe that extra display columns are needed, contact the system administration and ask them to use the Web Screen Painter utility to modify the default page columns for the Document List page.

Define a Document Approval Process

Contents

For the administrators who want to control the management of their knowledge base, the ability to modify the document editing and approval process is essential. You can design Approval Process templates that specify how, when, and by which an employee document can be modified and published to the public. Approval Process templates can designate different approval processes best suited to your business environment. The approval process that you implement can be modified over time to become simpler or more complex.

The Approval Process Manager lets you define Approval Process templates. By default, the Built-in Approval Process template is used. However, you can create a template or can edit an existing template. When creating an Approval Process template, you define statuses and you add tasks to the template. The approval process involves a series of tasks that are performed on a knowledge document. The owner that is assigned a task in the Approval Process template performs each task.

The following statuses are the various states that the document is associated with during the stages of the approval process:

- **Draft**
  Specifies a new document.
- **Published**
  Specifies a document that has passed through the complete approval cycle and becomes part of the viewable knowledge base.
- **Rework-Draft Version**
  Specifies a rework version of a copy of the document that is replaced in the knowledge base after it is verified and republished.
- **Retired**
  Specifies a document that has reached its expiration date. You can also create your own statuses, which you later associate with tasks.

Note: You can also create new document statuses. For more information, see Create a Document Status (see page 2708).

Approval Process Manager

Knowledge Administrators can use the Approval Process Manager to perform these actions:

- Determine which groups can read a knowledge document and which groups can write (or edit) the knowledge document.
- Identify the tasks in an approval process template that determine the lifecycle of documents that are created with the template.
- Define the various statuses that the document can be associated with during the approval process.

Important! When creating a knowledge document, verify that document permissions include users that can later be assigned to the document through the approval process. Users from that group do not necessarily have the permission to view the document. If the document is assigned to a specific user, default data partition constraints let the user view the document.

Define an Approval Process for Document Editing

Knowledge administrators can specify who can edit documents before the approval process and after publishing. Users with full (read/write) permissions can edit published documents.

Follow these steps:

1. On the Administration tab, browse to Knowledge, Approval Process Manager, Approval Process Settings.
   The Approval Process Settings page appears.

2. Specify who can edit documents *before* the documents are published. Select one of the following options:

   - **Documents may be edited by a task assignee, an owner or users with the appropriate Access Type views**
     Specifies that the following contacts can edit documents:

     - A contact that is assigned to the current task
     - A contact that is specified as an owner of the document for the current task
     - A knowledge manager
     - A system administrator

   - **Documents may be edited by users with full permissions**
     Specifies that any user with write permissions to the document can edit it.

3. Specify who can edit documents *after* the documents are published. Select one of the following options:

   - **User with full permissions may edit documents after they have been published**
     Specifies that a user with full permissions can edit published documents.

   - **User with full permissions can change published document's attributes**
     Specifies that any user with write permissions to the document can change only attributes of published documents such as configuration items or products.

   - **Document must be unpublished before editing is allowed**
     Specifies that the user must unpublish a document before editing it.

   Click Save.
   The approval process is defined.

Create an Approval Process Template

The tasks in an approval process template define the lifecycle of documents that are created with the template.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. From the Administration tab, select Knowledge, Approval Process Manager, Approval Process Templates.
2. Click Create New.
3. Enter a name for the template and a description.
4. Click Save.
   The Approval Process Template Detail page displays more fields.
5. Select the task that you want to perform when you create a rework version of the document using this template.
6. Select the task that you want to perform when you unretire a document that was created using this template.
7. Click Insert Task to create a task to add to the template.
   The Create New Task page displays.
8. Complete the fields.
9. Click Save.
   The approval process template is created.

Create a Document Status

You can add and delete user-defined document statuses, and modify the names and descriptions of predefined document statuses.

Follow these steps:

1. From the Administration tab, select Knowledge, Approval Process Manager, Document Statuses.
   The Document Status List appears.
2. Click Create New.
3. Enter a name for the status and a description.

4. Click Save.
   The document status is created.

Define Comment Types

Contents

If the analyst notices a typo or problem with the content in a document, they can add a comment. The comment flags the document for correction and then assign the problem to another analyst for followup. Administrators can define the comment types that appear in various list views within the end-user interface.

Create a Comment Type

You can define the comment types that appear in various list views within the end-user interface.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Administration tab, select Knowledge, Documents, Comment Types.
   The Comment Type List page appears.

2. Click Create New.
   The Create New Comment Type page appears.

3. Complete the fields as appropriate. The following fields require explanation:

   - **Time to Complete (Days)**
     Defines the number of days by which the user must follow up on this type of comment.

   - **Show in User View**
     Displays the comment in various list views within the user interface.

   - **Follow-up Required**
     Specifies if the user is required to respond to this type of comment.

   Click Save.
   The new comment type appears on the Comment Types List page.

Set Up a Follow-Up Comment Notification

Several default activity notifications that are listed on the Activity Notification List page let you set up notifications to users when a follow-up comment is assigned to them.

The Follow-Up Comments queue on the scoreboard is the repository for assigned and unassigned follow-up comments.

Follow these steps:

1. On the Administration tab, browse to Notifications, Activity Notifications.
   The Activity Notification List page appears.
2. Select *one* of the following activity notifications:
   - Follow-Up Comment Assigned
   - Follow-Up Comment Closed

   The Activity Notification Detail page appears.
3. Click Edit.
4. Change the fields as appropriate.
5. Click Save.

Define Document Templates

You can use document templates to control the format and default content of knowledge documents. Every knowledge document uses a document template to define its properties and appearance when opened. By default, a built-in template is associated with new knowledge documents.

The Template Editor lets you do the following tasks:

- Design a document template that can later be associated with a document.
- Modify the built-in template and other templates.
  By editing templates, you can create templates to associate with documents. You can select the Properties options and can edit the Header and Body sections using the HTML Editor.
- Update document templates from a previous release to support knowledge relationships (see page), such as parent-child links.

A document template specifies the content and appearance of documents in the knowledge base. You can apply the default templates:

- Built In -- Knowledge Document
- Built In -- Knowledge Tree
- Built In -- Quick Editing

The knowledge documents and knowledge tree documents use the default templates unless you create document templates and you associate them with your documents.

Note: When you are creating a knowledge document, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Administration tab, browse to Knowledge, Documents, Document Templates.
   The Document Templates List page appears.

2. Click Create New.
   The Create New Document Template page appears.

3. Complete the following fields:

   - **Template**
     (Required) Defines a unique name for the template.

   - **Detail**
     Displays the static content that appears in documents that are created using the current template. If you select the HTML Source option, you can edit HTML code for the body directly in the Body. Select the Quick View option to view the body content as it appears at run time.

4. (Optional) Click Set Default Values.
   The Default Values Template page appears.
   You can set default values when creating a document. If you change the template on an existing document, there is no impact.

5. (Optional) Hide the Title, Summary, Problem, or Resolution from appearing in your template.
   You can hide these fields when you want a simple document, such as a question and answer template.

6. Click Edit Detail.
   The HTML Editor page appears and you can specify the static content and layout of documents that use the template. You can edit the code using the toolbar to insert placeholder tags.

   Important! You can remove knowledge relationships, such as parent, child, and related links, by deleting the {TAG_PARENT} and {TAG_RELATED} tags from the template.

7. Click OK.
   The Detail field shows the updated content.

8. (Optional) Click Quick View.
   A quick view of the content as it appears in documents that are based on the template is displayed.

9. (Optional) Click HTML View.

> **Note:** You can update knowledge document templates from a previous release of CA SDM to display knowledge relationships. You modify the template by adding the {TAG_PARENT} and {TAG_RELATED} tags. The tags allows documents that are using the template to display document relationships, such as parent-child links and tenant. To do so, select *Select Template Placeholder* on the Edit Detail dropdown to add tags to the document template.

10. Click Save.

11. The Document Template Detail page appears.

12. Click Close Window.
    The new documents that use the template show the new content and layout.
    The name of the template appears in the Template List when you display the list again.

> **Note**: Changes to the document using the template display after starting a new session by logging in to the system.

Define FAQ and Solution Survey Settings

Contents

Solution Surveys let you collect and analyze customer feedback about Knowledge Document performance. You can modify the survey settings by selecting Knowledge, Solution Survey from the Administrative Interface. The survey appears on a published Knowledge Document. The customers, guests, and employees can take the survey and rate the effectiveness of the Knowledge Document.

This feature contains the following components:

- FAQ Settings
- Survey Settings

Define FAQ Settings

You can set the parameters by which the product calculates the FAQ rating that is assigned to each document. The product bases the FAQ rating on the following criteria:

- How frequently the document was accessed in the past?
- How helpful the document was to users?

- How the effectiveness of the document has decreased over time?

By default, the document list page displays documents that are sorted in the order of FAQ rating (in the order of usefulness). The most useful documents "bubble up" to the top of the document list. Over time, documents tend to move downward in the document list as users learn solutions to the problems.

Follow these steps:

1. Select Knowledge, Solution Survey, FAQ Settings from the Administration tab.
   The FAQ Settings page appears.

2. Complete the following fields as appropriate:

   - **Last Updated**
     Specifies whether to run the FAQ Rating Service and displays the date on which FAQ ratings were last updated.

     - Select the Run the FAQ Rating Service check box to run the FAQ calculation service using the settings on this window.

     - Clear the Run the FAQ Rating Service check box to turn off the FAQ calculation service.

   - **Schedule**
     Defines the frequency at which the product updates FAQ ratings. This field contains the following components:

   - **Perform the FAQ Calculation Every...**
     Specifies the time that elapses before the product updates the FAQ rating for documents.
     Default: 1 day

   - **From...**
     Specifies the time of day that the product must begin recalculating FAQ ratings.
     Default: 00:00 (12:00 A.M.)

   - **To...**
     Specifies the time of day that the product must stop recalculating FAQ ratings, regardless of whether the calculation is finished. This setting initially takes effect the day after product installation. For example, if you install the product on April 19, 2008, the FAQ server runs for the first time on April 20, 2008.
     Default: 07:00 (7:00 A.M.)

   - **Aging**
     Defines the number of times a document FAQ rating is recalculated before it reaches 0. Based on the specified value, the document FAQ rating decreases and eventually becomes 0. At this point it appears at the bottom of the document list (when the list is sorted by FAQ Rating).
     Default: 180
     For example, if the Aging value is 180 for a document with a rating of 4 (very helpful), the FAQ rating of the document is 0 (zero) when the product has recalculated the FAQ rating 180 times.

Note: By default, the FAQ bubble-up calculation requires bu_trans data for the last 180 days, where 180 is the aging factor. So, if you change the aging factor for FAQ to more than 365 days, you must extend the archive rules for the bu_trans table accordingly.

- **Days New**
  Specifies the number of days that a newly created or imported document displays in the New Documents folder on the Knowledge tab.
  Default: 5 days

- **Rating**
  Specifies the default rating (Not Helpful at All, Somewhat Helpful, or Very Helpful) for documents that users have opened but not rated.
  Default: Somewhat Helpful

Click Save.
The FAQ settings are defined.

Define Solution Survey Settings

You can configure the survey options that you want to show to the users when they access the document.

Follow these steps:

1. Select Knowledge, Solution Survey, Survey Settings from the Administration tab.
   The Survey Settings page appears.

2. Select the survey options that you want. Select the Display 'Voting Summary' option to display the number of votes that the document received and the average rating. The summary is displayed on the Employee interface.
   The solution survey settings are defined.

Create a Knowledge Category

Knowledge documents are arranged into *knowledge categories*. Knowledge engineers, knowledge managers, and administrators can manage the categories. Each of these individuals uses Knowledge Management to create, copy, and modify categories. However, only knowledge managers and administrators can delete categories. The category structure in Knowledge Categories helps you create a hierarchical structure that service desk employees, customers, and analysts use to navigate to relevant documents.

Assign each document to a primary category. For example, any knowledge that is related to Microsoft Word must be added to the Microsoft Word category. In addition, Knowledge Management lets you associate a document with multiple secondary categories and other documents. This feature allows a document to be classified under many different applicable categories and results in better search results.

The category structure performs the following functions:

- Organizes knowledge solutions into manageable groups.

- Makes it easier to assign access rights.
- Makes it possible to search for solutions using FAQ/Browse.
  To use category browse functionality from an incident, the incident area and the knowledge category must match. When you create an incident that is based on a knowledge document, the document category sets the incident area; therefore, the category and the area always match.
- Creates a document link -- A *see also* link appears when viewing either of the linked documents. The *see also* link lets you go directly from one linked document to the other.

For each category, you can define properties that identify attributes or qualities to be associated with the ticket. You can also create a workflow that identifies all the individual tasks that are required to fulfill the ticket.

You can use categories to specify default values for certain fields in tickets, or automatically associate a level of service to tickets by assigning a default service type to categories. Whenever an analyst assigns a category to a ticket, all the information you associate with the category is automatically associated with the ticket.

Note: If you are using multi-tenancy, a tenant drop-down list appears in the Knowledge Document search filter. If you select <empty> in this drop-down list, the search is public. A tenant column also appears on the list page.

Follow these steps:

1. On the Administration Tab, browse to Knowledge, Knowledge Categories.
   The Knowledge Categories page appears.
2. Right-click the category under which you want to create the category. Select New Category from the shortcut menu.
   The Create New Category page opens to the Content tab.
3. Complete the fields (see page 2716) as appropriate.
4. Click Permissions.
   The Permissions tab appears.
5. Select one of the following permissions options for the category:
   - **Inherit from Parent**
     Specifies that the new category has the same permission settings as its parent category.
     Note: The Inherit from Parent option is not available if you select the TOP category before opening the Create Category page.
   - **Control by Group**
     Specifies category permissions for groups to have read or write access to the category.
   - **Control by Role**
     Specifies category permissions for roles to have read or write access to the category.

Note: If you change controls, such as changing the category permission from group to role, a warning appears that previous permissions are deleted for that category.

- **Grant Write Permission to Everyone**
  Specifies that all users have write access to the category. Write access indicates that you can edit or delete this category.

  Note: The Grant Read Permission to Everyone check box is automatically selected if you select the Grant Write Permission to Everyone check box.

- **Grant Read Permission to Everyone**
  Specifies that all users have read access to the category. Read permission indicates that you can view the category, but you cannot edit or delete it. Users with administrative rights can edit a folder even if their associated permission group cannot. If a user belongs to multiple permission groups with varying levels of access to the category, the user gets the highest available access level (for example, if one group has read-only access and the other write access, the user gets write access).

  Note: The Grant Read Permission to Everyone check box is automatically selected if you select the Grant Write Permission to Everyone check box.

  Important: When you grant permissions for Everyone, the access by role or group is the same. If you selected Everyone and Control by Role, after you save the permissions, the Control by Group becomes selected.

6. (Optional) Specify the read-write permissions to specific groups or roles from the Available and Selected lists.
   You use this option to manage which groups or roles have read or write access to the category. You can select one or more permission groups or roles from the Available Groups /Roles list, and then use the Add and Remove buttons to move the selected groups or roles to the Groups/Roles with Write Permission and Groups/Roles with Read Permission lists.

7. Click Save.
   The Category Detail page appears.

8. Click Close Window.
   The Knowledge Categories pane refreshes to include the new category.

Category Fields

- **Title**
  Names the category.

- **Description**
  Describes the category.

- **Category Owner**
  Indicates the person responsible for the category. When a contact is defined as the owner of a category, the contact has a link on the Knowledge Report Card named "My Categories," from which they can view statistics for that category and the documents it contains. This person is also the default owner for new documents in the category when the user who creates the documents is not an analyst, or an analyst creates the documents with 'Assign to Category Owner' selected.

- **Documents Template**
  Defines the document template to use for all documents that are associated with this category. The <empty> option means that none have been defined, but by default, the predefined template is used.

- **Approval Process Template**
  Defines the default template to use for the approval process for all documents that are associated with this category. The approval process template defines the workflow steps a document must go through before it is published. The default is <empty>, which indicates the application default template is used.

- **Allow forums to be created in this category**
  Specifies whether analysts can create forums within this category.

- **Request/Incident/Problem Area**
  Designates a Request/Incident/Problem area that your administrator defines to designate an area of responsibility. You can click the search icon to select from the available areas.

- **Issue Category**
  Designates an Issue Category that your administrator defines to designate an area of responsibility. You can click the search icon to select from the available areas.

How to Set Up the KT Search Engine

The Search feature enables administrators to perform the following tasks:

- Manage the Knowledge Management search engine.

- Define the settings that are used to manage noise words, special terms, and synonyms that are excluded or included in searches.

- Define the settings that are used to parse documents.

- Define default search settings.

- Create "recommended documents" that display in the search results. Dynamic FAQ listing is used to push (bubble up) the recommended documents to users.

Note: A document can have different permissions than the attachments linked to the document.

KT Search Engine

Content:

After you install CA SDM, the KT search engine is configured as the default. Searches of the knowledge base are limited to knowledge documents. The search engine is on the Administration tab, Knowledge, Search, KT Search Engine node.

Note: You can define accessibility and defaults to all knowledge sources based on a user role. By default, knowledge documents are searchable for all user roles.

To configure the search engine, go to Options Manager, Search Engine from the Administration tab and edit the ebr_version as KT Search Engine. For more information about editing an option, see Install/Uninstall Options Manager Options (see page 2718) page.

Noise Words, Synonyms, and Special Terms

You can define words (synonyms, noise words, and special terms) that affect natural language and keyword searches that are performed in CA SDM. Adding or deleting the following terms has a significant effect on search results that are returned to the user:

- Noise Words
- Special Terms
- Synonyms

Create Noise Words

Specifies the words that do not generally contribute to the search process and can, therefore, be ignored. For example, prepositions such as a, an, the, or, and to are often identified as noise words. The search engine ignores the noise words in documents and queries without affecting search results.

Follow these steps:

1. On the Administration tab, select Knowledge, Search, KT Search Engine, Noise Words.
   The Noise Words List page appears.
2. Click Create New.
   The Create New Noise Word page appears.

3. Enter the word that you want to define as a noise word in the Noise Word FIELD.

   Note: You cannot define a noise word that exists as a synonym or keyword.

4. Click Save
   The new noise word appears on the Noise Words List page. You can click the Edit button to update the new noise word.
   Note: You cannot define a noise word that exists as a synonym or keyword.

Note: After you create, modify, or delete noise words, special terms, synonyms, or parse settings, use the Knowledge Re-Index utility that is provided with the product to re-index the knowledge base.

Create Special Term

Specifies a term that you want identified as a single word during the search process, although it can consist of several words or contain special characters. For example, words that have a nonalphanumeric character, such as the forward slash (/) in TCP/IP, the hyphen (-) in dial-up, or the underscore (_) in LOCAL_SERVER can be added as special terms. In your evaluation of which words to define, consider valid words that can be divided during the search process because they have a nonalphanumeric character.

Follow these steps:

1. On the Administration tab, browse to Knowledge, Search, KT Search Engine, Special Terms.
   The Special Terms List page appears.

2. Click Create New.
   The Create New Special Term page appears.

3. Enter the word or phrase you want to define as a special term in the Special Term field.

4. Click Save.
   The Special Term Detail page opens so you can review the word or phrase you added. You can use the Edit button to update the new term. The new special term appears on the Special Terms List page.

Create a Synonym

Specifies a word that has the same meaning as another word. When a user searches for a particular word, and a corresponding synonym for that word exists in your knowledge base, the information can be found. You can define several synonyms for the same word. The system automatically creates reverse synonyms from the keywords you define. For example, if you define computer as a synonym for the word PC, PC automatically becomes a synonym for the word computer. Use the Synonyms List page to specify keyword/synonym pairs that the product uses interchangeably when parsing documents and queries. These keyword/synonym pairs can improve search results.

Note: After you create, modify, or delete noise words, special terms, synonyms, or parse settings, use the Knowledge Re-Index utility provided with the product to re-index the knowledge base.

If you define a new complex synonym (that is, a synonym containing multiple words that are separated by spaces or other delimiters), also create an identical special term so that the product can treat the synonym as a single entity. For example, if you define "Computer Associates" as a synonym for "CA", also define "Computer Associates" as a special term.

You cannot define a synonym or keyword that exists as a noise word.

Follow these steps:

1. On the Administration tab, browse to Knowledge, Search, KT Search Engine, Synonyms.
   The Synonyms List page appears.

2. Click Create New.
   The Create New Synonyms page appears.

3. Enter the word or phrase you want to define as a synonym in the Synonyms field.

4. Click Save.
   The Synonyms Detail page opens so you can review the word or phrase you added. The new synonym appears on the Synonyms List page.

5. Right-click the synonym and select Edit if you want to edit the synonym,

Define Parse Settings

When you publish a document to the knowledge base, the product parses the information in the Title, Summary, Problem, and Resolution fields of the document into keywords. When a user searches the knowledge base, the product compares keywords from the user query with the keywords parsed from the knowledge base to produce a result list.

Use the Knowledge Re-Index utility to re-index the knowledge base after you change parse settings and when you add noise words, special terms, or synonyms. Re-indexing the knowledge base ensures that keyword searches are based on current and accurate information.

Note: Depending upon the size of your knowledge base, re-indexing may take a significant amount of time.

To re-index the knowledge base, see instructions on the pdm_k_reindex utility from the CA SDM PDM Database Commands (see page 3889) page.

Follow these steps:

1. Browse the Administration tab in Knowledge, Search, Parse Settings.
   The Parse Settings appears.

2. Use the following fields to define settings:

- **Maximum Search Keywords**
  Defines the maximum number of keywords to extract when the product parses the search text.
  Default: 20

  Note: The valid range is 1-100, so that a CA SDM Knowledge administrator can change the value within this range, which is based on search needs and parameters of a specific Knowledge database. Use a lower number of search keywords for faster performance.

- **Language**
  Specifies the language type to use for parse processing. Select one of the following settings:

  - **English**
    Performs certain types of processing specific to the English language (for example, de-pluralizing search terms) during a search, if applicable.

  - **Other European**
    Performs only European specific processing during the search.

  - **Korean**
    Performs only Korean specific processing during the search.

  - **Other Far East**
    Performs processing for other far east languages during the search.

    Note: When you are in a Chinese, Japanese, or Korean operating environment, verify that you understand the available parsing approaches, and limitations of Multi-Byte Character Set (MBCS) languages (see page 2723), before implementing your Knowledge Management system to help ensure that user expectations are set appropriately.

- **Valid Character Range**
  Defines the range of alphanumeric characters to consider valid when parsing the Title, Summary, Problem, and Resolution fields in a document. The product treats any other characters as separators.

  Note: When you select Yes from the Recognize Special Terms list, the product does not parse words and phrases defined as special terms.

Default: a-z, which indicate that the alphabetic characters a through z are valid characters for parsing.
The Valid Character Range field contains the appropriate letters that parsing uses. The letters that are not presented in the Valid Character Range are removed.
The recommended values for different languages are as follows:
Language Valid Character Range
German a-zäöüß
Spanish a-záéíóúüñ
French a-zàäâçéèêëîïôùû
Portuguese Brazil a-zàáãçéêíóúü
Italian a-zàèéìîïù
Simplified Chinese a-z
Japanese a-z
Traditional Chinese a-z
Korean a-z

Note: Japanese contains the "a-z" range plus a list of Katakana valid characters, excluding punctuation marks.

- **Remove Similar Words**
  Specifies whether the product removes structurally similar keywords from the groups that are used in a search. You can select one of the following settings:

  - **Yes**
    Removes structurally similar keywords from the search criteria.

    Note: When you select Yes, the product also removes similar words when you save or publish the document. This setting can impact whether a document is searchable if the Remove Similar Words field was set to Yes. The similar word may have not been indexed and used in the later search and retrieval of the document.

  - **No**
    Leaves structurally similar keywords in the search criteria.

  Default: No

- **Remove Noise Words**
  Specifies whether the product removes noise words when parsing the Title, Summary, Problem, and Resolution fields in a document. You can select one of the following settings:

  - **Yes**
    Removes noise words from the search criteria.

  - **No**
    Leaves noise words in the search criteria.

  Default: Yes

- **Recognize Special Terms**
  Specifies whether the product considers special terms as single entities or as multiple words when parsing the Title, Summary, Problem, and Resolution fields in a document. You can select one of the following settings:

  - **Yes**
    Processes special terms as single entities in the search criteria.

  - **No**
    Processes the words that comprise special terms as separate entities in the search criteria.

  Default: Yes

Multi-Byte Character Set Search Limitations

Make sure that you understand the available parsing approaches, and limitations of MBCS languages, before implementing your Knowledge Management system to help ensure that user expectations are set appropriately. This limitation of the product impacts search features using Japanese, Chinese, or Korean language text within the system. The word parsing mechanism used by the search mechanism is controlled on the Parse Settings (see page 2720) page.

For the English, Other European, and Korean settings, the product assumes that punctuation, “white space,” or both characters separates words. This assumption allows the document text to be broken into specific words, and allows noise words to be ignored and application of known synonyms and special terms to search terms.

Alternatively, when the Far East language setting is selected, the parsing routine uses a character-by-character parsing approach to accommodate some Far East language text approaches of not using white-space delimiters between words. This setting tells the parser to assume that each character is treated as a full word. The setting applies to all text to be searched. Because the language setting changes the way that the search parsing works, the entire search index must be recreated if the language setting is changed to or from Far East.

Create Recommended Documents

The CA SDM users can specify the criteria about an item of interest. The search engine then finds the matching knowledge documents and displays them on the search results page as a set of "recommended document" links. The search query can be expressed as a keyword or set of words (phrase) that identify the desired concept that one or more documents can contain.

The list of documents that meet the search criteria is sorted, and ranked (from highest to lowest) to place the most relevant documents first in the search results. Using recommended documents helps users reduce the time that is required to find the desired information.

To provide a set of matching documents that are sorted according to some criteria quickly, the search engine collects data through the condition type (phrase, keywords, or category), which the administrator configures on the Create Recommended Documents page.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. On the Administration tab, browse to Knowledge, Search, Recommended Documents.
   The Recommended Documents List appears.

2. Click Create New.
   The Create New Recommended Documents page appears.

3. Complete the following fields as appropriate.

   - **Knowledge Document**
     Specifies a knowledge document or click the search icon to open the Knowledge Document Search page.

   - **Condition Type**
     Specifies a condition type (see page 2724) by which the search engine sorts and matches the document.

     - If the condition type is Full Match, Exact Phrase, or Keywords, a text field appears. You can enter a phrase or keyword that identifies the concept you want for the document to contain.

     - If the condition type is Knowledge Category, the Knowledge Category link appears. You can specify a knowledge category to associate with this document.

   - **Status**
     Defines the status of this record as active or inactive.

   Click Save.
   The new recommended document is saved to the knowledge base and appears on the Recommended Documents List page.

Condition Type Field

The search engine locates documents by the following condition types:

- **Full Match**
  Searches for documents by the search phrase entered in the search text. A match occurs only when the search engine finds all the same words in a phrase.

- **Exact Phrase**
  Searches for documents by the exact phrase entered in the search text. A match occurs only when the search engine finds the exact set or sequence of words in a phrase.

- **Keywords**
  Searches for documents by the keywords entered in the search text. A match occurs only when the search engine finds all of the keywords.

- **Knowledge Category**
  Searches for documents by knowledge category. A match occurs only when a user navigates to a category configured for recommended documents.

Set Up Default Search Settings

You can set up default search options that appear when users search for knowledge using the search field.

Note: These search options are overwritten by any personal search settings users define in the Preferences window, or any additional search options that are specified in the following places:

- In the Knowledge Search pane on the Knowledge tab.
- In the Knowledge Categories pane on the Administration tab.

Follow these steps:

1. From the Administration tab, navigate to Knowledge, Search, Search Settings.
   The Search Options page displays.
2. Select the following options as appropriate:
   - **Recommended Results**
     Specifies the number of documents to display in the search results list.
   - **Default Search Fields**
     Specifies which document fields to include by default in keyword searches. The following document fields are available for searching:
     - Title
     - Summary
     - Problem
     - Resolution
     - Attachments
   - **Search Settings for All Sources**
     Specifies whether searches can include all knowledge sources. For example, knowledge categories and request areas.
   - **Search Settings in a Ticket Context**
     Specifies whether searches can include all fields that are defined in a service desk ticket (incident, problem, issue, change order, or request).
     For these options, select *one* of the following match types:
     - **Any of the words (OR)**
       Includes a document in the result set when it contains any of the words in the Search field. This option is the default selection.

- **All of the words (AND)**
  Includes a document in the result set only when it contains all the words in the Search field.

3. Click Save.
   The default search settings are set up.

How to Set Up Knowledge Management with Ticket Categories

This article contains the following topics:

Define the configuration options available for CA SDM Integration.

Define Field Mapping

Administrators can specify which fields to populate with Knowledge Management information, and whether to overwrite existing information.

Follow these steps:

1. On the Administration tab, browse to Knowledge, Service Desk Integration, Field Mapping.
   The Field Mapping page appears.

2. Complete the following fields as appropriate:

   - **Populate Service Desk Values from Knowledge Management**
     Specifies whether to use information from Knowledge Management to populate fields in service desk issues or requests.

     - Select the check box to make fields in the Knowledge Management, Populate Empty Service Desk Values, and Overwrite Service Desk Values columns available so you can specify which Knowledge Management information to use to populate fields in service desk issues or requests.

     - Clear the check box to make fields in the Knowledge Management, Populate Empty Service Desk Values, and Overwrite Service Desk Values unavailable. In this case, users must manually populate service desk issues or requests that are created from Knowledge Management.

     Default: This check box is selected.

- **Service Desk**
  Identifies the fields in issues or requests that correspond to fields listed in the Knowledge Management column.
  For each check box selected in the Populate Empty Service Desk Values column, information from the corresponding field in the Knowledge Management column populates the issue or request.

- **Knowledge Management**
  Identifies the Knowledge Management fields that correspond to the service desk fields listed in the Service Desk column.
  For each check box selected in the Populate Empty Service Desk Values column, information from the corresponding field in the Knowledge Management column populates the issue or request.
  The Knowledge Management column contains two drop-down lists:

  - The first drop-down list corresponds to the Summary field in the Service Desk column. It also specifies the Knowledge Management field (Title, Summary, or Problem) with which to populate the Summary field in an issue or request.

  Default: Summary.

  - The second drop-down list corresponds to the Description field in the Service Desk column. It also specifies the Knowledge Management field (Title, Summary, or Problem) with which to populate the Description field in an issue or request.

  - **Default**: Problem.

- **Populate Empty Service Desk Values**
  Specifies which empty fields in a service desk issue or request to populate with information from Knowledge Management.

  - Select a check box to map information from the Knowledge Management field to the corresponding service desk field if that field currently contains no information.

  - Clear a check box if you do not want to map information from the Knowledge Management field to the corresponding service desk field.

  Default: The check boxes corresponding to the
  Summary, Description, Product, Asset, and Request Area fields in service desk are selected.

- **Overwrite Service Desk Values**
  Specifies which fields in a service desk issue or request to overwrite with information from Knowledge Management.

  - Select a check box to replace information in the service desk field with information from the corresponding Knowledge Management field.

  - Clear a check box if you do not want to replace information in the service desk field with information from the corresponding Knowledge Management field.

These check boxes are only available when the corresponding check boxes in the Populate Empty Service Desk Values column are selected.
Default: All Overwrite Service Desk Values check boxes are cleared.

3. Click Save.
   Field mapping is defined.

Define Issue Search Configuration

You can define the fields within an Issue to search in when you click the Search Knowledge button on a ticket. The fields that you select are copied to the corresponding fields in the Search Filter on the Knowledge tab of the Issue Detail window. The population of the Search Filter fields from the ticket occurs when the Knowledge tab is selected or the Reset Filter button (on the Knowledge tab) is clicked.

Follow these steps:

1. From the Administration tab, select Knowledge, CA SDM Integration, Issue Search Configuration.
   The CA SDM Integration page displays.

2. Select the fields that you want to be available for Knowledge Base searches.

   - Summary
   - Description
   - Configuration Item
   - Priority
   - Category
   - Root Cause
   - Product

   Note: You cannot select both the Summary and Description fields.

3. Select the "Automatically run search when the Knowledge tab of an issue is selected" option if you want to search the knowledge base automatically when the Knowledge tab on the detail page is selected.

4. Click Save.
   Issue search is configured.

Define Request/Incident/Problem Search Configuration

You can define the fields within a request, incident, or problem to search in when you click the Search Knowledge button on a ticket. The fields that you select are copied to the corresponding fields in the Search Filter on the Knowledge tab of the ticket detail page. The population of the Search Filter fields from the ticket occurs when the Knowledge tab is selected or the Reset Filter button (on the Knowledge tab) is clicked.

Follow these steps:

1. From the Administration tab, select Knowledge, CA SDM Integration, Request/Incident /Problem Search Configuration.
   The CA SDM Integration page displays.

2. Select the fields that you want to be available for Knowledge Base searches.

   - Summary
   - Description
   - Configuration Item
   - Severity
   - Impact
   - Urgency
   - Priority
   - Request Area
   - Root Cause

   Note: You cannot select both the Summary and Description fields.

3. Select the "Automatically run search when the Knowledge tab of a request is selected" option if you want to search the knowledge base automatically when the Knowledge tab on the detail page is selected.

4. Click Save.
   The fields in a request, incident, or problem to use for Knowledge Base searches search is configured.

Knowledge Suggestions

Employees and customers can, where permitted, view a list of knowledge suggestions when they create a ticket in the self-service interface.

If a solution is found, and the ticket is not saved, the documents that were suggested can be credited through a self-service rating system in the document form. This rating system differs depending on the self-service policy settings that are defined on the Search Settings page.

The data that is retrieved can be used for reports, dashboards and also while searching the knowledge base, where users can filter the documents that have successfully resolved their tickets.

The benefits of self-service are in the form of fewer support calls and redundant tickets that are created, which translates into reduced operational costs.

The administrator must enable this feature before use and must configure the appropriate issue categories and request areas for which knowledge is suggested in the self-service interface.

Define Issue Categories

You can define issue categories for which knowledge is suggested to customers and employees during ticket creation.

You can also mark the Suggest Knowledge feature as active or inactive. When you mark this feature as inactive, it is no longer available to customers and employees, but it remains available in the database for future use. If you decide to use this feature in the future, you can go back and can mark it as active.

Follow these steps:

1. On the Administration tab, browse to Knowledge, Service Desk Integration, Suggest Knowledge, Issue Categories.
   The Suggest Knowledge for Issue Categories page appears.

2. Select the **Do not suggest knowledge** option to mark the Suggest Knowledge feature as active.
   Default: Inactive
   If you mark this feature active, the following options appear:

   - **By default knowledge will be:**

   - **Suggested**
     Indicates that you *do* want knowledge to be suggested for all issue categories except the definitions in the issue categories list.

   - **Not Suggested**
     Indicates that you *do not* want knowledge to be suggested for all issue categories except the definitions in the issue categories list.

   - **For all Issue Categories except the following:**
     Displays the list of request areas where knowledge is either suggested or not suggested to employees and customers in the self-service interface. The self-service user is not allowed to edit the request areas, they are read-only.

3. Click *one* of the following buttons:

   - **Add**
     Adds the selected request area to the list.

- **Remove**
  Removes the selected request area from the list.

- **Remove All**
  Removes all request areas from the list.

- **Save**
  Saves the request area information to the knowledge base.

The Issue categories are defined.

Define Request/Incident/Problem Areas

You can define request, problem, and incident areas for which knowledge is suggested to customers and employees during ticket creation.

You can also mark the Suggest Knowledge feature as active or inactive. When you mark this feature as inactive, it is no longer available to customers and employees, but it remains available in the database for future use. If you decide to use this feature in the future, you can go back and can mark it as active.

Follow these steps:

1. On the Administration tab, browse to Knowledge, CA SDM Integration, Suggest Knowledge, Request/Incident/Problem Areas.
   The Suggest Knowledge for Request/Incident/Problem Areas page appears.

2. Select the **Do not suggest knowledge** option to mark the Suggest Knowledge feature as active.
   Default: Inactive
   If you mark this feature as active, some additional options appear:

   - **By default knowledge will be:**

   - **Suggested**
     Specifies this option if you want knowledge be suggested for all request/incident/problem areas except those that are defined in the Request Area list.

   - **Not Suggested**
     Specifies this option if you *do not* want knowledge be suggested for all request/incident /problem areas except those that are defined in the request area list.

   - **For all Request/Incident/Problem Areas except the following:**
     Displays the list of request areas where knowledge is either suggested or not suggested to employees and customers in the self-service interface. The self-service user is not allowed to edit the request areas, they are read-only.

3. Click Save.
   The suggest knowledge request/incident/problem areas are defined.

Configure Self-Service Policies

You can configure self-service policies that credit documents based on a set of user scenarios.

Follow these steps:

1. On the Administration tab, browse to Knowledge, CA SDM Integration, Suggest Knowledge, Self-Service Configuration.
   The Search Settings page appears.

2. Specify the appropriate policy settings that credits documents and save avoided tickets that are based on the following user scenarios:

   - User did not open any suggested document.
   - User opened a suggested document.
   - User accepted a suggested document as a solution to their problem.
   - User searched for knowledge, opened the document, and exited.

   Click Save.
   Self-service policy settings are saved.

Create Knowledge Documents

This article contains the following topics:

Create the Knowledge Document

You can create knowledge documents to capture and organize information and expand your knowledge base. Knowledge documents provide users in your environment with solutions to complex issues.

Follow these steps:

1. Click the Administration tab and navigate to Knowledge, Knowledge Categories.

2. Select the desired knowledge category.

3. Click File, New Knowledge Document.
   The Create New Document page appears.

4. (Optional) Use the Find Similar tab to search for related documents.

5. (Required) Choose a document template from the drop-down list. The template specifies the content and format of documents that are displayed in the defined user view.
   You can also use templates to populate default values.

6. Depending on the template definition, complete the following fields display:

   Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

   - **Doc ID**
     A numeric unique ID is assigned to a knowledge document. The Doc ID is used by analysts and customers to refer to a particular knowledge document.

   - **Title**
     Defines a short, descriptive name for the document. For knowledge tree documents, Title defines the name of the primary node in the knowledge tree.

   - **Summary**
     Defines a summary that briefly describes the problem that is associated with the document.

   - **Problem**
     Defines the full description of the problem that is associated with the document.
     NLS search type is based on this field.

   - **Parent Document**
     Specifies the parent document of the knowledge document you are viewing. The tenant of the parent document also appears, depending on your permissions.
     Note: Modifying a parent document alerts you that the change can affect child documents.

   - **Related Documents**
     Specifies the related documents of the knowledge document you are viewing. The tenant of the related documents also appears, depending on your permissions.

   - **Resolution**
     Defines the description of how to resolve the problem.

   - **Quick View**
     Specifies to display content in the associated field as it appears at runtime. This field only displays when you are creating or updating a knowledge document.

   - **HTML Source**
     Specifies to display content in the associated field as HTML source code you can edit. Select this option to make simple changes directly to the HTML code. This field only displays when you are creating or updating a knowledge document.

- **Notes**
  Defines additional information about the document. The contents of this field are available only to analysts.

> **Note:** Modifying a parent document alerts you that the change can affect child documents.

7. Click Save and Close.
   The document appears on the Document List page and in the appropriate inboxes (see page 2741).

8. Edit the knowledge document (see page) and add permissions to the users to whom you have assigned the document.

Edit the Knowledge Document

You can edit a knowledge document that has not yet been published. All users with full write permissions can edit documents by default, but the administrator specifies your knowledge document permissions. For example, your administrator configures Knowledge Management so that only an assignee, the document owner, or a knowledge manager can edit documents.

Follow these steps:

1. On the Knowledge tab, select the appropriate category.
   The Knowledge Document List page displays documents in the selected category.

2. Right-click the title of the document, and select Edit from the shortcut menu. If the document has been published, create a rework version to modify the content.
   The Update Knowledge Document page appears.

3. (Optional) The properties (see page 2735) of a knowledge document can be changed on the Attributes tab, but you must have write access to the document to modify the properties.

4. (Optional) Complete or change the fields on the various tabs as appropriate.

   - Click the Attributes tab (see page 2735) to define the document attributes such as the Assignee, Approval Process Template.

     > **Note:** You must have write access to the document to modify the properties.

   - Click the Permissions tab (see page 2739) to define the permissions for the contacts who will be working on the document.

   - Click the Related Knowledge tab to add the related knowledge documents.

   - Click the Attachments tab to add a file or URL to the knowledge document.

- Click the Comments tab to add a comment for follow-up and assign the comment to a contact.
- Click the History tab to view the events that occurred on the knowledge document.
- Click the Versions tab to view the document versions and revisions.
- Click the Find Similar tab search for similar documents that may contain knowledge solutions. Locating similar documents can help you avoid creating duplicate information. You can also create knowledge relationships from the context menu.

5. (Optional) Do *one* of the following, as appropriate:
   - **Knowledge Document**
   - Click Edit Resolution on the Content tab to open the HTML Editor (see page 2740).
   - Modify the body (resolution) of the document.
   - Click OK to save your changes and close the HTML Editor.
   - **Knowledge Tree Document**
   - Click Design Tree on the Content tab to open the Knowledge Tree Designer (see page).
   - Edit the knowledge tree.
   - Click Save and Close.
6. (Optional) Click Spell Check to review the spelling in the content you entered.
7. (Optional) Click User View to open the Preview window, which presents the document as it appears when a user displays it.
   You can close the Preview window when you finish reviewing the document.
8. Click Save when you finish editing the document.
   The product saves your changes.
9. Do *one* of the following actions:
   - Click Save Version to save a new version of the document.
   - Click Publish to put the document in the knowledge base and make it available to users with the appropriate permissions.
   - Click Cancel to close the Update Knowledge Document window and open the Knowledge Document Detail window.

Update Document Attributes

You can use the Attributes tab to set properties of a knowledge document that define ownership, scheduling, approval process, layout, associations, and so on.

Note: You must have write access to a document to set its attributes.

Note: If the Priority Calculation is set up and a user opens a ticket on the Knowledge Document, the Priority, Urgency, and Impact fields on the Attributes tab automatically appear on the ticket.

The tab contains the following fields:

- **Initiator**
  (Read-only) Displays the name of the contact who created the document. You can click the name to open the Detail window for the contact.

- **Assignee**
  Defines the name (in "last name, first name" format) of the contact to whom the document is assigned during the current approval process task. You can enter or search the name of the contact in "last name, first name" format.

- **Author**
  Defines the name (in "last name, first name" format) of the contact with responsibility for the document content.

- **Owner**

  Defines the name (in "last name, first name" format) of the contact assigned to maintain the document. A document can have the same or a different owner in each stage of the approval process. All analysts with write access to a document can modify it, even if they do not own it.

  Note: If a guest user or customer submits a document using the Submit Knowledge feature, the document has no owner.

- **Subject Expert**
  Defines the name (in "last name, first name" format) of a contact with expertise in the subject matter of the document. Enter or search the name of the contact in "last name, first name" format.

- **Creation Date**
  (Read-only) Displays the date and time at which the document was created.

- **Modify Date**
  (Read-only) Displays the date and time at which changes to the document were last saved.

- **Published Date**
  (Read-only) Displays the date and time at which the document was published. If the document has not been published, the field is blank.

- **Last Accepted Date**
  (Read-only) Displays the date and time at which the document was last accepted as the solution to a ticket. If the document has not been accepted, the field is blank.

- **Start Date**

  Defines the date (in mm/dd/yyyy format) on which to make the document available in Search Tools. You can click the calendar icon to open the Date Helper window so you can select a date.

  > **Note:** A document can only become available on the Search Tools window when it is published and reaches its start date. For example, if you publish a document on March 1 with a start date of March 8, the document does not become available on the Search Tools window until March 8. If you publish a document with no start date specified, it immediately becomes available on the Search Tools window. The date format in Knowledge Management must match the date format that you have set up on your Windows operating system.

- **Expiration Date**

  Defines the date (in mm/dd/yyyy format) on which the product removes the document from the knowledge base and the Search Tools window. After the specified date, the document is available from the Administration tab to users with the appropriate permissions. You can click the calendar icon to open the Date Helper window so you can select a date.

  > **Note:** The date format in Knowledge Management must match the date format that you have set up on your Windows operating system.

- **Review Date**

  Defines the date on which the document must be next reviewed. Click the calendar icon to open the Date Helper window so you can select a date.

  > **Note:** The date format in Knowledge Management should match the date format that you have set up on your Windows operating system.

- **Disregard Life-Cycle Policies**
  Ignores the lifecycle policies in your organization.

- **Approval Process Template**
  (Required) Specifies an approval process template to associate with the document. The approval process template specifies the tasks in the document lifecycle. You can choose the default template provided with the product or a user-defined template. If left empty, it is set to the default template used in your knowledge environment.
  Note: For knowledge managers, knowledge engineers, and system administrators: The access

types that can select an approval process template during the first task (typically Create Knowledge Document) are selected on the Knowledge tab Access Type window. In subsequent stages of the approval process, the Approval Process Template box is read-only and displays the name of the template selected for the document.

- **Approval Process Priority**
  Specifies the approval process priority to associate with the document. Valid values include <empty>, Low, Normal, High, and Emergency.
  Default: Normal.

- **User Defined ID**
  Defines an ID for the document to use as an alternative to the product-defined ID.

- **FAQ Rating**
  (Read-only) Displays the current document FAQ rating, which the product calculates from the frequency at which a document is accessed, how helpful it has been to users, and its age.

- **Hits**
  (Read-only) Displays the number of times the document has been accessed.

- **Self-Service Count**
  (Read-only) Specifies the number of times that the knowledge document was used to solve a problem. It is a count of the number of times the customer responded with Yes to the question “Did this document solve your problem? “ in the document Solution Survey.

- **Average Rating**
  (Read-only) Specifies an average rating value. Each rating response (very helpful, somewhat helpful, and not helpful at all) has an assigned numeric value. The average rating is the total of the document response ratings divided by the total number of votes.

- **User Votes**
  (Read-only) Specifies the total number of votes for the document. Submitting a Solution Survey is considered a vote.

- **Priority**
  Specifies the priority to associate with the document, indicating the urgency of problems the document is meant to resolve.

- **Severity**
  Specifies the level of effect that the problem the document is meant to resolve may have on users.

- **Impact**
  Specifies the level of impact that you expect the document to have on work being performed.

- **Urgency**
  Specifies the importance level of the user tasks that are associated with the document.

- **Product**
  Defines a product to associate with the document. Enter the name of the product or click the magnifier to open the Product Search dialog so you can locate and select a product.

- **Configuration Item**
  Defines the name of a configuration item (hardware, software, or service) to associate with the document. Enter the name of the configuration item or click the magnifier to open the Configuration Item Search dialog so you can locate and select an asset.

- **Root Cause**
  Defines a root cause or core reason to associate with the document. Enter a root cause or click to open the Root Cause Selection window so you can locate and select a root cause.

- **Solution Count**
  (Read-only) Displays the number of tickets that are resolved by the document.

- **Parent Request**
  Defines an associated parent request record.

- **Parent Issue**
  Defines an associated parent issue record.

- **Problem**
  Defines a problem that is linked to this document.

Grant Permissions to Document Assignees

You can determine which groups or roles can access a knowledge document and which groups or roles can modify the knowledge document by modifying permissions for Knowledge Documents and Knowledge Categories.

Important! When creating a knowledge document, make sure that document permissions include users that can be assigned later on the document through the approval process. When a group is assigned to a document, users from that group cannot have the permission to view the document. If the document is assigned to a specific user, default data partition constraints allow the user to view the document. If you do not specify group permissions, the document is only viewable by privileged users.

You can view and grant permissions as follows:

- **From the Knowledge Category page**

  1. Right-click a category and select Edit Category from the shortcut menu.
  2. Click the Permissions tab.

- **From a Knowledge Document**
  If it is a published Knowledge Document:

  1. Click Rework.
  2. Create a Rework version, click Save.

3. Select the Permissions tab and make the appropriate changes.

Note: By default, a Knowledge Document inherits its permissions from Category Permissions. You can use empty write permissions for documents and categories. Empty write permissions are set when you do not select write permissions. Only privileged users can modify categories and documents with empty write permissions.

Use the HTML Editor

Use the HTML Editor for the following tasks:

- To define the layout and static content of a knowledge document template.
- To define the layout and content of the Resolution section of a knowledge document.
- To define the layout and content of a node in a knowledge tree document.

The HTML Editor opens when you do any of the following actions:

- Click Edit Detail on either of the following windows:
  - Create New Document Template
  - Update Document Template
- Click Edit Resolution on either of the following pages:
  - Create New Document
  - Update Knowledge Document
- Click Edit (HTML) in any of the following DT Builder panes:
  - Conclusion Text (HTML)
  - Query Text (HTML)
  - Tree Description (HTML)

Click the Insert menu to perform the following tasks:

- Insert a Horizontal Rule
- Insert a Link to a Document
- Insert a New Line
- Insert an Image
- Insert a Link to a New Ticket

- Insert a Link to Create a Change Order
- Insert Action Content

Working with Knowledge Documents

This article contains the following topics:

View Unassigned Documents

Documents that are not yet assigned to users are stored in the Unassigned queue on the scoreboard.

If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

Follow these steps:

1. On the Service Desk tab, browse to Knowledge Documents, Unassigned.
   The Document List page displayed the documents that are unassigned.

2. (Optional) Right-click the title to edit the document.

View Inbox or Group Inbox

When a document is created or updated, it is placed in the Inbox of the owner. Items that appear in an Inbox require the attention of the user as part of the publishing process. Until they are published, items in the Inbox will not appear as resolutions and are not added to the knowledge base. You must regularly monitor your Inbox to check for new documents.

You can view summary information for the documents that are contained in your Inbox or Group Inbox on the Document List page.

If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

Follow these steps:

1. On the Service Desk tab, browse to Knowledge Documents, Inbox, or Group Inbox.
   The Document List page displays the documents in the inbox.

2. (Optional) Right-click the title to edit a document.

3. All users with full permission to the document can edit the document. The current owner has full permissions to the document but may not have explicit write permissions. Only the owner can change the owner of the document (on the Attributes tab).

View Follow-Up Comments

You can view summary information for your follow-up comments on the Comment List page.

If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

Follow these steps:

1. On the Service Desk tab, browse to Knowledge Documents, Follow-Up Comments.

2. Do *one* of the following actions:

   - Expand the My Follow-Up Comments folder to reveal nested folders for your assigned Open and Closed items.

   - Expand the All Follow-Up Comments folder to reveal the nested folders.

3. Select the folder for the comments you want to see.
   The Comment List page appears. This page contains the following columns:

   - **Comment Type**
     Identifies the type of comment that is used to flag a document for correction, promotion, or retirement.

   - **Date Logged**
     Identifies the date on which the comment was logged in the system.

   - **Status**
     Indicates whether the comment is active or inactive.

- **Target Date**
  Identifies the date by which the comment must be followed-up on.

- **Contacts**
  The contact who received the follow-up comment.

4. (Optional) Click Show Filter and complete one or more of the fields to specify search criteria that restrict the list to the comments of interest.

5. Click Search.

The Comment List page displays summaries of the comments that match your search criteria.

1. (Optional) Click the Edit in List button to display some additional fields that can be associated with a comment.

   - **Assignee**
     The name of the person that is assigned to handle the comment. Enter the name of the person directly, or click the search icon to search for the name.

   - **Target Date**
     Identifies the date by which the comment must be followed-up on. Enter the target date directly, or click the calendar icon to specify a target date.

   - **Status**
     Indicates whether the comment is active or inactive.

   - **Reply**
     Allows you to enter more information.

2. (Optional) Click the More link to display the Additional Search Arguments field.

Publish Knowledge Documents

When you are ready to add a document to the knowledge base, you can publish it from the Update Knowledge Document page. Analysts can publish documents when they are at the last stage of the approval process. Administrators can publish documents at any stage of the approval process.

Follow these steps:

1. Open the document for editing.
   The Update Document page appears.

2. Click Publish.
   The Publish Document page appears.

3. Complete the following fields as appropriate:

   - **Owner**

(Required) Defines the name of the contact that is assigned to maintain the document. Enter the name of the contact in "last name, first name" format or click the magnifier to open the Contact Search dialog so you can search for a contact.

- **Comment**

(Optional) Enter a brief comment about the document.

4. Click OK.
   The published document is added to the knowledge base.

Create Rework Versions

If you have full (read/write) permissions to edit documents, you can create a *Rework-Draft* version of a published knowledge document while the document is online and available to users.

A rework version starts as a copy of the document that is replaced in the knowledge base after it is verified and republished.

Follow these steps:

1. From the Document List page, right-click the title of the document to edit, then select Edit from the shortcut menu.
   The Update Knowledge Document page appears.

2. (Optional) Complete the various tabs as appropriate.

3. Click Rework.
   A page opens displaying the list of approved document tasks from which you can select tasks to start with (if you are permitted to do so). By default, a built-in approval process template allows you to create a document.

4. Select the appropriate task from the list.
   The Create Rework Version page appears.

5. Complete the appropriate fields:

   - **Document Title**
     Displays the published document name.

   - **Document Status**
     Displays the status of the record (published).

   - **Keep Published Version Available**
     Specify whether or not to keep the original published version available to all users.
     Default: Available

   - **KD Approval Task**
     Displays the workflow tasks that you are able to perform if you have permission to do so.

   Note: You can cancel the rework version and can add comments about why you want to cancel the rework version.

6. (Optional) Select the Assignee link to assign this rework version to another person or group for review or follow-up. Once saved, the rework version appears in their Inbox.

> **Note:** If *Keep Published Version Available* is checked in the *Create Rework Version* form, it does not copy the assignee value to the rework document. If *Keep Published Version Available* is unchecked, it copies the assignee value to the rework document.

7. (Optional) Enter information about this document in the Comment field.

8. Click Save.
   The Update Document page appears.

9. Click Save.
   The *rework-draft* version appears in your Knowledge Documents Inbox on scoreboard. To display this page, select the Service Desk tab, then Knowledge Documents, Inbox.

Save Versions

You can create a draft version of a document for backup. The Save Version option is available for draft documents and rework versions that have not yet been published.

Follow these steps:

1. On the Document List page, open a draft document to edit, and select Edit from the shortcut menu.
   The Update Document page appears.

2. Complete or change the fields on the various tabs as appropriate.

3. Click Save Version.
   The Create New Version page appears.

4. (Required) Add a comment in the Comment field.

5. Click Save.
   The draft version displays on the Versions tab.

Rollback to a Previous Version

If there is a problem with the current version, you can roll back to a previous version of a published document.

Before you begin, consider the following factors:

- When performing a rollback of a published document, the earlier version appears in the document list as a new *rework-draft* document, which must be re-published in order to replace the currently published document.

- When performing a rollback of a draft document, the content of the current document is replaced with the content of the earlier version. The document remains in draft status until it is published.

Follow these steps:

1. From the Documents List page, right-click the published document to edit, then select Edit from the short-cut menu.
   The Update Knowledge Document page appears.

2. Click the Versions tab.
   The Versions List appears.

3. In the Version Number column, click the version number link.
   The Save Version page appears.

4. Click Rollback.
   The document rolls back to the previous version. If the document is published, a rework version of the document is started.

Retire a Knowledge Document

A knowledge document can be retired after it reaches an expiration date, or if the product removes it from the knowledge base. A privileged user can retire or rework a knowledge document manually.

Follow these steps:

1. Open the document for editing.

2. Click Retire.
   The Retire Knowledge Document page appears.

3. Enter a comment about why you want to retire the document.
   For example, the knowledge document described a workaround task that no longer applies to your organization.

4. Click Save.
   The document is retired.

Unretire Knowledge Documents

When a published document reaches its expiration date, the product typically retires it. A retired document is removed from the knowledge base and the approval process). A system administrator or a user with full permissions can unretire or republish the document to return it to the approval process and the knowledge base.

Follow these steps:

1. Open the document for editing.

2. Click Unretire.
   The Unretire Document page appears.

3. Do *one* of the following, as appropriate:

- If you are a system administrator, you can republish the document. To do so, click Publish this Document. A confirmation message appears.
- If you are a system administrator and there are multiple approval process tasks to which the document might revert, you can choose the task to which to assign the document, choose an assignee, and (optionally) enter a comment:
  - Click the name of a previous task to which to assign the unretired document. The Unretire Document page refreshes.
  - Select the name of a contact to assign as the owner for the document from the Assignee list.
  - (Optional) Enter a brief comment in the Comment box.
  - Click OK. A confirmation message displays.
- If you are a knowledge administrator or analyst, you can choose an assignee for the task and (optionally) enter a comment:
  - Select the name of a contact to assign as the owner for the document from the Assignee list.
  - (Optional) Enter a brief comment in the Comment box.
  - Click OK. A confirmation message displays.

4. Click OK.
   The product assigns the document to the specified task and owner and returns the document to the knowledge base and the workflow.

Document Search Fields

If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

- **Keywords for Advanced Search**
  Specifies the keywords (separated with comma or space) to use for the search in the Search field. The search result displays the keyword with the document frequency. This means the search result displays all the occurrences of the document names with that keyword. For example, in the following screenshot, we searched for a knowledge document associated with a CI and used the keyword as "updated". The search result shows updated(29), but does not display any document associated with this CI. This search result is correct. It means that 29 documents in the knowledge base contains the word "updated", but none are associated with the CI.

- **Search In**
  Specifies in which fields to search for specified keywords. When you click Search, the product returns only items that contain the specified keywords in the fields that are specified by the selected *Search In* check boxes.
  The check boxes only display when Keyword Search is the selected search type. If you select Natural Language Search from the Search Type list, the Search In check boxes do not display and the product only searches the Problem fields of documents.

- **Reset to my defaults**
  Resets all filters to their default values. This option is only available for knowledge documents.

- **Set as my defaults**
  Saves all filters and applies them as the default values. This option is only available for knowledge documents.

- **Search Type**
  Specifies the type of search to perform. Select one of the following options:

  - **Keyword Search** -- Searches for the specified keywords in the Title, Summary, Problem, and Resolution fields of documents. Use the Search In check boxes to exclude one or more of these fields.

  - **Natural Language Search** -- Searches for the specified text only in the Problem fields. Natural Language Search (NLS) lets you perform a search using natural language, which compares the pattern of words that are contained in the query with the patterns of words that are contained in the Problem field of knowledge base documents.
    Default: Keyword Search

  Note: Depending on how your administrator configured search capabilities, you may not have access to Keyword Search and Natural Language Search.

- **Match Type**
  Specifies the method for text matching during the search. Select one of the following options:

  - **Any of the Words (OR)** -- Retrieves the matches for *any* of the specified words in a document.

  - **All of the Words (AND)** -- Retrieves the matches only when the product finds *all* the specified words in a document.

  - **Exact Match** -- Retrieves the matches for *exactly* the specified words in a document.
    Default: Any of the Words (OR)

Important! Match Type and Match preferences only set the default search criteria when you search in Knowledge Management. For example, you log in as an analyst and click the Knowledge tab of any ticket. Knowledge searches from within a ticket always default to Match Type=Any of the words (OR) and Match=Whole Words, regardless of your preference settings.

- **Match**
  Specifies the method by which the product searches documents. Select one of the following options:
  - **Whole words** -- Retrieves only documents that contain the entire words entered.
  - **Words beginning with...** -- Retrieves the documents that contain the entire words entered or words that begin with the words entered. For example, a search for the word "print" also returns documents containing the words "printer" or "printing."
    The Match list setting overrides the default set on the Preferences window and is only available when you specify keywords or phrases for which to search.
    Default: Whole words
- **Order by**
  Specifies a criterion by which to sort search results. Select one of the following options:
  - **Relevance** -- Sorts documents by their relevance to the specified search criteria (expressed as EXCELLENT, GOOD, and so on). Documents with the highest relevance (EXCELLENT) are listed first.
  - **FAQ Rating** -- Sorts documents that are based on their FAQ rating, which considers how often the document is accessed, how helpful it has been to users, and its age. Documents with the highest FAQ ratings are listed first.
  - **Hits** -- Sorts documents by the number of times users have accessed them, with the most frequently accessed documents listed first. Hits may not be available for all record types. This field only displays for advanced searches on the Knowledge tab.
  - **Solution Count** -- Sorts documents by the number of issues or requests they have resolved, as reported by users. Documents with the highest solution counts are listed first. This field only displays for advanced searches on the Knowledge tab.
  - **Modify Date** -- Sorts the documents by the date on which they were last modified, with the most recently modified documents listed first.
- **Return only documents that solved tickets**
  Returns the documents that have successfully resolved tickets.
- **User Defined ID/Created By/Submitter**
  Define a user-defined ID or enter a name by which to filter documents retrieved. This field only displays for advanced searches of knowledge documents and free text content.
- **Product**
  Defines a product by which to filter documents retrieved. Enter the name of the product in the box, or click  to open the Product Search window so you can search for and can select one. When you click Search, the product returns only documents that are associated with the specified product.

- **Configuration Item**
  Defines the name of an asset (hardware, software, or service) by which to filter documents retrieved. Enter the name of the asset in the box, or click to open the Configuration Item Search window so you can search for and can select one. When you click Search, the product returns only documents that are associated with the specified asset.

- **Category**
  Define a category by which to filter documents retrieved. Enter the name of the category in the box or click to open the Category Search window. When you click Search, the product returns only documents that are associated with the specified category. Use the Remove and Clear Categories options as needed.

(Optional) Click the More link to display the following additional fields:

- **Owner**
  Defines the name (in "last name, first name" format) of the contact that is assigned to maintain the document. Enter the name of the contact in "last name, first name" format or click to open the Contact Search dialog so you can locate and select a contact.

- **Author**
  Defines the name (in "last name, first name" format) of the contact with responsibility for the document content. Enter the name of the contact in "last name, first name" format or click to open the Contact Search dialog so you can locate and select a contact.

- **Subject Matter Expert**
  Defines the name (in "last name, first name" format) of a contact with subject-matter expertise for the document. Enter the name of the contact in "last name, first name" format or click to open the Contact Search dialog so you can locate and select a contact.

- **Document Type**
  Specifies the type of document (knowledge document or knowledge tree document) to retrieve.

- **Approval Process Priority**
  Specifies the level (emergency, high, low, normal) by which to filter approvals retrieved.

- **Root Cause**
  Defines a root cause (that is, the core reason for opening the ticket) by which to filter documents retrieved. Possible root causes include Hardware Failure, Software Failure, and Network Cable. Enter the root cause in the box, or click the icon to open the Root Cause Selection window so you can search for and can select one. When you click Search, the product returns only documents that are associated with the specified root cause.

- **Priority/Severity/Impact/Urgency**
  Specifies the level (1, 2, 3, 4, 5, or None) by which to filter documents retrieved. When you leave <empty> as the field value, the product does not consider a level when filtering documents. When you click Search, the product returns only documents with the specified level.

> You can click the More icon to display the Additional Search Arguments field. This field is intended only for expert users who understand SQL and Majic. You can enter a SQL WHERE clause in this field to specify an additional search argument.

Manage Document Versions

Using the document versioning capabilities of Knowledge Management, an analyst with editing privileges can create a *Rework-Draft* version of a document. A rework version starts as a copy of the document that is replaced in the knowledge base after it is verified and republished. The need to unpublish the document first is avoided.

Users with editing privileges can also perform the following versioning tasks:

- Save a draft version of a document.
- Roll back to a previous version if a problem with the current version occurs (Draft or Published). The Versions tab on the Update Document page is where users can select different versions for rollback to replace the current version.
- Track the number of document versions that are saved, deleted, and archived in the knowledge base.

The Knowledge Documents Inbox on the CA SDM Scoreboard is the repository for documents in all statuses including saved and assigned draft and rework-draft documents.

Administrators can set up and can manage document versions by performing the following steps:

1. Identify who can edit published documents and can create the Rework-Draft versions. The role being used for a particular contact record controls editing privileges.
2. Define an approval process template that groups tasks or steps to complete during the document lifecycle. By default, a built-in approval process template allows users to create documents.
3. Determine whether to use the document approval process. Analysts who are permitted to bypass the approval process can identify which tasks they want to start with when they create a Rework-Draft version.
4. Create archive and purge rules for document version maintenance.

Create Knowledge Document Links

You can maintain your Knowledge Management environment by creating document links. Knowledge relationships let you create document hierarchies and manage changes to your knowledge documents.

Follow these steps:

1. Define knowledge document templates to display or hide the parent-child relationships in view mode.

2. Create or modify a knowledge document. You can only add links to an unpublished knowledge document by default. If the document is already published, open the document in edit or rework mode to create document links. You can modify the permissions for documents before the approval process and after publishing.

3. Create *any* of the following document links from the Related Knowledge tab, as appropriate to your Knowledge Management environment:

   - Link the document as a non-hierarchal See Also to link knowledge documents to other existing documents. Right-click the document in the Documents pane and select the option *Link this Document as See Also*.

   - Link the document as a parent or child. Right-click the document in the Documents pane and select the *Link this as Parent* or *Link this as Child* option to create the link between the documents. If you modify a parent document, an alert appears saying that child documents can be affected.

   - Link the global document to a tenanted document.
     You can link knowledge documents to a single tenant, or to multiple tenants. For example, a child document can have a different tenant than the parent document.

   The History tab updates when you create document links to help track changes.

4. Save the document and verify that the links appear when opening the document in User View. You can verify that the document links appear according to the permissions you established.

Create Action Content

Content

You can create "action content" (a live URL), which can be inserted into the Resolution field of a knowledge document. When the end user click the action content, it creates an incident, or performs some other action. Using action content, a substantial degree of definition and classification can be achieved without the user even realizing it.

The steps to insert a live "action content" link into a document are simple and no coding is required. The Knowledge Management HTML editor handles the generation of the HTML code.

Action content is primarily used for interaction with external applications.

Create Action Content (Action URL)

You can create Action Content for a knowledge documents. These action URLs can launch a live website that is accessible to all users of your system. You can also link action URLs to automated tasks on your server (any server where the KT daemon is running), and you can embed these scripts into knowledge documents, tree documents, document templates, and knowledge forums.

Follow these steps:

1. On the **Administration** tab, browse to **Knowledge**, **Action Content**.
   The Action Content list page appears.

2. Click **Create New**.
   The Create New Action Content page displays.

3. Complete the fields. The following fields require explanation:

   - **Code**
     Specifies a unique identifier for this action content item.

   - **Use Internal HTMPL**
     Creates an internal link (see page 2753)in the application that dynamically passes information, such as the user name and session ID, from knowledge documents into third-party applications. Do not select this option.

   - **Action URL**
     Specifies a URL that links to a web page, template, or automated script, for example: http://www.ca.com.

4. Click **Save**.
   The action content is created.

Create Action Content (Internal HTMPL)

These action URLs can launch self-service scripts and also third-party applications. This link is generated dynamically and automatically transfers attributes about the user, such as the user name, to the target application (http://www.ca.com?USERNAME=BBB, for example). User attributes are specified in an HTMPL file.

Follow these steps:

1. Create an internal HTMPL file that passes data to the target application.

   Note: The act_content_sample.htmpl file is available in the following location: NX_ROOT\bopcfg\www\htmpl\default.

2. Save the HTMPL file in the following location: NX_ROOT\site\mods\www\htmpl\default directory.

3. From the **Administration** tab, navigate to **Knowledge**, **Action Content**.
   The Action Content list page appears.

4. Click **Create New**.
   The Create New Action Content page appears.

5. Specify a unique identifier for this action content item in the **Code** field.

6. Select the **Use Internal HTMPL** check box.

7. Specify the appropriate HTMPL file in the Action URL field, for example: act_content_sample.htmpl

   Note: You can use Support Automation scripts by using the format *SA_SCRIPT=[Self-Service Script ID]* in the URL.

8. Click **Save**.
   The action content is created. When the user clicks this Action Content link within a knowledge document, attributes about the user, such as the user name, are dynamically passed on to the target application.

Create Knowledge Tree Documents

The Knowledge Tree Designer is a visual tool that is used to create knowledge trees quickly and easily. A knowledge tree is a representation of expert knowledge in a particular area. The Knowledge Tree Designer lets analysts and knowledge engineers build detailed trees that guide the user through a series of questions and potential answers until they reach a resolution. This tool eliminates the need for specialized scripting or programming skills and only involves an analyst working with a subject expert to create a tree design.

Knowledge trees can be complex in design. Therefore, it is recommended that you construct a diagram to map the design before creating a knowledge tree. The diagram must contain a series of question, possible responses, and associated resolutions. The hierarchy of questions and responses in the diagram you construct is the foundation on which the knowledge tree is built.

After you have mapped out a diagram of your knowledge tree, you build the tree using the Knowledge Tree Designer.

You can create a Knowledge Tree Document from the Knowledge tab.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. Select the desired knowledge category.

2. Click File, New Knowledge Tree Document.

Note: You cannot create a document directly under the TOP category. If necessary, add a new category in which to create the document.

3. Complete the required fields.
4. Choose a Document Template from the drop-down.
5. Click Save.
6. Click Design Tree on the Content tab to edit the knowledge tree in the Tree Designer (see page 2754).

Use the Tree Designer

The Knowledge Tree Designer tool employs rule-based modeling functionality that helps you develop and deploy business policies and intelligence by mapping any reasoning process into a knowledge tree structure. The knowledge tree is perfectly suited to guiding users through a logical process such as changing a toner cartridge in a printer or changing a hard drive in a server.

You can view the Tree Designer when you open a Knowledge Tree Document for editing.

Follow these steps:

1. Create or Edit a Knowledge Tree Document.
   The document opens.

   Note: If the document has been published, you may need to unpublish it before you can view it.

2. Click Design Tree on the Content tab.
   The Tree Designer opens.

   Note: You cannot perform any add or edit actions on the primary node. For example, you cannot add a query or conclusion to a primary node.

3. Click Node Actions, and select one of the following nodes:

   - Add Query (see page 2762)
     Allows you to write a question.
   - Add Conclusion (see page 2760)
     Allows you to write an answer.

- Link Jump Node (see page 2761)
  Links the currently selected jump node to the next node you select. You cannot link a jump node to the primary node or to another jump node.

- **Add Jump**
  Allows you to link to another document.

- **Delete**
  Deletes the currently selected node and its subnodes from the knowledge tree without putting them on the clipboard.

  Note: When you delete a query node, the query and its responses are removed from the knowledge tree. You cannot delete the primary node.

You can use the Quick View or HTML Source to modify the appearance of the nodes.

4. Click the Edit menu to perform copy and paste operations.

   Note: Use the Copy option to copy of the currently selected node (and its subnodes). Use the Copy Single Node option to copy the currently selected node (but not its subnodes or responses).

5. Click the Options menu to personalize your interaction with the Tree Designer. This menu contains the following commands:

   - **Copy Response**
     Specifies whether to use response text as the name of an associated node when you create it.

     - Select this command to automatically use the text of a node as its name when you create it. When the command is active, a check mark displays to the left of the command name on the menu.

     - Clear this command to use the default name (Default Node Name) when you create a node. You can use the Rename command on the Node Actions menu to change the name of the node.

     This command is also available on the shortcut menu that opens when you right-click a node in the Tree pane.

   - **Prompt on Node Delete**
     Specifies whether the Tree Designer prompts you before deleting nodes.

     - Select this command to display a confirmation prompt before deleting nodes. When the command is active, a check mark displays to the left of the command name on the menu.

- Clear this command if you do not want the Tree Designer to prompt you to confirm node deletion.

This command is also available on the shortcut menu that opens when you right-click a node in the Tree pane.

6. Click the Quick View option to view a preview of the node design.

7. Click Save.
   The Knowledge Tree Document is saved as a draft.

Access Knowledge Documents from the Self-Service Interface

This article contains the following topics:

Knowledge Submission from Self-Service

By default, any user that is logged in to Knowledge Management can submit knowledge for consideration . This page lets a customer submit knowledge without contacting their local service desk representative. After you submit knowledge, it passes through a publishing process. During this process, the knowledge is reviewed and edited before it is added to the knowledge base.

Specify information into every field that appears in the Submit Knowledge page. Pay special attention when completing the Summary field. Typically, this field contains a succinct overview of the document that you are submitting.

Knowledge Search

Knowledge Management provides users with the following options for retrieving knowledge:

- **Category browsing**
  Finds the solutions that are based on categories. In each category, additional subcategories can narrow the search results to a set of solutions that are likely to be most relevant to an issue.

Note: When you search for knowledge documents using the category, the search result displays the keyword count and the list of documents. The count within the parentheses is the total number of documents in the knowledge base that contains at least one occurrence of the keyword. For example, when searching for the string, "live assistance", if 3 documents each contain that keyword at least once, then "live assistance(3)" is displayed.

The count is not filtered according to the specified search criteria. So, it may not match the number of documents that are listed. Additionally, the count only includes documents that have been processed by pdm_k_reindex. So, documents which contain the specified string but which have been published after the most recent pmd_k_reindex are not included in the count.

To turn off the parenthesized count, add the following code to the $NX_ROOT/NX.env file:

```
@EBR_SHOW_WORDS_DF=No
```

- **Knowledge tree**
  Asks a series of questions to guide the user to possible solutions. The responses lead the individual to a solution that appears to be most relevant.

- **Bookmark**
  Provides access to frequently viewed documents that are included in a bookmark list.

Advanced Search

In Advanced Search Settings, customers and employees can use the following options to refine a search for the solution to a problem:

- **Knowledge Management Search**
  Searches for certain keywords, which serve as preliminary matches.

- **Natural Language Search**
  Searches for words and accounts for word proximity, word order, and relevance.

The search results are listed by relevance. The relevance is determined by the specified search criteria (expressed as EXCELLENT, GOOD, and so on). Documents with the highest relevance (EXCELLENT) are listed first.

Each result can include a title that appears as a link, a summary of the document, and additional statistics relevant to the document, such as Relevance Rating, Document ID, Modify Date, FAQ Rating, and Hits Received.

Depending on how the system administrator configures Knowledge Management, users can open an incident, rate a document, and can provide comments when a knowledge document is open.

Document Browsing and Bookmarking

You can categorize knowledge documents to let customers browse for information that is based on frequently asked questions (FAQs). By selecting a knowledge category, the related subcategories and knowledge documents appear. You can select the document that you would like to view or select a subcategory to narrow your search further.

To enhance self-service capabilities, a dynamic list of the most frequently used documents appear.

Note: Users can specify criteria about an item of interest and the search engine finds the matching knowledge documents and displays them on the search results page as a set of "recommended document" links. The search query can be expressed as a keyword or set of words (phrase) that identify the desired concept that one or more documents possibly contain. For more information, see Create New Recommended Documents (see page).

You can bookmark the document for easy access. The My Bookmarks folder stores links to the most frequently referenced documents. When you click My Bookmarks in the Category pane on the Knowledge tab, the list of bookmarked documents displays in the Knowledge Document List pane.

Incidents and Problems

Customers sometimes encounter problems that cannot be solved simply by searching for knowledge. Not all problems have a direct solution in the knowledge base. When a customer has a problem that cannot be solved, they can create an incident that is sent to an analyst for further processing. The incident describes the problem, and it can also be based on an existing knowledge document. The more information that is added to an incident, the easier it is for the analyst to solve.

Many ITIL-defined activities are supported in Knowledge Management, including the following activities:

- Incident Management
  - Knowledge searches can help find known errors during further incident investigation and diagnosis
  - Incident categorization
- Problem Management
  - Accessing information about known errors, and helping with problem matching to obtain the resolution when the problem has occurred before
  - Maintaining and providing access to information about workarounds
  - Recording information about procedures, work instructions, diagnostic scripts, and known errors (while supporting rich content, editing tools, measurement, and a definable approval process for the development of resolutions)
  - Problem analysis (through the linkage and analysis of incidents)

How to Use the Tree Designer

Contents

- Add the Tree Description (see page 2763)
- Add the Displayed Text for a Node (see page 2763)
- Add the Response Text for a Node (see page 2764)
- Check a Knowledge Tree for Errors (see page 2764)
- Set Tree Designer Options (see page 2764)

The following topics provide procedures for using the Tree Designer to create and edit knowledge trees.

Tree Pane

The Tree pane displays the nodes that comprise the knowledge tree. Each node represents a step in the process that is presented by the knowledge tree. A well-constructed knowledge tree guides the user along a systematic path to answering a question, resolving a problem, or completing a process. Click ⊞ or ⊟ as appropriate to open or close nodes in the Tree pane. When you click a node in the Tree pane, the associated information displays in the right pane.

The following information displays in the right pane of the Tree Designer window when you select a node in the Tree pane:

Icon	Node Type	Right Pane Display
 BSVC_r12.1--Tree pane (3)	Primary	Tree Description (HTML) pane
 BSVC_r12.1--Tree pane (4)	Query	Query Text (HTML) pane
 BSVC_r12.1--Tree pane (5)	Conclusion	Conclusion Text (HTML) pane
 BSVC_r12.1--Tree pane (6)	Jump	N/A

You can right-click a node in the Tree pane to open a shortcut menu that contains a subset of the menu commands.

Note: The right pane is empty when you select a Jump node.

Add a Conclusion Node

Use a conclusion node to describe the resolution for a particular problem, the final step in a procedure, or a possible termination point in a query. The Conclusion nodes do not have subnodes. You would not typically nest a conclusion node immediately beneath the root node of a knowledge tree. You can add up to seven subnodes to a query node.

Follow these steps:

1. Select the query node under which to add the conclusion node in the Tree pane.
   The Query Text (HTML) pane opens.

2. Click Add Conclusion.
   The Tree Designer adds a conclusion node below the selected node in the Tree pane and adds a response field in the Query Text (HTML) pane.

3. Enter a response to the question or statement that is posed in the parent node in the new field in the Query Text (HTML) pane.

4. (Optional) To rename the new node, right-click it in the Tree pane, then select Rename from the shortcut menu. The Prompt window opens. Enter a new name for the node and click OK to close the Prompt window. The Tree pane refreshes to show the new node name.

5. Select the new conclusion node in the Tree pane.
   The Conclusion Text (HTML) pane opens.

6. Do one of the following actions in the Conclusion Text (HTML) pane:

   - Enter the displayed text (that is, the information that is associated with the node) in the Conclusion Text (HTML) box. You can use plain text or can enter HTML codes as appropriate. To preview the text as it appears at run time, select the Quick View option.

   - Click Edit Conclusion Text (HTML) to open the HTML Editor so you can design the information that is associated with the node in WYSIWYG (what you see is what you get) format. When you finish editing the information, click OK to save your work and close the HTML Editor.

7. Click Save.
   The Tree Designer saves your changes.

Add a Jump Node

Use a jump node to link to previously defined nodes in the knowledge tree. For example, if the answer to the query posed in a parent node requires repetition of previous steps in a procedure. Jump nodes do not have subnodes. You would not typically nest a jump node immediately beneath the root node of a knowledge tree.

Follow these steps:

1. Select the query node under which to add the jump node in the Tree pane.
   The Query Text (HTML) pane opens.

2. Click Add Jump.
   The Tree Designer adds a jump node below the selected node in the Tree pane and adds a response field in the Query Text (HTML) pane.

3. Enter a response to the question or statement that is posed in the parent node in the new field in the Query Text (HTML) pane.

4. Right-click the new jump node in the Tree pane, then select Link Jump Node from the shortcut menu.

5. Select the query or conclusion node to which to link the jump node in the Tree pane.
   The jump node's name in the Tree pane changes to include the name of the linked query or conclusion node. For example, if you linked a node that is called "Wednesday", the jump node name changes to "NODE: Wednesday." When a user selects the jump node in the knowledge tree at runtime, the linked query or conclusion node displays.

6. Click Save.
   The Tree Designer saves your changes.

Add a Query Node

Use a query node to supply a possible answer to the question posed in its parent node and to serve as a parent node for further subnodes in the tree. The query text typically contains a question (the answer to which determines the next node in the tree) or a step in a procedure. The query nodes can have conclusion nodes, jump nodes, and other query nodes as subnodes.

Note: You can add up to seven subnodes to a query node.

Follow these steps:

1. Select the query node under which to add the new query node in the Tree pane.
   The Query Text (HTML) pane opens.

2. Click Add Query.
   The Tree Designer adds a query node below the selected node in the Tree pane and adds a response field in the Query Text (HTML) pane.

3. Enter a response to the question or statement that is posed in the parent node in the new field in the Query Text (HTML) pane.

4. (Optional) To rename the new node, right-click it in the Tree pane, then select Rename from the shortcut menu. The Prompt window opens. Enter a new name for the node and click OK to close the Prompt window. The Tree pane refreshes to show the new node name.

5. Select the new query node in the Tree pane.
   The Query Text (HTML) pane opens.

6. Do one of the following actions in the Query Text (HTML) pane:

   - Enter the displayed text (that is, the information that is associated with the node) in the Query Text (HTML) box. You can use plain text or can enter HTML codes as appropriate. To preview the text as it appears at run time, select the Quick View option.

   - Click Edit Query Text (HTML) to open the HTML Editor so you can design the information that is associated with the node in WYSIWYG (what you see is what you get) format. When you finish editing the information, click OK to save your work and close the HTML Editor.

7. Click Save.
   The Tree Designer saves your changes.

Add the Tree Description

The tree description displays at runtime when a user clicks the Tree Description link while viewing a knowledge tree document in tree view. For example, if you design a knowledge tree to help a customer choose a credit card, you can define a tree description such as "Use this document to find the best credit card for you."

Follow these steps:

1. Select the knowledge tree's primary node in the Tree pane.
   The Tree Description (HTML) pane opens.

2. Do one of the following action in the Tree Description (HTML) pane:

   - Enter the displayed text (that is, the information for the tree description) in the Tree Description (HTML) box. You can use plain text or can enter HTML codes as appropriate. To preview the text as it appears at run time, select the Quick View option.

   - Click Edit Tree Description (HTML) to open the HTML Editor so you can design the tree description in WYSIWYG (what you see is what you get) format. When you finish editing the information, click OK to save your work and close the HTML Editor.

3. Click Save.
   The Tree Designer saves your changes.

Add the Displayed Text for a Node

Use the Tree Description (HTML), Query Text (HTML), and Conclusion Text (HTML) panes to design the information that is displayed for a particular node. The displayed text presents the description of the knowledge tree, poses a question, or presents information to help the user navigate the knowledge tree.

Follow these steps:

1. Select the primary node, query node, or conclusion node for which to add displayed text in the Tree pane.
   Depending upon the node you selected, one of the following panes opens:
   If you selected the primary node, the Tree Description (HTML) pane opens.

   - If you selected a query node, the Query Text (HTML) pane opens.

   - If you selected a conclusion node, the Conclusion Text (HTML) pane opens.

2. Do one of the following actions in the Tree Description (HTML), Query Text (HTML), or Conclusion Text (HTML) pane:

   - Enter the displayed text (that is, the information that is associated with the node) in the field provided. You can use plain text or can enter HTML codes as appropriate. To preview the text as it appears at runtime, select the Quick View option.

- Click the Edit *xxx* (HTML) button to open the HTML Editor so you can design the information that is associated with the node in WYSIWYG (what you see is what you get) format. When you finish editing the information, click OK to save your work and close the HTML Editor.

3. Click Save.
   The Tree Designer saves your changes.

Add the Response Text for a Node

When you add a node to an existing query node in the Tree pane, the Tree Designer adds a response box for the added node in the right pane. Use the box to specify a response to the question or statement posed in the Query Text (HTML) pane.

Follow these steps:

1. Select the query node that contains the node for which to add response text in the Tree pane.
   The Query Text (HTML) pane opens.

2. Locate the response box for which to specify text in the Query Text (HTML) pane, then enter a response to the question or statement that is posed by the parent node.

   Note: By default, the response text you enter replaces the node name in the Tree pane (that is, the Tree Designer synchronizes the response text and the node name). To disable synchronization, select the Copy Response command from the Options menu to clear the check mark from it.

3. Click Save.
   The Tree Designer saves your changes.

Check a Knowledge Tree for Errors

Follow these steps:

1. Select Check Errors from the Tree menu.
   The Tree Designer scans the knowledge tree for missing displayed text, responses, and links, then displays the results in the Errors pane at the bottom of the window.

2. Select an error in the Errors pane to display its associated node.
   The Tree Designer selects the node in the Tree pane and displays its definition in the right pane.

3. Correct the indicated error.

4. Click Save.
   The Tree Designer saves your changes.

Set Tree Designer Options

Use the commands on the Options menu to control certain Tree Designer behaviors, as follows:

- To set whether the Tree Designer uses response text as the name of an associated node, select Copy Response from the Options menu.
  - If a check mark displays next to the command on the menu, the option is active and the response text you specify for a node replaces its name in the Tree pane. This is the default setting.
  - If no check mark displays, the option is inactive and you manually rename the node.
- To set whether the Tree Designer prompts you before deleting a node, Select Prompt on Node Delete from the Options menu.
  - If a check mark displays next to the command on the menu, the option is active and the Tree Designer displays a confirmation prompt when you attempt to delete a node. Click OK to close the prompt and delete the node and its subnodes. This is the default setting.
  - If no check mark displays, the option is inactive and the Tree Designer deletes the selected node and its subnodes without displaying a confirmation prompt.

Administering Knowledge Management

This article contains the following topics:

Document Permissions

You can set, view, and edit permissions for a document. These permissions can be assigned to different groups of individuals. When setting permissions, you can decide to inherit permissions from the primary category of a document or can specify new permissions. By default, documents inherit their permissions from their primary category. This default handles access permissions at the category level rather than the document level.

Important! When creating a knowledge document, verify that document permissions include users that can be later assigned on the document through the approval process. When a group is assigned to a document, users from that group may not have the permission to view the document. If the document is assigned to a specific user, default data partition constraints allow the user to view the document.

Version Documents

Using the document versioning capabilities of Knowledge Management, an analyst with editing privileges can create a *Rework-Draft* version of a document. A rework version starts as a copy of the document that is replaced in the knowledge base after it is verified and republished. The need to unpublish the document first is avoided.

Users with editing privileges can also perform the following versioning tasks:

- Save a draft version of a document.
- Roll back to a previous version if a problem with the current version occurs (Draft or Published). The Versions tab on the Update Document page is where users can select different versions for rollback to replace the current version.
- Track the number of document versions that are saved, deleted, and archived in the knowledge base.

The Knowledge Documents Inbox on the CA SDM Scoreboard is the repository for documents in all statuses including saved and assigned draft and rework-draft documents.

How to Manage Document Versions

Administrators can set up and can manage document versions by performing the following steps:

1. Identify who can edit published documents and can create the Rework-Draft versions. The role being used for a particular contact record controls editing privileges.
2. Define an approval process template that groups tasks or steps to complete during the document lifecycle. By default, a built-in approval process template allows users to create documents.
3. Determine whether to use the document approval process. Analysts who are permitted to bypass the approval process can identify which tasks they want to start with when they create a Rework-Draft version.
4. Create archive and purge rules for document version maintenance.

Document Expiration

When a published document reaches its expiration date, the product typically retires it (removes the document from the knowledge base and the approval process).

Document Archive and Purge

You can manage the size of your knowledge pool by using Archive and Purge, which removes old and unused documents automatically. Archive and Purge improve the efficiency of knowledge searches by returning only current documents.

Archive and Purge run as a background process and automatically removes inactive records in the CA SDM database according to rules that you configure. These rules act on CA SDM objects at specific time intervals.

Manage Export/ Import of Knowledge Documents

Contents

Knowledge Base Re-Index

The following changes to search settings require that you re-index the knowledge base using the Knowledge Re-index utility:

- After importing knowledge
- After changing parse settings
- After mass deletions
- When search failures occur

Re-indexing is necessary because existing documents do not reflect any changes that are made to the synonyms, noise words, special terms, and other research parameters until they have been re-indexed. All new synonyms, noise words, and special terms must be re-indexed to help ensure that keyword searches of the knowledge base are current and accurate.

You run Knowledge Re-index from the command line. The pdm_k_reindex.exe command is the executable file for Knowledge re-index.

Note: Re-indexing the documents in the knowledge base can be a time-consuming operation, depending on the size of your database. We recommend that you run the Knowledge Re-index utility after all changes have been added.

Export or Import Log Files

You can sort transactions by package, template, and status. All KEIT transactions are recorded in the following log files:

- **stdlog**
  Logs CA SDM information.
- **keitstat.log**
  Provides statistical information on the KEIT operation.
- **keitinfo.log**
  Provides detailed information on the KEIT operation.

If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

How to Export/Import Knowledge Documents

The Knowledge Management Export/Import tool (KEIT) migrates and synchronizes data between different Knowledge Management systems and enables export/import of Knowledge Documents. Use this tool to define export/import transactions.

Note: If multi-tenancy is installed, all tenanted and public categories that were imported from a previous system display as public in the new multi-tenancy system, but imported documents can be tenant-specific.

Follow these steps:

1. Allow Users to Export or Import Transactions (see page 2768).
2. Define the Export Import Directories (see page 2769)
3. Create an Export/Import Template (see page 2770)
4. Export and Import Transactions (see page 2773)

Allow Users to Export or Import Transactions

You can allow analysts to grant export and import permissions by managing your role list on the Administration tab.

Follow these steps:

1. Navigate to Security and Role Management, Role Management, Role List.
   The Role List appears.
2. Select a role with the Analyst Interface Type.
   The Role Detail page appears.
3. Click Edit.
   The Update Role page appears.
4. Click the Knowledge tab and select the options depending on the permissions that you want to grant.

5. Click Save.
   The Role Detail page reappears.
   Review your changes in the Knowledge tab and close the Role Detail page. You can also restrict users from exporting/importing by clearing the check boxes on the Knowledge tab of the Role Detail page.

Define the Export Import Directories

Follow these steps:

1. Select the **General Setting** page under **Administrator** tab, update the **Path For Knowledge Import/Export Files** option to define package directories.
   - (Conventional configuration) By default it uses "$NX_ROOT/site/keit". Restart the CA SDM servers after changing this path. Packages are stored in the following default directories:
     - Export Packages: $NX_ROOT/site/keit/export
     - Import Packages: $NX_ROOT/site/keit/import
   - (Advance Availability Configuration) This path must be UNC shared drive. Restart the CA SDM servers after changing this path. Packages are stored in the following directories:
     - Export Packages: *UNC Shared Location/*export
     - Import Packages: *UNC Shared Location/*import
2. To add attributes for the export/import availability, add the following attribute names to the NX.env file:
   - **@NX_KEIT_AVAILABLE_FIELDS**
     Adds the attribute name.
   - **@NX_KET_ADDL_FIELDS**
     Adds the attribute name, and if the new attribute is a SREL to another object, adds the attribute name that is used to synchronize the source and target systems.
     Example: Add Attributes
     @NX_KEIT_ADDL_FIELDS = STATUS_ID.STATUS,DOC_TEMPLATE_ID.TEMPLATE_NAME

   The export and import directories contain the following files:

   - **keit_config.xml**
     Contains the configuration file for an export or import package.
   - **data.xml**
     Contains the data file containing values of knowledge documents.
   - **rep.xml**
     Contains the repositories that are referenced in the data.xml file.
   - **images**
     Specifies the image files that are embedded in knowledge documents.

Create an Export/Import Template

You can create and modify a template using the Knowledge Export/Import Template Settings page in the Administration tab.

Follow these steps:

1. On the Administration tab, browse to Knowledge, Documents, Export/Import, Export/Import Templates.
   The Knowledge Export/Import Templates List appears.

2. Click Create New.
   The Create New Export/Import Template page appears.

3. Complete the following fields:

   - **Template Name**
     Identifies the name of the template.

   - **Description**
     Provides a brief description of the template.

4. Complete the appropriate fields on the following tabs:

   - Export Fields (see page)

   - Export Filter (see page)

   - Import Settings (see page)

5. Click Save.
   The template is created.

Export Fields

The Export Fields tab appears and contains the following fields:

- **Available**
  Displays the Knowledge Document fields that are available for export.

  Note: If you want to preserve status of the documents, such as Draft, for the export and import process, add STATUS_ID to the Exported column.

- **Exported**
  Specifies document fields to export.

- **Export Attachments**
  Exports the Knowledge Document file attachments.

You can use the arrows in the Select Document Attributes section to add document attributes export.

Note: If you edit the export/import template using Firefox, the list size does not change after you use the arrows in the first edit. Close and reopen the template in edit mode, and using the arrows again causes changes to the list size. This behavior does not occur when you use Internet Explorer.

Important! The exported fields in the KEIT have a higher priority than when the fields are selected as defaults in the Import Settings tab. If you select a default export field in the Import Settings tab, it is not processed as the default field.

Export Filter

The Export Filter tab appears and contains the following fields:

- **Category**
  Opens the Knowledge Category page. Use this option to add categories to the list on the Export Filter tab.
- **Remove Category**
  Removes categories from the list on the Export Filter tab.
- **Clear Category**
  Clears the category list on the Export Filter tab.
- **Include child categories**
  Exports the documents from child categories of exported categories.
- **Include secondary categories**
  Exports secondary categories of exported documents.
- **Include all documents linked to selected categories**
  Exports all documents that are linked to selected categories.

  Note: Enabled only if you select Include secondary categories.
- **Additional Filter**
  Provides an additional WHERE clause.

Import Settings

The Import Settings tab appears and contains the following fields:

- **Error Threshold (%)**
  Stops the import process (sets the status to Failed) if the percent of errors exceeds the specified number.

- **Override published documents**
  Allows imported documents to override published documents of the CA SDM server.

- **Override documents in all non-published statuses**
  Allows imported documents to override non-published documents of the CA SDM server.

- **Use default values when overriding documents**
  Uses default values on overridden documents for defined fields.

- **Index documents immediately**
  Indexes the document after the import process.

- **Status**
  Select Draft, Published or Retired.

- **Priority**
  Sets the priority level of the import settings.

- **Template**
  Selects one of the following default templates:

  - Built in - Knowledge Document
  - Built in - Knowledge Tree
  - Built in - Quick Editing

- **Owner**
  Allows you to set the owner by opening the Contact Search page.

- **Author**
  Allows you to set the author by opening the Contact Search page.

- **Subject Expert**
  Allows you to set the subject expert by opening the Contact Search page.

- **Assignee**
  Allows you to set the assignee by opening the Contact Search page.

- **Expiration date**
  Opens the date helper.

- **Review Date**
  Opens the date helper.

- **Product ID**
  Allows you to set the product ID by opening the Product Search page.

- **Asset**
  Opens the Configuration Item Search page.

- **Root Cause**
  Opens the Root Cause Search page.

- **Service Desk Priority**
  Sets the Service Desk priority of the import settings.

- **Severity**
  Sets the severity level of the import settings.

- **Impact**
  Sets the impact level of the import settings.

- **Urgency**
  Sets the urgency level of the import settings.

Export and Import Transactions

Follow these steps:

1. Export the data to another system by clicking **Export** on the **Export/Import Template Detail** page or by running the pdm_ket utility (see page).

   Note: In the advanced availability configuration, you cannot export packages from the application server using web interface. Use the pdm_ket utility to export packages from any server.

2. Import knowledge data from the package by performing any of the following actions, depending on your CA SDM configuration:

   - In the conventional configuration, copy the desired knowledge package from the default $NX_ROOT/site/keit/export directory and place it in the $NX_ROOT/site/keit/import directory. On the **Knowledge Import Packages List** page, right-click a knowledge package, and click **Import** on the shortcut menu.

   - In the advanced availability configuration, copy the desired knowledge package from the *UNC Shared Location*/export directory and place it in the *UNC Shared Location*/import directory. You cannot import packages from the application server using web interface. Use the pdm_kit_txt utility (see page 2775) to import packages from any server.

     Note: The knowledge package name must start with "package_" prefix for it to be listed in the Knowledge Import page.

     Important! The r11.0 import utility has been renamed pdm_kit_txt.exe to allow importing r11.0 text files. This utility does not support any of the r12.0 import enhancements.

3. Documents that are not indexed after import are stored in the Unindexed queue on the scoreboard. Users cannot search for unindexed documents, therefore, they do not appear on the Document list. To display this queue, select the **Service Desk** tab, **Knowledge Documents**, **Unindexed**. You can import knowledge data when the Index Document option is enabled. If Knowledge Documents are imported with the option disabled, you cannot search the documents after importing. Run pdm_k_reindex to make the documents searchable.

If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

Knowledge Export/Import CLI

Contents

pdm_ket Utility -- Knowledge Management Export Tool

The pdm_ket utility exports knowledge from a source computer to a knowledge package, using a template that is created from the web interface.

Attachments and their links are exported to data.xml during the export. Before you import the attachments, manually move them to following directory on the background server:

$NX_ROOT/site/attachments/default

Note: For advanced availability configuration, you can execute the pdm_ket utility using attachments UNC path.

Use this utility to do the following tasks:

- Create configuration file based on the related knowledge export template.
- Export data with UUID of document, and content such as title, summary, problem, resolution and other document attributes like owner, status, and so on.
- Export all unique images that are used by the exported documents (always exported).
- Export all unique attachments that are used by the exported documents (EXP_ATTMNT field). The files are copied from the remote repository to the local package folder.

The utility is invoked as follows:

```
pdm_ket -n <template name> [-h] ]-v]
```

- **-n <template name>**
  Defines the name of the template that is used for export (case sensitive).

- **-h**
  (Optional) Displays help on the utility.

- **-v**
  (Optional) Enables extensive logging (bop_logging) of program events. This option is commonly used for internal problem solving.

Example: Using pdm_ket to Export Knowledge Using the my_template Template.

```
pdm_ket -n my_template
```

The pdm_ket utility can be scheduled using a third-party scheduler for exporting Knowledge Documents.

pdm_kit Utility -- Knowledge Import Tool

The pdm_kit utility imports data to the destination server according to the settings in the configuration file of a package.

Important! Before you execute the pdm_kit utility from the application server, ensure that the path (local or UNC) of the package is accessible by the background server. If the background server is not able to access this path, the package is not imported from the application server.**Important!** The r11.0 import utility has been renamed to pdm_kit_txt. exe to allow importing r11.0 text files. This utility does not support any of the Release 12.9 import enhancements.

The referenced data that is previously referenced by the pdm_ket utility gets the real UUID or ID value of the destination server. When running pdm_kit utility a new userid parameter is applied. The pdm_kit utility works as follows:

1. Imports the documents by replacing the userid value (for contacts) or referenced name (for fields like asset) with appropriate UUID of the destination server.
2. Imports the images.
3. Imports the attachments.
4. Uploads the files from the local package folder to the remote repositories.

Note: If editing published documents is disabled, then the imported document is created as a rework version.

The utility is invoked as follows:

```
pdm_kit [-h] -f -u [-v]
```

- **-h**
  (Optional) Displays help for the utility on the interface.
- **-f**
  Specifies the path to the package.
- **-u**
  Specifies the default user.
- **-v**
  (Optional) Enables extensive logging (bop_logging) of program events. This option is commonly used for internal problem solving.

Note: For advanced availability configuration, you can execute the pdm_kit utility on background server. For Windows, you can also execute the pdm_kit utility on application server if the package resides in a UNC shared drive. For non-windows platform, you cannot execute pdm_kit utility on application server.

Example: Using pdm_kit to Import a Package

```
pdm_kit -f c:\package_path -u ServiceDesk
```

Managing Automated Policies

Contents

An automated policy describes the condition by which documents are flagged for correction and are promoted to publication or retirement throughout the various stages of the document lifecycle process. For example, you can specify the "fix broken links" default policy that matches documents that are found in the knowledge base with broken links. The task of fixing the problem can be assigned to an analyst.

Administrators can automate certain tasks in the knowledge document approval process that is based on document lifecycle policies and actions they define. By automating tasks, end users who are searching for solutions can solve problems faster, and they can do so without contacting other individuals, which provides a benefit to the organization.

Automated policies work with events and macros. Each policy is associated with the following components:

- **Stored Query:** Contains a set of action macros that execute when the policies identify and match a document during processing. After processing, the stored query condition event displays a role-based Knowledge Management lifecycle policy report on the CA SDM Scoreboard. The administrator is responsible for monitoring the reports and for providing feedback and recommendations to the appropriate document editors.
- **Action Macro:** Contains code that lets users set a flag, increase the priority, or perform some other action. You can modify the macros that appear on the Macro list, or can define your own.

How to Set Up Automated Policies

Administrators can set up the Automated Policies feature by performing the following steps:

1. A batch process must be defined in the Automated Policies Scheduler that executes on the background server to present the data that is required to view the Knowledge Management Lifecycle Policy reports. This action step also applies to the Knowledge Report Card.
2. For security and role management, define the stage by which users can view and search on documents during their lifecycle on the Knowledge Document Visibility tab in Role Management.
3. On the Automated Policy List page, you can edit the default policies, or can define your own.

Create an Automated Policy

You can create an automated policy that activates when an action occurs, such as when a document is published or retired from the knowledge base.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Important! For new policies, the administrator must include the "Disregard Life Cycle Policies" field in the stored query; otherwise, it does not appear on the Attributes tab.

Follow these steps:

1. Select **Administration** tab, **Knowledge**, **Automated Policies**, **Policies**.
   The Create New Automated Policy page appears.

2. Enter a name and description for the policy in the appropriate fields.

3. Enter a stored query name or select one using the search icon.

4. Click **Add Action**.
   The Macro List page appears.

5. On the Macro List page, select one of the predefined action macros, or define your own (click **Create New**).
   The action macro appears in the Action Information list on the Create New Automated Policy page.

   Note: You can delete an action macro: right-click the name and select Delete from the shortcut menu.

6. Click **Save**.
   The new policy appears in the Automated Policy list.

Run the Automated Policies

The Automated Policies List page contains the details of the policies you can manage. To display this page, select the Administration tab, Knowledge, Automated Policies.

Each policy contains a stored query that executes when documents are matched during processing. After processing completes, a Lifecycle Policy report appears on the CA SDM Scoreboard. To view a report, select Knowledge Documents, Automated Policies. From the scoreboard, the analyst can manage their own documents, and by default, the administrator can manage all documents for each role.

To implement the reports, run a batch process with the Automated Policies Scheduler. The scheduler runs on the following CA SDM server, depending upon the configuration and displays the data that is required to view the reports.

- Conventional:Primary or secondary
- Advanced availability: Background

When you are finished, run the Knowledge Report Card (see page 2818).

Follow these steps:

1. Select the **Administration** tab, **Knowledge**, **Automated Policies**, **Scheduling**.
   The Automated Policies Scheduler appears.

2. Complete the following fields:

   - **Last Updated** -- Select the Run Calculation check box.

- **Schedule** -- Specify a date and time from which CA SDM performs the calculation and runs the policies.

3. Click Save.

View Document LifeCycle Policy Reports

Administrators can view the Document Lifecycle Policy Reports that are generated by the automated policies on the Document List page. Each report is role-specific and provides administrative information about the documents that are flagged for correction and promoted to publication or retirement throughout the various stages of the document lifecycle process.

If multi-tenancy is installed, the list page displays Tenant and Public Data settings in the search filter. Public Data can be Excluded or Included with Tenant data; Only searches for public objects exclusively. On detail pages, select the appropriate tenant from the list. If you select <empty>, the object is public.

Follow these steps:

1. On the **Service Desk** tab, **Knowledge Documents**, **Automated Policies**.
2. Do *one* of the following:
   - **Expand the My Documents** folder to reveal nested folders for your assigned items.
   - **Expand the All Documents** folder to reveal nested folders for all items.
3. Select the folder that you want to view.
   The Document List page displays the following columns:
   - **Title**
     Displays the title of the document that is either flagged for correction or promoted for publication or retirement.
   - **Policy/Actions**
     Displays the policy name and action content defined for the policy.
   - **Attributes**
     Displays the properties of the document that are affected by the policy it is assigned to.

Knowledge Documents Schedule

This article contains the following topics:

- schedConfig Macro -- Configure Schedule (see page 2783)
- schedAttr Macro -- Specify a Stored Attribute (see page 2785)
- schedGroup Macro -- Specify an Event Group (see page 2786)
- The setSchedEvents() JavaScript Function (see page 2787)

The Knowledge Documents Schedule provides Change Managers, Knowledge Managers, and Level 2 Analysts a high-level view of key events in the knowledge management lifecycle. The following events can be scheduled for a Knowledge Document:

- Submission
- Publication
- Review
- Expiration

The Knowledge Management Schedule tab displays a calendar format similar to the Change Calendar, but instead of showing start times and end times, it only shows specific dates.

Configuring scheduling views (see page 2783) involves setting macros statements.

The Knowledge Document Schedule can also be exported to iCalendar format.

Note: When exporting schedules on some calendar programs, selecting the Open option instead of Save causes the file to import incorrectly. To avoid this issue on Knowledge Management and Change Order schedules, select the Save option instead of Open. After you save the exported file, import it through the calendar program interface.

Knowledge Schedule Filter

The Knowledge Schedule Filter displays the following fields:

- **Tenant**
  Filters the search by tenant. This field displays for the privileged user in a multi-tenancy installation.
- **Event Type**
  Filters the search by the following event types:
  - Submission
  - Review
  - Publication
  - Retirement

- **Schedule Start Date**
  Specifies the date for the beginning of a range for filtering the history to show only entries for a specified time frame.

- **Schedule End Date**
  Specifies the date to specify the end of a range for filtering the history to show only entries for a specified time frame.

- **Schedule Timezone**
  Specifies a timezone to view your search results.
  Note: If no timezone is selected, the events are displayed in your current timezone.

- **Owner**
  Defines the name of the contact that is assigned to maintain the document. Enter or search the name of the contact in "last name, first name" format.

- **Assignee**
  Defines the name of the contact that is assigned to handle the record. Enter or search the name of the contact in "last name, first name" format.

- **Subject Expert**
  Defines the name of a contact with expertise in the subject matter of the document . Enter or search the name of the contact in "last name, first name" format.

- **Status**
  Select one of the following document statuses to perform your search:

  - Draft
  - Published
  - Retired

- **Category**
  Defines a category by which to filter documents retrieved. Enter the name of the category in the box or open the Category Search window. When you click Search, the product returns only documents that are associated with the specified category.

- **Initial View**
  Select the view of the Knowledge Management Calendar you want to see:

  - **Month**
    Displays a calendar for the full month that includes the earliest implementation start date that is specified in the Start Date field. The calendar shows abbreviated information about each change within the range (change number, start and end time, and first affected CI).

  - **Week**
    Displays seven consecutive days in a single column, beginning with the earliest implementation start date specified in the Start Date field. The calendar includes summary information about each change within the specified range (change number, start and end time, summary description, assignee, group, and the first ten affected CIs).

- **Day**
  Displays a view similar to the week view, except that it shows only the day that is specified in the Start Date field.

- ***n* Days**
  Displays a view similar to the week view, except that it continues for the specified number of days.

- **List**
  Displays a standard CA SDM list page.

  You can click the More icon to display the Additional Search Arguments field. This field is intended only for expert users who understand SQL and Majic. You can enter a SQL WHERE clause in this field to specify an additional search argument.

Knowledge Schedule Views

The Knowledge Documents Schedule has the following views:

- **Month**
  Displays a calendar for the full month that includes the earliest implementation start date that is specified in the Schedule Start Date field. The calendar shows abbreviated information about each change within the range (change number, start and end time, and first affected CI).
  The Knowledge Documents Schedule has similar functionality to the Change Orders Month view with the following exceptions:

  - Knowledge events only have a date (no time) and event type groups them, similar to change orders that are grouped for each time period and change type.

  - Events types have the following default predefined colors, using the schedGroup macros:

    - Submission -- Black

    - Review -- Green

    - Publication -- Blue

    - Retirement -- Red

  Note: If you see a review date referring to the past, it indicates that the review was probably not done.

- **Week**
  Displays seven consecutive days in a single column, beginning with the earliest implementation start date specified in the Schedule Start Date field. The calendar includes summary information about each change within the specified range (change number, start and end time, summary description, assignee, group, and the first ten affected CIs).

- **Day**
  Displays a view similar to the week view, except that it shows only the day that is specified in the Schedule Start Date field.

- ***n* Days**
  Displays a view similar to the week view, except that it continues for the specified number of days.

- **List**
  Displays a standard CA SDM list page.

Scheduling View Configuration

You configure the monthly and weekly scheduling views by specifying pdm_macro statements in the <head> section of the HTMPL forms defining the schedule. We recommend using the Source View of Web Screen Painter to edit these forms.

Any form that displays a schedule must contain the following:

- A schedConfig macro
- At least one schedAttr macro
- At least one schedGroup macro

The configuration macros are in a separate source file that is referenced by a pdm_include statement in the main source file. This file lets you configure your schedule without modifying the main source file.

For example, the configuration macros for the Change Calendar form list_chgsched.htmpl are in a file named list_chgsched_config.htmpl. For the Knowledge Lifecycle Schedule, you can modify the list_kdsched_config.htmpl using the same macros.

You can find list_chgsched_config.htmpl and list_kdsched_config.htmpl in the following directory:

$NX_ROOT\bopcfg\www\htmpl\web\analyst\

schedConfig Macro -- Configure Schedule

The schedConfig macro specifies that a form contains a schedule and provides basic configuration information. The following values are valid macro arguments:

- **autosearch=1|0**
  Specifies whether the schedule form reloads data from the server when the user selects a view outside the currently selected date range. Setting the value to 1 (default) causes the form to search automatically when the user selects a view with one or more days outside the date selection range of the search filter. Setting the value to 0 requires the user to press the Search button to initiate a search.

- **defaultView=0|1|7|30|99**
  Specifies the default view for the search filter as 0 (list), 1 (day), 7 (week), 30 (month), or 99 (n-day).
  The specification for defaultView affects only the initial display of the search filter. After the

schedule displays, CA SDM automatically keeps the filter view selection aligned with the current view.
Default: 30

- **firstday=0|1|2|3|4|5|6|7**
  Specifies the first weekday on the monthly view as a number between 0 (Sunday) and six (Saturday).
  Default: 0

export=xxx|0

Specifies

the code name of the template that is used for exporting in iCalendar format. Setting the value to 0 indicates the export and disables the buttons.

Default:

ChangeSchedule

- **legend=1|2|0**
  Specifies the location of the schedule legend showing the name and formatting of the groups on the schedule. You can set the value to 1 to position the legend above the schedule, or 2 to position the legend below the schedule. Set the value to 0 to disable the legend.
  Default: 2

- **maxGroups=0/*n***
  Specifies the maximum number of groups to be displayed in a single cell of the calendar month view.
  If there are more than maxGroups scheduled for a single day, CA SDM displays only the first maxGroups-1, and replaces the last with a "..nn more changes" hyperlink that the user can mouseover or click to see the full list. Set the value to 0 to disable this feature and allow an unlimited number of events in a calendar cell.
  Default: 4

- **nday=(n,n,...)**
  Specifies selections for the drop-down list for the n-day view.
  The specification is a list of day counts that are to be included in the drop-down list, or 0 to indicate that the n-day drop-down list is omitted from the schedule. The first value specified is the default for the drop-down list.
  Default: (3,7,14,28)

- **round=(*hr,min*)|0**
  Specifies whether schedule start and end dates are rounded when collecting change orders or knowledge documents into groups. Specify round=0 to disable rounding.
  By default, schedule start and end date groups objects. All CA SDM dates include a time, and without rounding, objects scheduled as little as a minute apart would be in separate groups. Rounding determines the group after adjusting the start date to an earlier hour or minute and the end date to a later hour or minute.
  The value of round specifies either an hour or a minute (but not both). Times are rounded to the nearest multiple of the value specified, for example:
  round=(0,15) rounds to the nearest quarter hour
  round=(0,30) rounds to the nearest half hour

round=1 rounds to the nearest hour
round=12 rounds to the nearest half day (12:00 AM or PM)
round=24 rounds to the nearest day
Default: (0,15)

- **timefmt=24hr|([am],[pm])**
  Specifies the format of times on the calendar views of the schedule.
  The default value of 24hr specifies that times are displays in 24 hour format (0:01 - 23:59). The alternative value of (am,pm) specifies a suffix for either morning or afternoon times, or both.

Note: All schedConfig arguments are optional.

schedAttr Macro -- Specify a Stored Attribute

The schedAttr macro specifies an attribute stored for each item selected for the list. Stored attributes are available for hover information on the monthly view, for the detailed or summary information in views other than the monthly view, and in the setSchedEvents() JavaScript function. The following values are valid macro arguments:

- **attr=xxxx**
  (Required) Specifies an attribute from the object on the schedule, such as a change order or Knowledge Document. Dotted attributes are permitted. The keyword attribute name CI*nn* can be used on the Change Calendar to specify that first *nn* CIs associated with the change order are included with the information stored.

Note: This argument is the only required argument for the schedAttr macro.

attrRef=.COMMON_NAME|xxxx

Stores the attribute of the referenced

table stored

for an SREL attribute (ignored for non-SREL attributes). The attribute name must be prefixed with a dot.

Default:

.COMMON_NAME

- **label=**
  Displays a label for the attribute on the n-day view.
  Default: the Majic DISPLAY_NAME of the attribute

- **ident=1|0**
  Specifies whether the attribute is an identifier for the object (such as a reference number of a change order). The identifier attributes are displayed without a label in front of the group name in hover information and the n-day view.
  Default: 0

- **detail=1|0**
  Specifies whether the attribute is included in the detail information that is shown on views other than the monthly view. Detail information is the information shown when the Summary Only check box on the view is not selected.
  Default: 1

- **hoverInfo=1|0**
  Specifies whether the attribute is included in the hover information pop-up that is displayed on the monthly view. The hover information appears when the mouse pointer hovers over a group, or the user presses Alt+Right Arrow when focus is on the group.
  Default: 0

- **summary=1|0**
  Specifies whether the attribute is included in the detail information that is shown on views other than the monthly view. Detail information is the information shown when the Summary Only check box on the view is not selected.
  Default: 0

Note: CA SDM displays attributes in summary, detail, or hover information in the same order as their schedAttr macros.

schedGroup Macro -- Specify an Event Group

The schedGroup macro specifies the name and color coding of a group of items. The monthly view aggregates all items in a group into a single event. Views other than the monthly show individual items in the format for the group to which they belong. The following optional values are valid macro arguments:

- **grpname=xxx**
  (Required) Specifes the name of the group. The macro automatically assigns a number to the group and assigns the number to a JavaScript variable with a name of the form schedGroup_xxx, where xxx is the name of the group. This variable can be used in the setSchedEvents() JavaScript function to create an event belonging to the group.

  Note: This argument is the only required argument for the schedGroup macro.

- **label=xxx**
  Specifies a label for the group. If specified, the label is displayed in all views.

- **legend=xxx|0**
  Displays a description of the group for the legend that appears at the bottom of the schedule. Groups appear in the legend if at least one example of the group exists in the current view. Specifying 0 causes the group always to be excluded from the legend.
  Default: 0

- **color=black|*color***
  Specifies the color of text in items of this group. You can specify color in CSS format, either a valid web color or a hexadecimal value that is preceded by a pound sign.
  Example: Enter either "#FF0000" or "red" for red.
  Default: black

- **bgcolor=white|*color***
  Specifies the background color of items of this group. You can specify bgcolor in CSS format, either a valid web color or a hexadecimal value that is preceded by a pound sign.
  Example: Enter either "#FF000" or "red" for red.
  Default: white.

- **style=normal|bold|italic**
  Specifies the style of text of this group in the normal, bold, or italic style.
  Default: normal

The setSchedEvents() JavaScript Function

The setSchedEvents() JavaScript function creates events in the schedule. Modify this function when you want to view any new group objects. The predefined group objects appear by default.

CA SDM calls setSchedEvents() once for each object (change order or knowledge document) selected by the schedule search filter. The function creates events for the object by calling a second function, schedEvent(), and passing the group ID, start date, and end date of the event.

The function can create any number of events (including zero) for an object. The default setSchedEvents() function for the Change Calendar (list_chgsched.htmpl) creates one event for each change order and groups change orders by change type. This function is coded as follows:

```
1.    function setSchedEvents( chg )
2.    {
3.    var grpnum;
4.    switch( chg["chgtype"] - 0 ) {
5.        case 100: grpnum = schedGroup_std;  break;
6.        case 300: grpnum = schedGroup_emer; break;
7.        default:  grpnum = schedGroup_norm; break;
8.    }
9.    chg.schedEvent( grpnum, chg["sched_start_date"], chg["sched_end_date"] );
10.    }
```

The case parameter specifies the change type ID. To list the case IDs, see Create a Change Type.

The function has a single argument of a JavaScript object containing the attributes that are specified by schedAttr macros. The switch statement in lines 4-8 examines the chgtype attribute of the change order, and assigns the appropriate group number from one of the schedGroup_xxxx variables that are defined by previous schedGroup macros. On line 9, it calls the schedEvent() function to create an

event in the schedule, passing the group number that is previously assigned and the schedule start and end dates. The dates are available in the argument object because they were specified in earlier schedAttr macros.

Integrating Multiple Search Engines Using Federated Search

The Federated Search feature extends the capabilities of the CA SDM built-in knowledge base.

- When a user performs a knowledge search, the results from the internal knowledge database are augmented with results from the external search engines. We provide out-of-the box search adapter configuration for CA Open Space, Microsoft SharePoint, and Google.

The Federated Search architecture is flexible. Support for other search engines can be added by developing a custom search adapter using the CA Federated Search SDK. The SDK interface provides information and source code samples for extending the Federated Search functionality.

- Information that is contained in CA SDM tickets and knowledge articles can also be searched with an external search engine. The new Crawler Surface component allows an external search engine crawler to discover the CA SDM information easily. The crawler stores this information in its repository. This indexed information can be searched using Federated Search. Attachments for tickets and knowledge articles is also supported.

The main components of Federated Search are as follows:

- Configure Federated Search
- Configure Crawlers
- SDK Custom Search Adapter

How to Configure Federated Search

The Federated Search feature consists of the following components:

- **UI components**
  Enables the CA SDM Analyst users to enter search arguments and pass the search request to the Federated Search server.
- **CAFedSearch servlet**
  Main component of the federated Search feature and uses a REST interface. The Federated Search servlet runs on a dedicated Tomcat instance within the CA SDM application.
- **Plug-in search adapter**
  The plug-in search adapter interfaces the CA SDM application to an external search engine. The adapter translates the generic search requests to a search engine proprietary format and calls the search engine. The Federated Search servlet returns the configured search engine results to the CA SDM UI component.

Follow these steps:

- Complete the Prerequisites (see page 2789)
- Enable Federated Search (see page 2789)

Complete the Prerequisites

Complete the following prerequisites:

- Ensure to select the Federated Search option on the Configure Federated Search wizard while installing the CA SDM application.
- Know and decide the search engines that you want to use for Federated Search.
- Ensure to have an active Google Account for configuring the Google Plug-in Search Adapter. A Google API key and Google Custom Search Engine ID is also required. For more information, see Google Custom Search Engine https://www.google.com/cse/all
- Verify that IIS on the SharePoint server is configured with basic authentication. The Microsoft SharePoint adapter requires the basic authentication. By default, Basic Authentication is turned off in SharePoint. For more information about how to enable basic authentication in SharePoint, see the Microsoft SharePoint Documentation.

  Note: Enable Basic Authentication for _vti_bin in IIS.

- To integrate with CA Open Space, version 2.0 SP1 on-premise solution is required. For more information, see the CA Open Space documentation. The CA Open Space SaaS offering is not currently supported.

Enable Federated Search

A dedicated Tomcat instance is installed to host the CAFedSearch and FSCrawl servlets. The Federated Search Tomcat is under the control of the Daemon Manager. Tomcat Starts and stops automatically when CA SDM runs or shuts down respectively.

Configure the Federated Search (FS) Tomcat with the following installation options:

- **Configure Federated Search**
  Ensure to select this option when installing the CA SDM application. The Tomcat options are available only after selecting this option.
- **Tomcat Port**
  Specifies the Federated Search Tomcat Port.
  Default: 8040

- **Tomcat Shutdown Port**
  Specifies the Federated Search Tomcat Shutdown Port.
  Default: 8045

Generate Configuration XML Files for Federated Search

To configure Federated Search and to decrease editing errors, a utility file fs_adapters_cli is provided. A batch file for Windows and a Shell script for Linux and Unix is provided. The utility file is a Java application that is contained in two Jar files.

Three template files are supplied for CA Open Space, Google, and SharePoint adapters. The adapters-config.xml file is used for both input as well as output to the utility. The adapters.properties file is used as input to the utility. This file holds all the necessary configuration parameters for the adapters. The jfedsearch.log file contains the log file information.

The fs_adapters_cli utility is used to configure the adapters-config.xml file. The utility file installs and uninstalls the adapters by adding or removing entries from the adapters-config.xml. Individual adapter XML configuration files are generated. These files are then included in the adapters-config. xml with the <import> bean directive. Ensure to maintain a clean copy of the adapters-config.xml.

- To install an adapter, two entries are added for registering and importing the adapter in the adapters-config.xml file.
- To uninstall an adapter, two entries are removed for registering and importing the adapter from the adapters-config.xml file.

Federated Search Utility Files

The fs_adapters_ cli utility file is located in the CA SDM $NX_ROOT\samples\cafedsearch directory. The following utility file components are available in this location:

- The following Script files are located in the NX_ROOT\bin folder:
  - fs_adapters_cli .bat (for Windows)
  - fs_adapters_cli.sh (for Non-Windows)
- The following JAR files are available in the NX_ROOT\java\lib folder:
  - fs_adapters_config_cli.jar
  - fs_adapters_config_schema.jar
- The following templates and properties files are located in the $NX_ROOT\samples\cafedsearch directory:
  - openspace-tmpl.xml
  - google-tmpl.xml
  - sharepoint-tmpl.xml

- adapters.properties

To install the federated search utility file, run the following command:

```
fs_adapters_cli -i -k <key> -b <bean> -t <filename> -p <filename>  -o <filename> [-c <filename>]
```

Use the fs_adapters_cli - h option to get Help on the Utility file. The following attribute options are available:

- **-b (Optional)**
  Attribute value to map adapters. Refers to an actual ID of an adapter bean. If not specified, then the value from - k is taken as the value for - b.
- **-c (Optional)**
  The main XML file that contains all the configured adapters.
- **-h (Optional)**
  Provides Help for the Federated Search Utility.
- **-i**
  Specifies the option that is used for installing the adapter.
- **-k**
  Specifies the adapter key attribute.
- **-o**
  Specifies the Output XML filename to be generated. Name of the XML file to create and update the merged content of the XML template and SharePoint properties file.
- **-p (Optional)**
  Indicates the properties file name to merge with the Adapter Definition XML template.
- **-t**
  Specifies the name of the XML template file for defining an adapter.
- **-u**
  Specifies the name of the adapter XML file to uninstall the adapter.

Invoke the Utility File to Configure the Search Adapters

A Search engine requires specially coded plug-in adapters. A plug-in search adapter translates generic search requests to a search engine proprietary format, calls the search engine, and returns the search requests.

Note: If CA SDM is configured for multi-tenancy, your Tenant is passed along to the search engine. Federated Search has built-in support for multi-tenancy. You can use federated search to isolate data by a tenant in a single SharePoint implementation.

Important! Do not use ampersands or spaces in the adapters.properties file values.

Follow these steps:

1. Encrypt the passwords for search adapters using the encrypt password utility. To encrypt passwords, navigate to the following CA SDM directory:

   ```
   $NXROOT\bin
   ```

2. Run the following command for generating encrypted passwords:

   ```
   encrypt_pwd [-e] <search engine password>
   ```

   The default option is -e.

3. Open the adapters.properties file from the following CA SDM directory:

   ```
   $NX_ROOT\samples\cafedsearch
   ```

4. Edit the adapters.properties file. Specify the appropriate parameters for the adapters you want to configure.

5. For SharePoint, update the following values in the adapters.properties file:

   - **sharepoint_username=**
     Enter the user name for SharePoint access.
   - **sharepoint_password=**
     Enter the encrypted password for SharePoint access as shown in Step1.
   - **sharepoint_hostname=**
     Enter the hostname.
   - **sharepoint_domainName=**
     Enter the domain name.
   - **sharepoint_protocol=**
     Enter the communication protocol (http or https).
   - **sharepoint_portNumber=**
     Enter the port number. Default is 80.

6. For Google, update the following values in the adapters.properties file:

   - **google_googleCx=**

     Enter the unique key value that Google uses to decide which Google Custom Search Account to use.

- **google_googleApiKey=**
  Enter the unique key value that helps Google determine the identity of an application. To retrieve the key in the APIs Console, activate JSON/Atom Custom search API. This API provides a new API key for Simple API Access.

7. For CA Open Space, update the following values in the adapters.properties file:

   - **openspace_protocol=**
     Enter the communication protocol (http or https).

   - **openspace_portNumber=**
     Enter the port number for CA Open Space. Default is 8686.

   - **openspace_default_tenant_userName=**
     If CA SDM is not configured with multi-tenancy, enter a username to perform search in CA Open Space.

   - **openspace_default_tenant_password=**
     Enter the CA Open Space encrypted password. For more information, see Step1.

   - **openspace_default_tenant_companyHost=**
     Enter the tenant company host details.

     a. If CA SDM uses multi-tenancy, add an entry for each tenant in the openspace-tmpl.xml: For example, if CA SDM has a tenant that is named Tenant 1, provide the following values in the openspace-tmpl.xml file:

     ```
     <entry key="Tenant1">
      <bean class="com.ca.ServicePlus.cafedsearch.adapters.openspace.
     OpenSpaceCompanyDetail">
       <property name="userName" value="$(openspace_tenant1_userName)"/>
        <property name="password" value="$(openspace_tenant1_password)"/>
       <property name="companyHost" value="$(openspace_tenant1_companyHost)"/>
       </bean>
     </entry>
     ```

     b. Add the following entries for Tenant 1 in the adapters.properties file:

     ```
     openspace_tenant1_userName=
     openspace_tenant1_password=
     openspace_tenant1_companyHost=
     ```

     Repeat steps a and b for all required tenants in the openspace-tmpl.xml file.

8. Invoke the fs_adapters_cli once for each adapter you want to configure.

   - If you want to configure a CA Open Space adapter, use the bean value as OpenSpaceSearchAdapter and the template as openspace-tmpl.xml as shown in the following example:

   ```
   fs_adapters_cli -i -k OpenSpace -b OpenSpaceSearchAdapter -t "openspace-tmpl.xml" -o "openspace.xml"
   ```

- To configure a Google adapter, provide the the bean value as GoogleSearchAdapter and the template as google-tmpl.xml as shown in the following example:

  ```
  fs_adapters_cli -i -k Google -b GoogleSearchAdapter -t "google-tmpl.xml" -o "google.xml"
  ```

- If you want to configure a SharePoint adapter, use the bean value as SharePointSearchAdapter and the template as sharepoint-tmpl.xml as shown in the following example:

  ```
  fs_adapters_cli -i -k SharePoint -b SharePointSearchAdapter -t "sharepoint-tmpl.xml" -o "sharepoint.xml"
  ```

  Modify the -k and -o attribute values with a name of your choice. For more information about the federated search utility file and attributes,.see Federated Search Utility Files (see page 2790).

9. After the installation, if there are any errors, check the log file that is located in the CA SDM directory:

   ```
   $NXROOT\log\jfedsearch.log
   ```

10. Optionally, you can also create your own XML file for registration. All adapter entries are registered in the adapters-config.xml located in the following directory:

    ```
    $NX_ROOT\samples\cafedsearch
    ```

11. To create your own XML file for registration, you can also make a copy of the existing adapters-config.xml file name. Optionally, change the name of the modified adapters-config. xml file.
    Use the -c option with the modified XML file (xyz.xml) to register adapters.

12. Change the resource value in bean.xml <import resource="adapters-config.xml"/>.

13. Copy the adapters-config.xml or the modified xyz.xml (step 11) and any associate adapter-specific XML files for Google (google.xml), CA Open Space (openspace.xml), SharePoint (sharepoint.xml) in the following CA SDM directory:

    ```
    $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF
    ```

14. Restart the Federated Search Tomcat instance:

    ```
    pdm_tomcat_nxd  - c STOP  - t FS
    pdm_tomcat_nxd  - c START  - t FS
    ```

    The federated search adapters are configured.

15. Verify and check the error log files in the CA SDM directory:

    ```
    $NX_ROOT\log\jfedsearch.log
    ```

Create the Federated Search Sources in CA SDM

The CA SDM web UI is loosely coupled with the CAFedSearch Servlet. Configure Search Sources in CA SDM to create a new record.

Follow these steps:

1. Log in to the CA SDM application as Service Desk Administrator.

2. Select **Administration**, **Knowledge**, **Federated Search**, **Search Source** to create a new record that represents a federated search engine.
   The Search Source contains the Name of the Federated Search Source that is displayed to users.

   Note: Code value must match the key value attribute of an entry in the adapters-config.xml.

3. Click Create New to add a Federated Search Source.

4. Enter the following field values:
   Search Source Name
   Specifies a unique name for the search source.
   Code
   Specifies a unique identifier for the search source.
   Record Status
   Specifies the status of the search source. If the search source is inactive, you cannot find information from this source and this source option is not displayed in the Knowledge Search Source page.

5. (If multi-tenancy is enabled) Click Update Tenants and add the tenants.

6. Click Save.
   You added the search source.

Search the Knowledge Solution using the New Custom Search Adapter

Search for knowledge documents and articles in the CA SDM application using the new custom search adapter.

Follow these steps:

1. Log in as a CA SDM Service Desk Administrator.

2. Navigate to **Administration**, **Knowledge**, **Federated Search**, **Search Sources**.

3. Add search source **Code** Key value.

4. Click **Save**.

5. Navigate to **Knowledge Management** using a new or existing ticket.

6. Search for the knowledge source that you have created. Click **Show Filter** to enter the search criteria and click **Search**.
   The search information is displayed.

Modifying the Cross-Origin Resource Sharing (CORS) Filter

The default CORS filter setting allows any server to send requests to Federated Search. We recommend that you restrict this setting to allow incoming requests only from the web interface servers.

Follow these steps:

1. Navigate to the following CA SDM directory on the server where you have installed federated search:

   ```
   $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\web.xml
   ```

2. Open the web.xml file and check for:

   ```
   <web-app><filter><init-param><param-name>cors.allowOrigin</param-name>
   ```

3. Update the <param-value> tag with a space-separated list of domains. For example, the base URL address of the servers from which you want to allow incoming requests:

   ```
   <param-value>http://web01:8080 http://web02:8080 http://web03:8080</param-value>
   ```

4. Save the web.xml file. Tomcat is restarted automatically.

5. Test and verify the Federated Search configuration on the web client interface. Ensure that it is functional.

6. For the web interface updates to persist after running the CA SDM Configuration, repeat the same updates to the web.xml.tpl file.

Uninstall the Search Adapter

To uninstall the search adapters, use the fs_search_cli utility command with the - u option. Use the following utility file command:

```
fs_adapters_cli -u -k <key> -b <bean> [-c <filename>]-f <filename>]
```

- **-u**
  Specify the -u option to uninstall the search adapters.
- **-k**
  Specify the key name value that is provided at the time of installation.
- **-b**
  Specify the bean value that is provided at the time of installation.
- **-c**
  Specify the name of the new search adapter configuration xml, if you created any while configuring the search adapters with Utility.
- **-f**
  Gives the Generated output file name at the installation time.

For example, if you want to uninstall the Google search adapter, perform the following steps:

Follow these steps:

1. Run the utility file command with the -u option for uninstalling the Google search adapter:

   ```
   fs_adapters_cli -u -k Google-b GoogleAdapter-f Google.xml
   ```

2. Check and verify that the adapters-config.xml removes registration for Google.

3. Google.xml file is deleted from the following CA SDM directory:

   ```
   $NX_ROOT\samples\cafedsearch
   ```

4. Copy the adapters-config.xml to the following directory:

   ```
   $NX_ROOT\samples\cafedsearch\WEB-INF
   ```

   Delete the google.xml file from this location.

5. Restart the FS Tomcat:

   ```
   pdm_tomcat_nxd  - c STOP  - t FS
   pdm_tomcat_nxd  - c START  - t FS
   ```

6. In the CA SDM UI, verify the Activate Search source entry for this Adapter (Google, in this case).

7. To uninstall other external search adapters, repeat steps 1 through 6.

How to Configure SDK Custom Search Adapters

This article contains the following topics:

Important! CA Federated SDK sample source code is provided to users for creating and deploying alternate custom adapters. However, CA Support does not provide support to write the actual custom code. We do not actively support the creation and deployment of additional adapters beyond the SDK source code samples shipped with CA SDM.

The CA Federated Search SDK architecture is designed for extensibility. The SDK contains all the necessary JAR files to develop a custom adapter. Sample Eclipse projects can be imported, and Ant build targets are also provided to build custom search adapters. The SDK is located in the CA SDM directory:

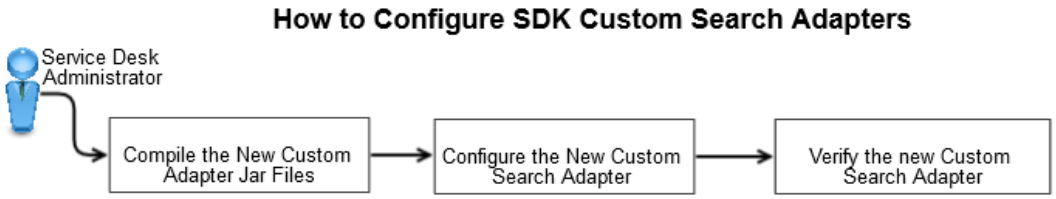
```
$NX_ROOT\samples\sdk\fedsearch\adapters-source.tar.gz
```

The source code of the following adapters can be used to write more custom adapters:

- Google
- CA Open Space
- Microsoft Share Point

> **Note:** Source code for the CAFedSearch servlet, its underlying framework, and the security filter are not provided. No source code is provided for any of the Crawler Surface components.

The SDK component is written in java and is shared as a jar file (cafedsearch-adapter-sdk-1.0.0.jar). The SDK provides a simple interface to enable customers to develop and deploy their own search adapters.



Compile the New Custom Adapter Jar Files

Compile the custom adapter jar files successfully.

Follow these steps:

1. Compile the new custom search adapters. Ensure that you have the following jar files in your Java Classpath:
   - **jsr311-api-1.0.jar**
     This jar file is available in the CA SDM directory:

     ```
     %NX_ROOT%\java\lib\CXF\
     ```

   - **cafedsearch-core.jar**
     This file is available in the directory:

     ```
     %NX_ROOT%\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\lib
     ```

   - **cafedsearch-adapter-sdk-1.0.0.jar**
     This file is available in the directory:

     ```
     %NX_ROOT%\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\lib
     ```

- **log4j-1.2.15.jar (optional)**
  This file is available in the directory:

  ```
  %NX_ROOT%\java\lib
  ```

2. Write a new Java Class which extends the SearchAdapter Class and provides an implementation for the abstract method.

   `search`

   The CAFedSearch component invokes and passes search method parameters. These parameters are embedded inside the SearchOptions parameter for each search request from the client.

   Note: Ensure that your implementation is thread safe as the CAFedSearch component maintains only one instance of the Java Class. For each search operation, search method is invoked on the same instance.

3. The SearchOptions parameter for the search method has the following methods:

   - **getSearchTerms()**
     Specifies the method for retrieving the search string.
   - **getStartIndex()**
     Specifies the start index method, the number from which the client wants to search items. Index starts from 1.
   - **getItemsPerPage()**
     Specifies the maximum number of search results that the client expects.

   Note: You can also use other Java Class methods. For example: getUserId()

4. Send the collected information to the external search engine API for retrieving the search results.

   Note: For information about Java Class Methods, see Java Documentation.

5. The search method returns an instance of ResultCollection class. Create an instance of ResultCollection and populate values using the following methods:

- **setSources(String name)**
  Specifies the name of the search adapter. Names are case-sensitive and must match exactly with the name that is provided in the utility configuration file. For convenience, SearchAdapter provides a method getName() which should be used.
  For example:

```
results.setSources(getName());
```

- **setTotalResults (int total)**
  Specifies the total search result count.

- **setStartIndex(int startIndex)**
  Specifies a start index of results. This value is as per results from your search engine.

```
results.setStartIndex(startIndex);
```

6. A collection of ResultItems must be passed to the ResultCollection object by calling the setSearchResultItems method. To add an instance of ResultItem at a time, use the addSearchResultItem() method.

   Note: For more information about ResultCollection Java class, see the Java documentation.

7. The ResultItem class has the following important methods, which must be filled for each search result item (row).

   - **setContentText(String txt)**
     Specifies a method for setting the search result actual content.

   - **setContentHTML(String txt)**
     Specifies a method for setting the HTML (can contain the HTML tags) content. If the search engine gives HTML highlighted, then set the highlighted text using this method.

   Note: If your search engine does not have this feature, you can write a simple Java class method to highlight the text. The CA Open Space adapter has a simple method to bold terms in the search results.
   Note: If the search adapter requires more jar files, modify the build.xml to compile and prepare an adapter jar file. Ant binaries are required to use the build.xml. Use Ant to run the targets in build.xml to compile and make the JAR files Keep the build. xml along with your source (src) folder. The build.properties file is optional. For more information about Ant binaries, see Ant Help.

   The jar file is successfully compiled.

Configure the New Custom Search Adapter with the CAFedSearch Component

Configure the new search custom adapter jar file with the CAFedSearch Component for creating the CA SDM search sources.

Follow these steps:

1. Copy the jar file from the location dist\lib (created in Compile the New Custom Adapter Jar Files (https://wiki.ca.com/display/CASM1401/How+to+Configure+SDK+Custom+Search+Adapters#HowtoConfigureSDKCustomSearchAdapters-CompiletheNewCustomAdapterJarFiles)) to the following CA SDM directory:

   ```
   %NX_ROOT%\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\lib
   ```

2. Navigate to the following CA SDM directory:

   ```
   $NX_ROOT\sample\cafedsearch\
   ```

Create template xml file for the custom search adapter. For example, the XYZ-tmpl.xml file.

- The template file contains the following contents:

```
<?xml version="1.0" encoding="UTF-8"?>

<beans default-autowire="byName" xsi:schemaLocation="http://www.springframework.org/schema/beans

http://www.springframework.org/schema/beans/spring-beans-2.5.xsd

http://cxf.apache.org/core

http://cxf.apache.org/schemas/core.xsd

http://cxf.apache.org/jaxrs

http://cxf.apache.org/schemas/jaxrs.xsd" xmlns:cxf="http://cxf.apache.org/core"

xmlns:jaxrs="http://cxf.apache.org/jaxrs"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns="http://www.springframework.org/schema/beans">


    <bean autowire="autodetect"

        class=" com.abc.xyz.XYZAdapter "

            id="XYZAdapterConfiguration" scope="singleton">

<property name="username" value="$(xyz_username)"/>

    <property name="password" value="$(xyz_password)"/>

</bean>

<bean autowire="autodetect" class="com.abc.xyz.XYZAdapter" id="XYZSearchAdapter" init-method="init" destroy-method="

destroy" depends-on="XYZAdapterConfiguration">

            <property name="config" ref="OpenSpaceAdapterConfiguration" />

    </bean>

</beans>
```

- You can create property values that are based on the input values provided for the search adapters in step 4.
  Add xyz_username and xyz_password in the adapters.properties file and provide values to the property.

- Run the utility file to generate configuration XML for custom search adapters:

```
fs_adapters_cli -i -k XYZ - b XYZSearchAdapter -t "XYZ-tmpl.xml " -o "xyz.xml
```

- The xyz.xml file is created and registered in the adapters-config.xml file.

- Copy the xyz.xml file and adapters-config.xml to the following CA SDM directory:

```
$NX_ROOT\samples\cafedsearch\WEB-INF
```

- Run the following command to restart Federated Tomcat Services:

```
pdm_tomcat_nxd  - c STOP  - t FS

pdm_tomcat_nxd  - c START  - t FS
```

- Create the federated search sources for the XYZ adapter in the CA SDM UI.
  For more information about federated search sources, see Create the Federated Search Sources in CA SDM (see page 2794).

- In CA SDM, navigate to the **Knowledge Management** Tab. Select the XYZ check box and perform search operations.
  The new custom search adapter is successfully configured with the CAFedSearch component.

Verify the new Custom Search Adapter

Verify the functionality of your new custom search adapter by using the REST client.

Follow these steps:

1. Download the REST client from the Internet:
   https://code.google.com/p/rest-client/ (http://www.code.google.com/p/rest-client/)

2. Launch it using Java (JRE is required).

3. Enter the following URL in the REST client UI:

   ```
   http://sdmhostname:<FS_Tomcat_Port>/cafedsearch/sdm/search?
   q=search&userid=<sdmuserid>&source=<Adapter Name>
   ```

4. Turn off the CA SDM security interceptor. Open the following file for editing and comment out the “<jaxrs:inInterceptors> “ section:

   ```
   $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\beans.xml
   ```

> **Note:** Turning off the security filter is not recommended in a production environment. Turn off the Security filter in a test environment for verifying the new custom search adapter functionality.

5. Verify that the new custom search adapter is functioning properly. If search results are not displayed, try reviewing the logs, or increase the log level to Debug.

Call the CAFedSearch Servlet Using REST

The CAFedSearch servlet exposes a RESTful interface where custom search clients, programs, and User Interfaces (UI) can send search requests.

This RESTful interface only accepts the HTTP Collection GET requests following the OpenSearch specification. It provides support for JSON and XML responses. Each request must contain a Service Desk BOPSID token which can be obtained from CA SDM RESTful or SOAP Web Services.

Follow these steps:

1. Obtain a BOPSID token using a CA SDM RESTful Web Service.

2. Get a REST Access Key by sending an HTTP POST request on the rest_access resource along with login credentials.
   You can also obtain a BOPSID token using the REST Access Key by sending an HTTP POST request on the bopsid resource.

3. For the details on sending requests to CA SDM RESTful Web Services, see the sample files in the following CA SDM directory:

   ```
   NX_ROOT\samples\sdk\rest\java
   ```

4. To use the Federated Search API for searching, send an HTTP GET request on the search resource and pass search criteria and BOPSID token through the CA SDMURL.

   ```
   GET
   http://<sdmhostname>:<FS_TOMCAT_PORT>/cafedsearch/sdm/search?
   q=<searchTerms>&source=<adapterName>&BOPSID=<bopsidToken>&userid=<userId>
   ```

   - **searchTerms**
     Specifies a space delimited list of keywords. Must be URL encoded.

   - **adapterName**
     Specifies search engine name as specified in the Search Source record Code field using the adapters configuration utility.

   Other supported arguments are as follows:

   - **index**
     Specifies the first index that is desired in the search results, must be integer > = 1.

   - **page**
     Specifies Indicates the first page that is desired in the search results, must be integer >= 1.

- **size**
  Specifies the number of results per page that is desired by the search client.

- **type**
  Valid values include JSON or XML.

How to Configure the Crawler Surface for SharePoint

This article contains the following topics:

The administrators can configure CA SDM to allow Microsoft SharePoint 2010 and SharePoint 2013 Servers to crawl the Crawler Surface. The Crawler Surface contains a FSCrawl Servlet component that lets you search the CA SDM knowledge solutions and articles.

A crawler is a search engine component that browses the Internet and indexes search terms. The Crawler Surface is a read-only web-based interface to the CA Service Desk Manager application. With this interface, external search engine crawlers can discover information using the Java Server Page (JSP) technology. The Crawler Surface uses the JSP to provide the information in plain text and individual hyperlinks to tickets and knowledge documents.

Note: The CA Service Desk Manager content that is exposed to a crawler can be modified using an XML configuration file. For more information, see Crawler Surface XML Configuration File. (see page 2807)

Complete the Prerequisites

Complete the following prerequisites before you start configuring the Crawler Surface for a Microsoft SharePoint Server:

- To enable Federated Search, select the Configure Federated Search option while installing CA Service Desk Manager.

- Identify a dedicated User ID for accessing the search result information. The User ID controls the information that is present in the Crawler Surface. For multi-tenancy configuration, you can create several user IDs to allow the segregation of tenant information.

Create the CA Service Desk Manager User Crawler Surface

In your CA Service Desk Manager configuration, create user identities to segregate information by tenant.

The process of creating a user ID for the Crawler Surface is the same as creating the CA Service Desk Manager user identities for regular users. Create a contact with Access Type and Role as "Crawler" in the CA Service Desk Manager Application. The Crawler Access Type and Role provide the user with read-only access to the CA Service Desk Manager data. A contact is a person who uses the system regularly, such as an analyst or customer. After you have created the business structure and groups, you can create contacts and can map them to their respective location and organization. You can create contacts using the following ways:

- Create Contacts Manually
- Create Contacts Using the LDAP Database

Configure the Tomcat Remote IP Address Filter

Change the Tomcat Remote IP Address Filter setting to point to the remote system that hosts the SharePoint Server. The IPV4 and IPV6 addresses are supported.

The crawler surface uses the Tomcat Remote IP Address Filter mechanism to access the CA Service Desk Manager information. The Tomcat filter mechanism uses an IP Address pattern (maintained by the CA Service Desk Manager administrator) to match authorized IP addresses. By default, the Remote IP Address filter is configured with the loopback adapter IP address 127.0.0.1. For a secure communication in a production environment, consider using Secure Sockets Layer (SSL) encryption between the crawler and the crawler surface.

Follow these steps:

1. Log in to the following server, depending on your CA Service Desk Manager configuration:
   - Conventional: Primary or Secondary Server
   - Advanced Availability: Application Server
2. Open the web.xml file in the following CA Service Desk Manager directory:

   ```
   $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\fscrawl\WEB-INF
   ```

3. Save a backup of the web.xml file.
4. Find the <filter-name>Remote Address Filter</filter-name> section. Change the pattern in <param-value> in the <filter>.
   This parameter allows you to specify a range of IP Address patterns and provides access from the remote system hosting the SharePoint server. For more information about the Tomcat Remote IP Address Filter, see the Apache Tomcat documentation.

5. Save the XML file.

6. Restart the Federated Search Tomcat server.
   The Tomcat Remote IP Address Filter value is changed and the Crawler Surface can now be accessed from the remote system.

   Note: Do not access the crawler surface from an unconfigured IP address. You are redirected to the CA Service Desk Manager UI.

7. The Crawler Surface is accessed through a URL like other web application. To validate SharePoint logging, enter the following URL in a browser:

   ```
   http://<sdmhostname>:<FS_TOMCAT_PORT>/fscrawl/index.jsp?farm=<FarmName>
   ```

   Note: All elements of the URL are case-sensitive.

Configure the Crawler Surface User ID

The CA Service Desk Manager information content that is exposed to a crawler surface can be modified using a configuration xml file. External search engine discovers information using the Java Server Page (JSP) technology. The crawler surface user ID controls the information that is present in the Crawler Surface.

To modify the crawler surface, you can configure the crawler surface user ID in the crawler_surface_config.xml file.

Important! Verify the language settings of your browser as Microsoft SharePoint is sensitive to the language used in the search request.

Follow these steps:

1. Log in to the following CA Service Desk Manager server that hosts the Crawler Surface depending on your install configuration:

   - Conventional: Primary or secondary Server
   - Advanced Availability: Application Server

2. Open the crawler_surface_config.xml from the following CA Service Desk Manager directory:

   ```
   $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\fscrawl\WEB-INF
   ```

3. Save a backup of the crawler_surface_config.xml file.

Important! Make all XML file modifications in a test environment before porting the final changes to a production server.

4. In the original file, locate *<sdm_user>CHANGE_THIS</sdm_user>* under each *<farm>* section and replace *CHANGE_THIS* with the crawler user ID that you created earlier.

5. You can further modify and restrict the XML object attributes depending on your requirements.

Note: For more information, see the Crawler Surface XML Configuration File.

6. Save the XML file.

7. Restart the Federated Search Tomcat server to reload the file.
The Crawler Surface XML file is modified.

Crawler Surface XML Configuration File

The crawler_surface_config.xml file contains the following XML sections.

- **<objects>**
Specifies the information about the objects and attributes that the Crawler Surface exposes for an object. The objects section describes the layout of a detail page for each object type that is exposed to a crawler. This section does not control the selection of individual records. The <objects> section is a collection of <object> sections.
Each object is defined in an <object> section. The default specifications for these objects are provided as:

  - **KD**
  Specifies Knowledge Documents.

  - **chg**
  Specifies Change Orders.

  - **iss**
  Specifies Issues.

  - **in**
  Specifies Incidents.

  - **pr**
  Specifies Problems.

  - **cr**
  Specifies Requests.

The XML file contains the following sections that create the <head> section of a detail page in CA Service Desk Manager:

- **<name>**
  Specify the Majic object name of the exposed object.

- **<note>**
  Specify a location for a short description of the object. This element is only for documentation purposes, and the Crawler Surface ignores this element.

- **<last_mod_dt>**
  Specify the attribute name that stores the last modified date and time. The time and date is exposed to the search engine crawler to allow the search engine to determine whether the record was updated. The search engine crawler skips the crawl when the record is not updated.

- **<title>**
  Specify the attribute that is used for the title of the detail page. The search engines use this element as the title of the document that is returned in search results. This element entry generates an HTML <title> tag in the <head> of the detail page. For a knowledge document, the title defaults to the title of the knowledge document. The summary is used for the title for incidents, problems, requests, change orders, and issues.

- **<meta_data>**
  Specify one or more properties that is exposed as a metadata. A Metadata allows a search engine to store extra characteristics of the document in its index. Metadata is not searched directly but instead is used to filter search results. This section generates HTML <meta> tags in the <head> of the detail page.
  Each entry in the <meta_data> section contains one or more <property> entries. Each <property> element consists of a <name> element and a <content> element.

  - **<name>**
    Specify the name of the metadata property.

  - **<content>**
    Specify the attribute of the object that is used as the value for the metadata.
    Together, each <name> and <content> element pair of a <property> generate an HTML <meta> tag. The search engine crawlers use the following two metadata properties by default:

    - **Description**
      Specify the metadata property of a search engine that stores a short summary of the document.

    - **Author**
      Specify the author of the document.

The CASDMTENANT metadata property is also configured by default for each object. This property is a CA Service Desk Manager specific-metadata property. The Crawler Surface uses this property to expose the Tenant name of the object to the crawler of the search engine. During a Federated Search, the results that are obtained from the search engine are filtered based on this metadata property.

The Crawler Surface XML Configuration file contains the following attributes that are used to create the <body> section of a detail page in CA Service Desk Manager:

- **<additional_attributes_to_index>**
  Indicates a list of attributes from the object that the Crawler Surface exposes. Separate multiple entries with a comma and a space. For example, PROBLEM, RESOLUTION, SD_ASSET_ID.name (http://SD_ASSET_ID.name).

- **<activity_logs>**
  The Crawler Surface displays information from Activity Logs for objects that have activity logs. The <activity_logs> section contains the <object>, <select_criteria>, <rel_attr>, and <attributes> elements.

  - **<object>**
    Specifies the object name that contains the activity log entries for the object. For example:

    - *alg* is the activity log object entry for Incidents, problems, and requests.
    - *chgalg* is the activity log object entry for change orders.
    - *issalg* is the activity log object entry for issues.
    - O_COMMENTS is the activity log object entry for knowledge documents.

- **<select_criteria>**
  Allows you to filter the activity log objects that are exposed. This element is important to increase the relevancy of your search results by decreasing frequently occurring words. For example, the <select_criteria> for chgalg contains the following Magic Where clause:

  ```
  "type IN ('ST', 'UPD_RISK', 'CB', 'RS', 'LOG', 'TR', 'ESC' ,'NF', 'UPD_SCHED')"
  ```

  Includes only activity log entries that allow a user to enter comments and eliminates activity log entries with fixed text like Initial or Attached document.

- **<rel_attr>**
  Specifies how an activity log entry relates to its parent object. The <rel_attr> subsection contains <parent_obj_attr> and <join_attr> elements.

  - **<parent_obj_attr>**
    Indicates an attribute of an activity log that contains an SREL (or foreign key pointer) to the parent object. For example, the change_id is the attribute of activity log object *chgalg*.

  - **<join_attr>**
    Indicates the relational attribute (Rel Attr) of the parent object that is stored in <parent_obj_attr>. You can verify these values by using the following command:

    ```
    bop_sinfo -df chgalg
    ```

  You can verify both of these values by using the bop_sinfo -df chgalg command. The output must show that the value for change_id is *SREL -> chg.id (http://chg.id)* and ISS is *SREL -> iss. persistent_id.*

- **<attachments>**
  The attachments subsection allows you to expose attachments to the crawler so that content can be indexed. The <attachments> section is only allowed for objects that have attachments.

The attachments are handled in a special manner by the Crawler Surface. The Crawler Surface exposes a hyperlink that the crawler follows to download the attachment from CA Service Desk Manager. If an attachment is included in the search results, you can click on the hyperlink to navigate to the parent object.

The <attachments> section contains <object>, <rel_attr>, <attmnt_id>, and <is_parent_updated> elements.

- **<object>**
  This element specifies the Majic object that links the Attachment to its parent object.

- **<rel_attr>**
  This subsection works the same as it does in activity logs. Specifies how the parent object relates to this object which links the parent object to the attachment.

- **<attmnt_id>**
  This element specifies the attribute of this linking object that points to the attachment.

- **<is_parent_updated>**
  Specifies the Crawler Surface on how to expose the last-modified date for the object. For some objects like Knowledge Documents (KDs) when an attachment is added, the last modified date of the Knowledge document is not updated. The last-modified date is important when the search engine is doing an incremental crawl.

- **<configuration_items>**
  Used for objects that contain a list of configuration Items. This section contains the <object>, <rel_attr>, and <attributes> elements.

  - **<object>**
    Works the same as in activity logs and attachments.

  - **<rel_attr>**
    Work the same as they do in activity logs and attachments.

  - **<attributes>**
    This element works the same as in attachments.

- **<multi-farm_datasets>**
  The <multi-farm_datasets> specifies how records are selected. The <multi-farm_datasets> section is a collection of <farm> sections.

- **<farm>**
  Each <farm> section controls the CA Service Desk Manager information that is exposed to a crawler. When a crawler is configured, the <farm> section is specified in the URL. Only the information that is specified in the <farm> section is exposed to the crawler. Each <farm> section contains <name>, <data_sets>, and <sdm_user> elements.<name>.

  Note: This value is case-sensitive.

Configure the SharePoint Crawler

Configure Crawlers to crawl and search for content in SharePoint. The Crawler is a multithreaded application capable of high throughput and can sometimes have a negative impact on the CA Service Desk Manager performance. To improve performance, ensure that you have considered the following factors:

- Limit the number concurrent SharePoint crawle rs accessing the Crawler Surface at any one time.
- Use SharePoint Crawler Impact Rules to throttle the crawlers
- Schedule crawls at off-peak times of the day
- Dedicate an Object Manager <sdm_domsrvr_name> to the Crawler Surface in crawler_surface_config.xml. For more information, see Crawler Surface XML Configuration File (see page 2807).
- For CA Service Desk Manager Advanced Availability, dedicate an entire Application Server to the Crawler Surface.

Follow these steps:

1. Create the Content Source in SharePoint (see page 2811)
2. Create Crawler Rules (see page 2812)
3. Run the Crawler in SharePoint (see page 2813)
4. Configure the Metadata in SharePoint (see page 2814)
5. Verify the Crawler Data in SharePoint (see page 2814)

Create the Content Source in SharePoint

Create Content Sources for identifying the type of content that the SharePoint crawler processes.

Note: The names of SharePoint specific settings can vary depending on the SharePoint version you are using. For more information about creating content sources in SharePoint, see the Microsoft SharePoint Documentation.

Follow these steps:

1. Log in to the MS SharePoint Central Administration console.
2. Click **Manage Services Application**, **Search Service Application**.
3. Click **Content Source** for creating new content Sources:
4. Enter data name for the Content Source in **Name** as CA Service Desk Manager.

5. Set the Content Source Type to Web Sites.

6. Enter the following URL in **Start Address**:

   ```
   http://<sdmhostname>:<FS_TOMCAT_PORT>/fscrawl/listObject.jsp?farm=<Farm Name>
   ```

7. To prevent the crawler from straying away from the Crawler Surface, consider limiting the Page Depth to 2 and the Server Hops to 1. Minimum recommended values to allow crawling of Attachments.

8. Click **Save**.

Create Crawl Rules

The Crawl rules define how the SharePoint Web Crawler Surface URL is crawled. Define the following Crawl Rules:

- A crawl rule that lets SharePoint crawl the Crawler Surface.
- A crawl rule that allows SharePoint to access attachments.

Follow these steps:

1. Log in to the MS SharePoint Central Administration console.

2. Click **Manage Services Application**, **Search Service Application**.

3. Click **Crawler Rule**. Create new Crawler Rule.

4. Enter the following URL in the browser:

   ```
   http:// <sdmhostname>:<FS_Tomcat_Port>/fscrawl/*farm=<farm-name>*
   ```

   Important! The Crawler Surface URL is case-sensitive. SharePoint changes uppercase hostnames to lowercase. For SharePoint 2010, ensure to select the **Match Case** check box.

5. Select '**Include all items in this path**' to configure the crawler.

6. Select '**Crawl complex URLs (URLs that contain a question mark - ?)**'.

7. Select '**Specify a different content access account**'.

8. If you have Disabled the Basic Authentication (see page 2815) in CA Service Desk Manager Crawler Surface;

   a. Select one of the following options:

- (SharePoint 2013), Select the '**Specify a different content access account**' and ' **Anonymous access**' options.
- (SharePoint 2010), Select the default content access account (NT AUTHORITY\NETWORK SERVICE).

b. Save this Crawl rule and skip to step 10 for defining second crawl rule.

9. Enter the CA Service Desk Manager user account name and password for the Crawler Surface.
10. Create a second crawler rule for the CA Service Desk Manager attachments:

    `http://<sdmhostname>:<WEB_TOMCAT_PORT>/CAisd/*`

    Note: <sdmhostname> is the configured host name that is used for downloading the CA Service Desk Manager attachments.

11. Specify the default authentication:

    Note: The Crawler Surface uses Basic Authentication. The CA Service Desk Manager Repository Daemon uses proprietary BOPSID security which is not directly supported by Microsoft SharePoint. Specify any user ID and password or choose Anonymous Access if that option is available in your version of SharePoint.

12. For (SharePoint 2013), select the '**Specify a different content access account**' and ' **Anonymous access**' options or for (SharePoint 2010) select the default content access account (NT AUTHORITY\NETWORK SERVICE).

    The Microsoft SharePoint Crawl rule is created.

Start a Crawl in SharePoint

Start a full or incremental crawl of the content sources in SharePoint to index the search content.

Follow these steps:

1. Navigate to the Microsoft SharePoint Central Administrator page.
2. Click **Manage Services Application**, **Search Service Application**.
3. Click **Content Sources**. Select the that you configured for the SharePoint Crawler Surface.
4. Select **Start Full Crawl** or **Start Incremental Crawl**.
   A full crawl crawls the entire content under a content source. Full crawls take more time and resource to complete than Incremental crawls.

In an incremental crawl, the index remains intact, and the crawler crawls only the content that is added or modified since the last successful crawl. For more information, see the Microsoft SharePoint Documentation.

Configure the Metadata in SharePoint

Note: This topic is applicable to CA Service Desk Manager multi-tenancy environments.

When the crawler encounters a CA Service Desk Manager metadata, it stores the metadata in SharePoint as Crawled properties. These properties are discovered during the initial full crawl of the CA Service Desk Manager Crawler Surface. The SharePoint crawler discovers the metadata and creates the Crawled properties.

The metadata is used to pass extra information to a crawler in the detail pages using the <meta> tag in the <head> section. This information is available for searching and filtering. When CA Service Desk Manager is configured for multi-tenancy, the Crawler Surface exposes only the tenant metadata information.

When you perform a Federated Search, the tenant name is passed to the search engine to filter the results appropriately.

Follow these steps:

1. Log in to the MS SharePoint Central Administration console.
2. Click **Manage Services Application**, **Search Service Application**, **Metadata** (SharePoint 2010), or **Search Schema** (SharePoint 2013).
3. Ensure that the SharePoint crawling is successful on the CA Service Desk Manager data.
4. Click **Managed Properties**.
5. Click **New Managed Property**.
6. Enter **CASDMTENANT**as Property Name.
   CASDMTENANT Indicates the tenant name for the CA Service Desk Manager object. The sub tenant information is not displayed.
7. Select **Text** as **Property Type**.
8. Scroll down. Click **Add a Mapping**.
9. Search for the CASDMTENANT Crawl Property and select it.
10. Click **OK** to save the new Managed Property.
    The metadata in SharePoint is configured.

Verify the Crawler Data in SharePoint

Verify the Crawler data in SharePoint in order to display search results.

Follow these steps:

1. Log in as CA Service Desk Manager Service Desk Administrator.
2. Click the **Knowledge Management** tab for a new or existing ticket.
3. Select **SharePoint Search Source**.
4. Enter the search key. Click **Search**.
   The Crawler displays the search results.

(Optional) Disable Basic Authentication

The Basic authentication authenticates and authorizes the users accessing CA Service Desk Manager content from an HTTP client and provides additional security to the Crawler Surface. However, basic authentication is an overhead for every HTTP request to the Crawler surface and eventually impacts product performance. If you have configured the remote IP address filter on Tomcat to limit the computers that can access CA Service Desk Manager content, you can disable basic authentication.

Follow these steps:

1. Take a backup of web.xml at
   $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\fscrawl\WEB-INF.
2. Open the file using a text editor.
3. Comment or remove the tags <security-constraint>, <login-config>, <security-role>.
4. Save the file.
5. Restart FS Tomcat.

The basic authentication for Crawler Surface is disabled.

Troubleshooting

The Crawler Surface has the usual array of log files:

1. If you want to enable the debug mode for Federated Search, navigate to the following CA Service Desk Manager directory:

   ```
   $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF
   ```

2. Open the log4j.properties file and modify info to debug mode.
3. To enable debug mode for fscrawl, navigate to the following CA Service Desk Manager directory:

   ```
   $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\fscrawl\WEB-INF
   ```

4. Open the log4j.properties file and modify info to debug mode.
5. To correct the syntax errors that are encountered while configuring the SharePoint crawler surface, open the jfscrawl log file from the CA Service Desk Manager directory:

```
$NX_ROOT\logs directory
```

6. If you locate any syntax errors, correct the XML file and restart the Federated Search Tomcat. The log is located in the CA Service Desk Manager directory:

   ```
   $NX_ROOT\logs\jfscrawl.log
   ```

   For example, if a <meta_data> tag is accidentally corrupted, then the log indicates the following error:

   ```
   08/06 15:43:52.624 [pool-2-thread-1] ERROR FSCrawlApplicationListener 302
   XmlException::Problem loading config_file::C:
   \PROGRA~2\CA\SERVIC~1\bopcfg\www\CATALINA_BASE_FS\webapps\fscrawl\WEB-
   INF\crawler_surface_config.xml:274:8: error: </meta_dataxxxxx> does not close
   tag <meta_data>
   08/06 15:43:52.625 [pool-2-thread-1] ERROR FSCrawlApplicationListener 144
   crawler_surface_config.xml could not be loaded, cannot read.
   ```

7. If there are no syntax errors, the following message is displayed:

   ```
   08/06 15:46:27.924 [pool-2-thread-1] INFO FSCrawlApplicationListener 58 fscrawl
   context had been loaded successfully.
   ```

8. Correct any other errors that do not show up until you try to access CA Service Desk Manager. For example, an unknown attribute xxxxx is requested to be exposed for Incidents in the <additional_attributes_to_index> element of crawler_surface_config.xml. The Crawler Surface application does not detect the error. But, when the Crawler Surface sends the request to the Object Manager, the error is detected and reported in the stdlog.x file as follows:

   ```
   08/06 15:51:23.92 SDMSERVER domsrvr 10860 ERROR domset.c 8049 Unknown attribute
   "xxxxx" requested from domset MLIST_STATIC of factory
   ```

9. Use the bop_sinfo -d command to resolve the error.

10. Modify the crawler_surface_config.xml file.

11. Restart the Federated Search Tomcat.
    The Crawler Surface objects are configured without any errors.

Knowledge Management Reports and Metrics

This article contains the following topics:

You can monitor the efficiency of the knowledge base using the reporting tools that are described in this article. These tools let you view statistics on the usefulness of your documents and their effectiveness in solving problems.

Knowledge Report Card

The Knowledge Report Card displays information about the knowledge contribution from each end user and provides feedback about which knowledge documents are most effective. You can use the information to improve the processes of creating knowledge documents and providing the best support to end users in your environment.

Define Knowledge Report Card Statistics

As an Administrator, you define the schedule at which the product calculates and sends notifications about the Knowledge Report Card. You also define content of Knowledge Report Card notification emails.

Note: Rework versions and retired documents are not presented when the Knowledge Report Card calculation is run.

Follow these steps:

1. Select the **Administration** tab, **Knowledge**, **Knowledge Report Card**.
   The Report Card page opens.

2. Complete the following fields as appropriate.

   - **Last Updated**
     Runs the Report Card calculation.
     Default: Deactivated
     Note: When the calculation is not run, and the statistics to present the data are not collected. The following message appears when the Knowledge Report Card command is specified from the View menu on the Knowledge tab: "Please Run Report Card Calculation."

   - **Schedule**
     Schedules the Report Card.

     - **Report Card Calculation will next run on xxx and will run every xxx**
       Specifies the frequency at which to recalculate the Report Card statistics.

     - **Report Card Email Notifications will be sent on xxx and will be sent every xxx**
       Specifies the frequency at which to send the Report Card notifications.
       Default: Never

     - **Report Card Email Should Display Statistics for the Past xxx**
       Specifies the amount of time for which the Report Card notification contains information. This field is only available when you select a value other than Never from the Report Card Email Notifications will be Sent Every xxx list.
       Default: 365 days

3. Click **Save**.
   The Knowledge Report Card statistics are defined.

Run the Knowledge Report Card

The Knowledge Report Card displays information about the knowledge contribution from each end user and provides feedback about which knowledge documents are most effective. You can use the information to improve the processes of creating knowledge documents and providing the best support to end users in your environment.

Note: After you run the knowledge report card, the analyst will be able to view their knowledge report card statistics.

Follow these steps:

1. Select the **Administration** tab, **Knowledge**, **Knowledge Report Card**.
   The Knowledge Report Card appears.

2. Complete the following fields and click Save.

   - **Last Updated** -- Select the Run Calculation check box.

   - **Schedule** -- Specify a date and time from when CA SDM performs the calculation and runs the Report Card.

Note: For information about using Automated Policies and the Knowledge Report Card, see View Document LifeCycle Policy Reports (see page 2779)

Web-Based Reports for Knowledge Management

CA Business Intelligence installs a set of predefined Knowledge Management reports. These reports are automatically deployed to the CA Business Intelligence after the CA SDM installation.The reports are developed with either BusinessObjects Web Intelligence or Crystal Reports. The authorized users can display reports on the CA SDM Reports Tab.

Role-Based Report Web Forms

If you are an authorized manager or analyst, perform the following:

Follow these steps:

1. Click the Report List icon on the Reports tab to define the report web forms.

2. Additionally, you can click the **Administration**, **Security and Role Management**, **Role Management** to see how Report web forms are managed through the Role List.
   For more information, see Define Role-Based Reports for the Role (see page 3184).

Define Knowledge Report Card Statistics

The Knowledge Report Card provides feedback to analysts and administrators about which knowledge documents are most effective. You can use the provided information to improve the processes of creating knowledge documents and providing the best support to customers.

Note: These statistics are collected only when the Knowledge Report Card calculation service is run, as specified by your Knowledge Management administrator.

As an Analyst, you use the Knowledge Report Card to view statistics about knowledge you submitted and reviewed. These statistics are collected only when the calculation runs, as specified by your Knowledge Management administrator.

Note: The rework versions are not presented when you run the Knowledge Report Card calculation.

Follow these steps:

1. On the Knowledge tab, select View, Knowledge Report Card.

   Note: Access to the Knowledge Report Card tab depends on your role.

   The Knowledge Report Card appears.

2. Complete the following fields as appropriate.

   - **My Documents:** Specifies the number of days on which to recalculate the Report Card statistics.
   - Specifies the section on which to recalculate the Report Card statistics.
   - **My Statistics:** Displays the totals of any documents the analyst has authored as follows:
     - **Submitted** -- Specifies the document totals, regardless of status (Published, Draft, Rework-Draft, Retired).
     - **Published --** Specifies the number of published documents.
     - **Hit --** Specifies the total number of page visits to the knowledge documents.

- **Voted --** Displays the number of votes an individual document has received from its Solution Survey form. You can click the Vote column header to display all documents in descending order, by document votes.

Create a Forum

Forums let you communicate about existing issues. Using the forums, you can share documents globally or among predefined groups that work together in knowledge-sharing and brainstorming over existing challenges. Forums broaden the scope of knowledge contributions by allowing communication on general questions, usability tips, and so on. You can create a forum from the Knowledge tab and from a service desk ticket.

You can create a new forum from the Knowledge tab.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

A forum can be created using the following ways:

- From the Knowledge tab
- From a Knowledge category
- From a Knowledge document
- From a ticket

Follow these steps:

1. Depending on your requirement, perform one of the following actions:
   - From the Knowledge tab, click File, New Forum.
   - From the Knowledge tab, right-click a category, click New Forum.
   - Open a Knowledge Document and click New Forum from the Page Options menu.
   - Click a support ticket (for example, click an incident from My Incidents on the Service Desk tab), Knowledge tab and click New Forum.
2. Specify the title for your post and the question.
3. Click Save.
   The forum is created.
4. (Optional) Click the Attributes tab and select Assignee to assign a contact to the forum during the content approval process task.

Support Automation

This article includes the following topics:

You can implement a support strategy using a combination of processes and tools. CA SDM provides the tools to administer live assistance and develop automated tasks. The application also lets you deliver the tools through various channels.

Use the associated processes to create and maintain an environment that provides the following benefits:

- Reduced average support call duration
- Reduced overall support costs
- Increased resolution rates
- Improved end-user satisfaction

Support Automation Users

System administrators and tenant administrators configure CA SDM contacts, role permissions, access levels, and privacy levels to define user permissions. The users that use Support Automation are as follows:

- **System Administrator**
  Defines system-wide access to add, edit, and modify all Support Automation defaults and functions in the Administration tab. The system administrator sets up tenants and analysts, modifies Support Automation system properties, and performs system password resets.
- **Tenant Administrator**
  Defines administrative rights at the tenant level. The rights do not include granting access to creating or editing other tenants or resetting user passwords. The Service Provider tenant determines permissions.
- **Analyst**
  Defines the rights for users that provide live assistance to end users in your support environment.
- **End User**
  Defines the rights for users that request live assistance from analysts in your support environment, such as employees and customers.

Support Automation Anonymous and Registered Users

The Support Automation server accepts registered or anonymous users, depending on CA SDM permissions. If permitted, the guest user lets anonymous users log in to CA SDM. You can authenticate with the server to gain access to the following tools and services:

- Live Assistance
- Self-Service
- Automated Tasks Editor
- End-User Client

Live Assistance

Live Assistance provides end-user support through tools that enhance remote interaction between analysts and end users. You can use automated, predefined responses to communicate with the end user. You gather detailed information about an end-user computer and act to provide support.

You provide live assistance using the Support Automation Analyst Interface and End-User Client.

Support Automation Analyst Interface

Important! The Support Automation Analyst Interface only runs on Windows. For more information about supported operating systems, see the Supportability Matrix (see page 119).

You can provide Live Assistance to end users by using the Support Automation Analyst Interface. You monitor queues, manage multiple end-user assistance sessions, and interact with end users to resolve their computer problems.

You access Live Assistance from a ticket page, such as an incident, issue or request, or the Support Automation tab. You can also open a CA SDM ticket from Live Assistance.

Important! Analysts without read access to their tenant cannot launch the Support Automation analyst client. A warning message appears in CA SDM, such as from the main Support Automation tab or a ticket.

Use the following tools to provide live assistance to end users in your support environment:

- **Chat**
  Launches instant message to the end user or to use preset text and URLs. If the end user uses the web client, only chat is enabled in a browser. You can request to use the full Support Automation tools by selecting Sessions, Launch Full Tools.

- **Automated Tasks**
  Runs predefined diagnostic or repair scripts on the end-user computer.
  Note: Scripts are created and uploaded from the Automated Task Editor IDE and your administrator configures permissions.

- **File Explorer**
  Browses the files on the end-user computer and lets end users create, modify, rename, or delete files and directories.

- **File Transfer**
  Copies and transfers files and folders to the end-user computer. You can also copy and transfer files from the end-user computer.

- **Remote Registry**
  Performs the following registry management operations:

  - Create, edit, or delete registry records.

  - Export or import registry values from the end-user registry.

- **Screenshot**
  Captures the screenshots of the end-user computer when connection quality is not sufficient for remote control assistance.

- **Remote Control**
  Controls the end-user computer remotely.

- **Remote System Tools**
  Restarts or shuts down the end-user computer.

- **Run Program**
  Launches a program on the end-user computer without using the Remote Control tool.

- **Impersonate**
  Impersonates authentication credentials on the end-user computer, such as a privileged user. Impersonation credentials are configured in System Wide Credentials, Default Credentials.

Note: Your system administrator or tenant administrator can configure access levels, role permissions, and can disable any Live Assistance tools.

End-User Client

The end-user client connects end users to analysts in live assistance sessions. End users chat with analysts in WebChat. When you use the tools in the Support Automation Analyst Interface, the client is launched on the end-user computer. When the client launches, instructions appear for the end user specific to their web browser.

How to Set Up Live Assistance for Analysts

As an administrator, set up the live assistance and manage access levels for tools that the analysts use. You can enable and disable Support Automation tools for specific tenants. If a tool is disabled for a tenant, analysts cannot use that tool in assistance sessions.

Follow these steps:

Set Up Access Level Permission

You can configure the CA SDM roles to have Support Automation permissions. In some cases, there can be a few analysts that are categorized within a single access level. For example, Analyst. In some cases, the tenant administrator sets up many analyst access levels, each with different privileges.

Important! If you are in a multi-tenancy environment, analysts that do not belong to the service provider only have write access to their own tenant and subtenants. You can give the write access to the analyst to other tenants and subtenants. To give the access, update the function access of the accessed tenant and include non-service provider tenants.

The following access levels are available:

- **Analyst**
  Specifies the contact type that provides live assistance to end users in your support environment. Access levels define which queues, automated tasks, and tools are available for the analyst to use.

- **End User**
  Specifies the contact type that receives live assistance from analysts, such as employee and customer.

Create an Analyst Access Level

You can create access levels for Support Automation analysts. Access levels define which queues, automated tasks, and tools analysts use in the Support Automation Analyst Interface.

Follow these steps:

1. Select Security and Role Management, Support Automation Access Control from the Administration tab.
   The Support Automation Access List page appears.

2. Click Create New.
   The Create New Support Automation Access Level page appears.

3. Enter the analyst name, select Analyst from the drop-down list, and click Save.
   The Support Automation Access Level page appears.

4. Click Edit.
   The Update Support Automation Access Level page appears.

5. Assign the appropriate permission, queues, and tools for the access level.

   - Allow to Join Existing Session.

   - Allow to use Automated Tasks IDE.

     Note: In a multi-tenancy environment, enable the Update Public option for analysts that belong to the Service Provider tenant. This setting lets analysts upload task and library content.

6. Click Update Queues on the Queues tab.
   The Queues Assigned Update page appears. You can add the queues this access level can select.

   Note: You can select a queue and click Set Default Queue to set the desired queue as default. The default queue displays at the top of queue list in Support Automation Analyst client. If you do not set a default queue, the queue list displays in alphabetically order.

7. Click Update Tools on the Tools tab to modify the tools this access level can use.
   The Tools Assigned Update page appears.

8. Click Update Target Queues on the Transfer Target Queues tab to modify the queues this access level can select.
   The Target Queues Assigned Update page appears.

9. Click Update Tasks on the Automated Tasks tab to modify the automated tasks this access level can select.
   The Automated Tasks Assigned Update page appears.

10. Click Save.
    The analyst access level is created.

Create an End User Access Level

You can create access levels for end users to determine what actions the analyst can perform on the end-user computer.

Follow these steps:

1. Select Security and Role Management, Support Automation Access Control from the Administration tab.
   The Support Automation Access List page appears.

2. Click Create New.
   The Create New Support Automation Access Level page appears.

3. Enter the end-user name, select End User from the drop-down list, and click Save.
   The Support Automation Access Level Detail page appears.

4. Click Edit to assign the appropriate permissions and security levels.

   - Allow Editing Privacy Level
   - Default Privacy Level
   - End-User Client Launch Mode

   The Update Support Automation Access Level page appears.

5. Click Update Privacy Levels.
   The Privacy Levels Assigned Update page appears.

6. Modify the privacy levels for the end-user access level and click OK.
   The Update Support Automation Access Level page appears.

7. Click Save.
   The end-user access level is created.

Assign an Access Level to a Role

You can assign Support Automation access levels to existing CA SDM roles in your environment.

Follow these steps:

1. Select Security and Role Management, Role Management, Role List from the Administration tab.
   The Role List page appears.

2. Click the role that you want to assign the access level, such as Administrator.
   The Role Detail page appears.

3. Click Edit.
   The Update Role page appears.

4. On the Authorization tab, select the access level that you created from the SA Access drop-down list. Click Save.
   The Role Detail page appears. Verify that the Support Automation access is assigned to the role.

Manage Queues for the Live Assistance Environment

You use queues to route the assistance session requests to the most appropriate analyst. The end user can select a category, or can enter a description of their computer problem. When the ticket (such as an incident) is saved, it routes to the appropriate queue. Consider the following capabilities:

- Set up several queues to sort and track different support requests, according to your business needs. To achieve this capability, you need to assign a queue to an issue and/or incident/ request area.
  For example, you map an issue category to a queue. Once mapped, and the customer selects the same category for a assistance request, he or she is routed to the appropriate queue.
  Similarly, you can map an incident/ request area to a queue. If the end-user has selected the same area, the related assistance session request is routed to this queue.

  Note: If no category is defined to a queue, the assistance session request is routed to the default tenant queue. If the default tenant queue is missing, the default public queue is used.

- You can activate or deactivate queues, specify tenant and analyst permissions.

- Assign a default queue. After the initial product installation, the default queue is named as Support. You can assign only one default queue per tenant.

  Note: If the default tenant queue is missing or unavailable, the default public queue is used.

- Assign the hours of operation for your queues.
  You can manage queues that are based on the availability of users in your support environment. For example, you can enable Support Automation services during business hours.

Important! You can assign workshifts to both your Support Automation hours and individual live assistance queues. Different workshifts assigned to Support Automation hours and individual queues can cause conflicts for analysts and end users in your support environment.

- Establish a session escalation process.

Follow these steps:

1. Select Queues, Queue List from the Support Automation menu.
   The Queue List page appears.

2. Click Create New.

3. On the Create New Queue page, complete the fields. The following fields require explanation:

   - **Default**
     Specifies if this is the default queue. You can route end users to the default queue when their queries do not match the queues in your environment. You must have a default queue.

     Note: You can configure only one default queue per tenant.

   - **Status**
     Specifies the status of the queue.

   - **Default Chat Preset**
     Specifies the default chat preset for the queue.

   - **Queue Hours**

     You can enable Support Automation for each queue for specific hours of the day, to accommodate the working hours of analysts.Use the following procedure:

     - Create a separate schedule for each queue and for all automated support services.

       Note: These settings do not limit self-service functions.

     - Define support hours for the Support Automation server by a global open or close status. An entry for each hour of the week indicates a difference from the global status of the server.

     - The server uses the first entry for each hour that is based on the rules you establish. This action effectively merges the support hour definitions from the parent tenant (or public) settings. This action can have counter-intuitive results if a mix of ‘default-closed’ and ‘default-open’ is used in the hierarchy.

You can set the hours of operation for each queue. The queues determine multi-tenancy, which is optional on the tenant. The queues are automatically filtered from the list page to the tenancy of the currently logged in user.

- **Issue Category**
  Associate an issue category to this queue. When a customer selects the same category for an assistance request, he or she is routed to the appropriate queue.

- **Incident/Request Area**
  Associate an incident/request area to this queue. When a customer selects the same area for an assistance request, he or she is routed to the appropriate queue.

- **Auto Transfer Users**
  Select the check box to automatically transfers the users to another queue if this queue is not addressed within a specified time. You can specify the timeout (in seconds) and the target queue where the users will be transferred.

4. Click Save.

The queue is ready for use.

Note: You can deactivate a queue if it is no longer needed. Edit a queue and select Inactive from the Status drop-down list. You must have at least one queue active. If it is the only queue, you cannot make it inactive.

Manage Activity Notifications for the Live Assistance Environment

As a system administrator, you can modify how end users and analysts track and can receive notifications for activities. For example, a notification can be sent when an analyst ends an assistance session. You create email notifications to alert analysts when they get an assistance session request in their queue. Go to Administration, Notification, Activity Notifications and select a notification.

Select any of the following default notifications (as they are inactive), as appropriate to your environment:

- **Queue Entry Notification**
  Notifies the analyst when an end user joins an assistance session queue and when the session is transferred to another queue.

- **Analyst Notification**
  Notifies the analyst when end-user queue wait time expires. The event of expiration is recognized with a CA SDM Event conditional macro.

- **Invite End User to Assistance Session - Incident**
  Notifies the end user when the analyst invites them to an incident or request assistance session.

- **Invite End User to Assistance Session - Issue**
  Notifies the end user when the analyst invites them to an issue assistance session.

- **Session Ended Notification**
  Notifies the system when the assistance session ends.

> **Note**: When Support Automation is used with an external system such as Star, System_SA_User is set to *Session Ended Notification* by default.

Create Chat Presets for the Live Assistance Environment

You can create common responses to frequently asked questions. Instead of repeatedly typing the same response, you can save a response and can reuse it in other chat sessions. These saved responses are named chat presets. You can send the presets to the end users at the beginning of each session automatically, such as a greeting. You can also automatically populate the presets with information specific to the current session, such as the analyst name.

You can use the following presets types in a live assistance session:

- **Chat Preset**
  Identifies a commonly used text response to an end-user question.

- **URL Preset**
  Identifies a commonly used URL that the end user can access.

You can localize each chat preset. The chat preset is synchronized with the end-user localization so that the end user receives correct localized presets. You can use predefined responses to commonly asked questions and situations.

Create a Chat Preset Group

You can manage chat presets responses into categories (groups).

Follow these steps:

1. Select Tools, Chat Presets, Chat Preset Group List from the Support Automation menu.
   The Chat Preset Group List page appears.

2. Click Create New.
   The Create New Chat Preset Group page appears.

3. Complete the fields and click Save.
   The chat preset group is created.

4. (Optional) Click Edit in List to modify the Chat Preset Group Localizations.
   The Localized Chat Preset Group List page appears.

Create a Text Preset

You can create a chat preset for commonly used text responses to end-user questions. When you save a response, you can use it in other chat sessions.

Follow these steps:

1. Select Tools, Chat Presets, Text Preset List from the Support Automation menu.
   The Chat Text Presets List page appears.

2. Click Create New.
   The Create New Chat Text Preset page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **Default Chat Preset for Session Join**
     Select to define as the default Chat Preset for Session Join.

   - **Text Preset Group**
     Specifies the text preset group.

   - **Text Preset Name**
     Specifies the text preset name.

   - **Preset Text**
     Specifies the text of the preset.

   Click Save.
   The text chat preset is created.

4. (Optional) Click Edit to modify the Localized Chat Text Preset List.
   The Update Chat Text Preset page appears.

5. Click a localization link.
   The Chat Text Preset Localization Detail page appears.

6. Click Edit.
   The Update Chat Text Preset Localization page appears.

7. Enter the localized name and text and click Save.
   The localized text for the text chat preset is added.

Create a URL Preset

You can create a URL preset for a commonly used URL that the end user can access. When you save a URL, you can use it in other chat sessions.

Follow these steps:

1. Select Tools, Chat Presets, URL Preset List from the Support Automation menu.
   The Chat URL Preset List page appears.

2. Click Create New.
   The Create New Chat URL Preset page appears.

3. Complete the following fields:

- **Tenant**
  Specifies the tenant.
- **URL Preset Group**
  Specifies the URL preset group.
- **URL Preset Name**
  Specifies the URL preset name.
- **Preset URL**
  Specifies the URL of the preset.
- **URL Title**
  Title for the URL Preset.

Click Save.
The URL chat preset is created.

4. (Optional) Click Edit to modify the Localized URL Chat Preset List.
   The Update Chat URL Preset appears.
5. Click a localization link.
   The Chat URL Preset Localization Detail page appears.
6. Click Edit.
   The Update Chat URL Preset Localization page appears.
7. Enter the localized URL information and click Save.
   The localized URL preset is added.

Manage Automated Tasks for the Live Assistance Environment

Install and configure the Automated Tasks Editor to manage the automated tasks that the Support Automation analysts use. The end user can launch an automated task from a knowledge document and the self-service interface. Whereas an analyst executes an automated task during an assistance session. The automated tasks provide analysts the detailed information about an end-user computer. You create self-service automated tasks that interact with the end user and process their input. These tasks can change the file system, registry, download install software, and so on.

Follow these steps:

1. Install the Automated Tasks Editor.
   Use the following location and launch the installer on the installation media from the DVD:

   ```
   casd.nt\SAScriptWriter
   ```

   Note: In your support environment, you can also copy and deploy the installer to the appropriate users. The Automated Task Editor is installed and creates a shortcut on your desktop.

2. Double-click to open the Automated Tasks Editor.

3. Click Tools, Server.
   The Server Configuration dialog appears.

4. Enter your hostname and port.

5. Enter the user name and password of a user with read or write access to the Automated Task Editor. For example, Support Automation Analyst.

6. Click Test.
   The tool tries to access the Service Desk application using the webservices call. It also verifies whether the application exists and is able to access it using the credentials.

7. Click OK.
   The automated tasks are created and uploaded to your server.
   You can upload public tasks or can assign them to specific tenants and subtenants.

   Important! Only the roles from the Service Provider tenant can upload tasks and libraries to the server. The roles must have the Update Public flag enabled. All task library content and static content are stored as public data.

The setup is completed and analysts can use this setup to help the users. Support Automation analysts monitor and manage multiple end-user requests in the live assistance sessions. Analysts use Support Automation tools to interact with end users and provide the live assistance. Analysts access the interface from a CA SDM ticket or the Support Automation tab and initiate a session.

How to Set Up Support Automation for a Guest User

As a system administrator, you configure your live assistance environment to allow guest users to interact with the analysts. You can configure a guest user for a specific tenant or can make the user available to the entire system. Tenant is a user who uses a single instance of a software application that serves multiple customers in a multi-tenancy environment.

Follow these steps:

- Create an Access Type for a Guest User (see page 2833)
- Assign the Guest Access Type to a Contact (see page 2834)
- Verify the Guest User (see page 2834)

Create an Access Type for a Guest User

To let the guest users log in to CA SDM without an authentication, create a specific access type in CA SDM. If you are the service provider, you can create a guest access type for each tenant in your environment.

Follow these steps:

1. Log in to CA SDM.

2. On the **Administration** tab, click **Security and Role Management**, **Access Types**.
   The **Access Type List** page opens.

3. Click **Create New**.
   The **Create New Access Type** page opens.

4. Complete the fields as appropriate.

5. Click the **Web Authentication** tab. In the **Validation Type** drop-down list, select **Open-always allow access**.

6. Click **Save**.
   The access type for guest users is created.

7. (Optional) Right-click the **Access Type List** page and select **Refresh**.
   The guest access type appears in the list.

Assign the Guest Access Type to a Contact

Assign the guest access type to a contact after you create an access type. This helps the guest user use Support Automation live assistance functionality. The guest user uses a web authentication to log in to CA SDM. A contact is a person who uses the system regularly.

Follow these steps:

1. On the **Administration** tab, click **Security and Role Management**, **Contacts**.
   The **Contact Search** page opens.

2. Click **Create New**.
   The **Create New Contact** page opens.

3. Select a guest from the **Contact Type** drop-down list.

4. (Optional) **Associate the contact with a tenant and make the contact public**. This association helps the contacts to accept an automatic assignment of a request.

5. Click **Save**.
   The guest access type is assigned to the contact.

Verify the Guest User

After you assign the access type, you can verify the existence of the appropriate users in your environment.

Follow these steps:

1. On the **Administration** tab, click **Security and Role Management**, **Contacts**.
   The **Contact Search** page opens.

2. Select the **Contact Type** as **Guest** and **Access Type** that you have assigned.

3. Click **Search**.
   The **Contact List** page opens.

The contact type and the access type are available on the **Contact List** page.

This step completes the Support Automation setup for a guest user.

How to Resolve Tickets Using Live Assistance

An *assistance session* lets a Service Desk Analyst provide Live Assistance to End Users in CA SDM to resolve tickets. You view details in a CA SDM ticket about an End User that has a computer problem. You chat with the user and can invite the user to an assistance session. Use the Support Automation functionality in CA SDM to resolve tickets using Live Assistance. For example, the End User creates a ticket about a network connection problem with a software application.

Follow these steps:

- Initiate the Live Assistance (see page 2835)
- Provide Live Assistance (see page 2837)
- (Optional) View the Session Log (see page 2839)
- (Optional) View or Modify your Support Automation Security Settings (see page 2840)
- End the Assistance Session and Close the Ticket (see page 2840)

Initiate the Live Assistance

A end user can request live assistance (see page 2841) or submit a ticket that describes an issue.

If a ticket is submitted, the analyst can view the ticket details from an email alert or the CA SDM Scoreboard and launch the support automation interface.

Important! By default, Java uses browser network settings. If you are unable to launch the Support Automation Analyst Interface, change your Java Web Start network settings to "Direct connection" by entering java -viewer in the command line.

Note: Ensure that 32-bit Java Runtime Environment (JRE) version 1.6 or later is installed in your environment. The Support Automation Analyst Interface does not support the 64-bit JRE. Safari browser requires the 32-bit JRE 1.6.0_30 or later. The sa_login_session table creates a record every time an analyst launches the Support Automation Analyst Interface and when an end user launches the Web Client.

Follow these steps:

1. As an analyst, log in to CA SDM and select Scoreboard, My Queue.

2. Open a ticket and review the ticket description.

3. (Optional) Add a comment to the ticket asking the user to provide more information about the application they configured incorrectly.

4. On the Support Automation tab of the ticket Detail page, click Invite End User.

   Note: If you are unable to connect to Support Automation, Edit Browser or Java Connection Setting Options (https://wiki.ca.com/display/CASM/.Edit+Browser+or+Java+Connection+Setting+Options+v14.1).

5. Enter a greeting for the End User.

   - Enter text in the chat window.
   - Whisper a message to the end user.
     Whisper messages do not appear in the Session Log. You can only use whisper messages when more than one analyst handles the session.
   - Push a specific URL to the end user.
     The end user can open the link, or you can open their browser, depending on the administrative settings.
   - Send a preset response to commonly asked questions and common situations.
     Presets can consist of text messages or commonly pushed URLs.

   The message appears in the chat window.

6. Click Launch.
   The Support Automation Analyst Interface appears and you wait for the user to join the assistance session.
   As the end user, you will receive an email notification with the URL to join the session. You can click on the URL from the email notification or click the Join Analyst Now link from the Home page to open the session. The Join Session Code is available in the email (URL).
   Important! You cannot run the Support Automation Analyst Interface on multiple computers using the same login credentials. If you try to launch the interface on one computer, the already running instance appears. If you try to launch the interface on a different computer, a warning message appears telling you that someone is already logged in with the same account.

7. Click Application, Configuration to u se the Communication Configuration dialog to configure your local connection settings. The end-user computer inherits these communication settings in their home directory in a configuration file. Configuring communication settings lets you do the following:

   - Restore a connection when the server fails.
   - Specify a unique proxy with an optional password.
   - View and edit your Support Automation communication settings.

Provide Live Assistance

As an analyst, use the Support Automation Analyst Interface to provide Live Assistance by performing different actions on the end-user computer. Perform the actions such as running diagnostic scripts, browsing the file system, and controlling the end-user computer remotely. For example, a chat session determines that you can resolve the application synchronization issue by using Live Assistance. On the Support Automation Analyst Interface, click the appropriate tool tab to resolve the ticket. For example, execute a program on the end-user computer or force the computer to reboot.

The following table lists the assistance that an analyst can provide:

Assistance	How?
Execute an Automated Task You can execute predefined automated tasks that run on end-user computer. The automated tasks let you gather telemetry information, diagnose common problems, and implement resolutions. The administrator sets your automated task permissions. **Note:** You can enable autorun and execute an automated task when the tool launches.	1. Select an automated Task, click Execute. 2. Right-click the task in the Executed Tasks pane and click View Result.
Browse the End-User File System Browse the file system of the user. For example, browse the hard drive to locate a specific file in the installation directory of the software application. The File Transfer tool can transfer files in both directions (see page).	1. Select File Explorer. 2. Browse the file system of the end user in the assistance session. 3. Use the context menu and select Download to transfer files.
Transfer Files with the End User Transfer a file between computers. For example, transfer a file from your computer to replace a corrupt file in the installation directory.	1. Select File Transfer. 2. Select the appropriate transfer

Assistance	How?
	option, such as Local to Remote. 3. Select the appropriate destination folder, such as Desktop. 4. Click Add to Transfer Queue.
Modify the End-User Registry Browse the end-user registry and modify a registry entry. For example, modify registry values for the software application.	1. Select Remote Registry, navigate through the end-user registry. 2. Modify the appropriate registry entries.
Capture a Screenshot Capture a screenshot of the end-user computer. For example, connection issues prevent remote control from operating successfully, so you guide the user after viewing screenshots.	Click Get Screenshot on the Screenshot tab, click the picture.
Impersonate the End User You can impersonate CA SDM login credentials during an assistance session. By default, you perform actions on the end-user computer with the end-user rights. You can also impersonate user rights with more privileges, such as an administrator. Use impersonation when attempting to use tools that require higher privileges. For example, when modifying the end-user registry, or executing an automated task.	1. Click Session, Impersonate. 2. Select an available impersonation login or use other credentials. 3. Click Impersonate.

Assistance	How?
Control the End-User Computer Remotely You can take full control of the end-user computer, to perform diagnostic and repair functions remotely. You can see and manipulate everything on the end-user computer, as if you were physically sitting at the end-user desk. **Note:** Your administrator establishes security levels for end users. **Note:** Remote Control uses Message Routing Servers to locate the best connection. If the connection quality is poor, you can use screenshots and can chat to diagnose the end-user computer. Connection quality symbols appear on the interface. For example, an excellent connection appears as green, yellow as fair, and red as poor.	1. Select Remote Control. 2. Wait for the end user to click Accept. 3. After the user accepts, control the computer and provide live assistance.
Run a Program on the End-User Computer Execute a program on the end-user computer or force the computer to reboot. For example, execute the configuration interface of the software application.	1. Select Remote System Tools. 2. Enter a command to run on the end-user computer. 3. Click Run Program.

(Optional) View the Session Log

As an analyst, all actions that you perform during the assistance session are updated in the Session Log. The actions include chat dialog (excluding Whisper conversations), automated task results, and using a specific Support Automation Analyst Interface tool.

Follow these steps:

1. Open the active session view.
   The Active Session page appears.

2. Select the Session Log from the toolbar or Sessions menu.
   The Session Log page appears.

3. Click Refresh Now.
   The page refreshes.

4. (Optional) Select the Auto-Refreshing check box.

5. (Optional) Click Save Log to Disk.
   The save dialog appears. You can save the session log locally as an HTML file.

(Optional) View or Modify your Support Automation Security Settings

As an end-user, you can view your Support Automation security settings during an assistance session. The administrator sets your privacy levels for when connecting with analysts. Depending on your settings, analyst actions can prompt you for confirmation, such as remote control. Click Security and select the appropriate security level.

Note: Your administrator sets privacy levels, so some options cannot be modified.

End the Assistance Session and Close the Ticket

As an analyst, after you verify that the ticket has been resolved, update the ticket and close the assistance session.

Follow these steps:

1. Click End in the Support Automation Analyst Interface to close the session.
   The user receives an email notification with the session log.

2. (Optional) Click Session Log to view chat logs and Support Automation tool results.

3. Click the ticket number on the Support Automation Analyst Interface. For example, click Incident 40.
   The Incident 40 Detail page opens in CA SDM.

4. Click Edit.

5. Change the ticket status to SA-Resolved.

6. Click Save and Close.
   The Activity Log for the ticket is saved and the Live Assistance process is complete.

Edit Browser or Java Connection Setting Options

Edit the browser or Java connection setting options if the Support Automation Analyst Interface is unable to connect to the server. The issue occurs when the browser of the analyst is not configured for your environment and the browser fails to launch Live Assistance. You can edit the analyst connection settings from a browser or the Java Control Panel.

Follow these steps:

1. Open any web browser. Click **Tools**, **Internet Options**.

2. Configure the appropriate connection settings, such as a direct connection or proxy server.

3. To configure connection options in the Java Control Panel, enter the following command to open the Java Control Panel:

   ```
   javaws –viewer
   ```

4. On the General tab, click **Network Settings**.
   Configure the appropriate settings, such as a direct connection or proxy server.

Request Live Assistance

You can chat with an analyst to discuss your CA SDM ticket or whenever you need live assistance. The analyst works to diagnose and fix your computer problem.

Follow these steps:

1. Click Live Chat in the Customer Service/Request Support section of your home page.
   The Support Automation Live Chat Launch page appears.

2. Complete the appropriate fields, such as Incident area (employees), Issue category (customers), and description.

3. Click Continue.
   The console displays your position in the help queue.
   The end-user client appears, and you can chat with the analyst.

4. If you are in a non-Windows environment, WebChat appears.
   Your administrator can also enable or disable the end-user client in Windows. If your ticket is not resolved by using WebChat, CA SDM launches the end-user client on your computer. The end-user client lets the analyst perform privileged actions on your computer. Your administrator can enable or disable this option

Important! If you lose connection to an active assistance session, you can rejoin the session in the end user client by double-clicking the temporary shortcut that appears on your desktop. You do not have to log in to CA SDM again.

Note: When the Support Automation end-user client is launched, an executable is downloaded to launch the program. The end user starts it manually, however for security reasons there is a limited time to launch the executable. After the time expires, an error message appears on the end-user computer when they try to start the launcher executable.

Manage Existing Live Assistance Session

Contents

Join Existing Assistance Session

You can join an existing assistance session as a consultant when another analyst invites you to the session.

Follow these steps:

1. Perform *any* of the following tasks:

   - Accept the invitation from another analyst.
     The assistance session appears.

   - Click **Queues** in the Support Automation Analyst Interface.
     Select a handled session.
     Click **Join Queued** User Sessions.

2. Proceed to provide live assistance to the end user.
   You help the other analyst complete the assistance session or they transfer it for you to control.

Invite Another Analyst to the Assistance Session

You can invite another analyst to help you in your assistance session. The invited analyst can perform the same support functions as you, and can take control over the session, if necessary.

Follow these steps:

1. Click I**nvite Analyst** from the active sessions page.
   The list of available analysts appears.

2. Select an analyst from the list, click **Add Analyst**.
   Messages appear indicating the submitted and accepted invite.
   The other analyst joins the assistance session.

Transfer the Assistance Session to Another Analyst

You can transfer an assistance session to another analyst.

Follow these steps:

1. Click Sessions, Transfer Session from the toolbar or the Transfer to Queue button in an active assistance session.
   The list of queues that are available for session transfer appear.

2. Select the appropriate queue and click OK.
   The assistance session transfers to another queue, where another analyst handles it.

Create a Ticket from the Support Automation Analyst Interface

You can create a CA SDM ticket from the Support Automation Analyst Interface, such as an incident.

Follow these steps:

1. Open an active assistance session.
   The active session appears.

2. Provide live assistance to the end user.

3. Select a template, such as *SA-Open* or *SA-Resolved,* from the Status drop-down list.
   CA SDM creates the ticket when you close the assistance session by selecting a status.

> **Note:** Your administrator configures the ticket status types available in Live Assistance.

Associate an Assistance Session with an Existing Ticket

You can associate an assistance session with an existing CA SDM ticket. You can also link multiple assistance sessions to a single ticket.

Follow these steps:

1. Open an assistance session from the queue.
   The assistance session begins.

2. Click Incident, Associate with Existing from the Sessions menu.

> **Note:** The administrator configures the ticket type that you see in the file menu.

3. Enter the ticket number, click OK.
   The CA SDM ticket page appears.

Administering Support Automation

Contents

Update a Support Automation Property

You can modify many of the ways in which Support Automation handles activities to differ from the default installation. You can use the property list settings to modify Support Automation behavior. For example, you can enable or disable some of the following Support Automation properties:

- Display the live chat link to employees and customers on the home page.
- Display the link that lets employees and customers join assistance sessions from the home page.
- Create a CA SDM incident when the end user disconnects while waiting to be served on a Support Automation queue.

You do not have to restart CA SDM after changing the Support Automation properties. However, some properties do require launching the Support Automation client or logging in to CA SDM. The Global properties cannot be tenanted and require restarting CA SDM.

Note: System properties are tenant optional. If a tenant has not defined its properties, Support Automation uses the public (shared) settings. The product installation creates the default public properties.

You can configure the Support Automation properties in the Property List node under Support Automation in the Administrator tab. Select and edti the property. The following properties are available:

Support Automation Properties	Description
system.art.fe.shownetworkdrives	Defines if network drives are displayed in File Explorer. This option is set to True by default, which allows the analyst to see the end-users network drives.
system.chat.agent.msg.color	Specifies the color of the analyst message in the Chat window.
system.chat.agent.showWhisperDialog	Displays the Whisper tab to analysts. When set to False, the whisper tab is removed.
system.chat.agent.url.color	Specifies the color of an analysts URL push in the Chat window, and by default is set to dark blue.

Support Automation Properties	Description
system.chat.agent.whisper.color	Specifies the color of the analyst whisper message in the Chat window and by default is set to blue.
system.chat.autoopen.pushed.urls	Automatically opens the end-users Internet Explorer with the pushed URL sent by the analyst. When you set this feature to False, it does not open the end-users Internet Explorer with the pushed URL. However, the pushed URL is shown in the Chat window and the end user can click it.
system.chat.cust.msg.color	Specifies the color of the end-users chat messages in the Chat window and is set to black by default.
system.chat.logging.removeCreditCards	Specifies that any credit card numbers in chat logs are cleared when they are written to the session log.
system.chat.notifyClientWhenConsultantJoins	Specifies the end user is notified when consulting analysts join or leave an Assistance Session.
system.chat.presets.hideUnusedLocalizations	Displays only the localized presets per the language of the end-user session.
system.chat.showChatPresets	Specifies the chat presets that can be selected in Chat.
system.chat.showTimestamps	Specifies a timestamp with each chat message received.
system.consult.restrictToSameRole	Displays the analysts having at least one Access Control in common with the consulting analyst when in consult.
system.customer.createRejoinLink	Set to False by default. When set to True, it creates a rejoin link on the end-users desktop in case of disconnection from the analyst.

Support Automation Properties	Description
system.customer.view.live.log	Allows the end user to view the Live Log for activities that are performed during their session. If the key is set to False, it removes the Live Log button from the end-users Assistance Session window.
system.log.consulting.inhibitCustomerNotification	Logs in the end-user Live Log when a consulting analyst joins or leaves an Assistance Session. When set to True, the end-user Live Log does not show that a consulting analyst has joined the Assistance Session.
system.security.forceFIPSCompliance	Forces the encryption to use FIPS Compliant libraries. This option requires a client-side download of 3.2 MB in addition to normal downloads.
system.security.prompt.autoallow	Indicates whether the end-user executable automatically allows the requested action to occur after the prompt timeout expires.
system.security.prompt.timeout	Specifies the duration of the countdown on the end-user security prompt.
system.selfServe.maxScriptsAllowed	Specifies the maximum number of scripts an end user can execute before they are offered Live Automation.
system.selfServe.maxSessionTimeAllowed	Specifies the maximum time (in minutes) a Self-Service Automation session can run.
system.sharing.countdown	Specifies the countdown that end users see before giving permission to the analyst to share a desktop.
system.sharing.countdown.defaultAction	Declines desktop sharing when the countdown has reached zero. If this key is set to True, desktop sharing initiates after the countdown has reached zero.
system.sharing.default.color	Sets the default color quality when the Remote Control starts.
system.sharing.drs.mainserver.	Specifies the main server is a Message Routing Server. Setting this value to false off-loads MRS traffic (remote control, and so on) from the main server. It also improves performance for some larger deployments, depending on system configuration and

Support Automation Properties	Description
enabled (Global Property)	usage patterns. Ensure that an MRS equivalent to the main server has been configured before you enable this setting. If it is not configure, you may experience a drop in remote control performance. **Note:** The Global properties cannot be tenanted and cannot require a CA SDM restart.
system. sharing. takecontrol. default	Gives the control of the mouse and keyboard to the analyst when sharing the desktop. The end user can enable or disable this check box whenever desktop sharing is requested.
system. sharing. takecontrol. prompt	Prompts the end user when the analyst tries to take control of the mouse and keyboard. If this key is set to False, the message is disabled and the end user is not prompted.
system. SDM. HomePage. LiveChat. Link	Enables or disables the link for live chat from the CA SDM Employee and Customer home page.
system. SDM. HomePage. JoinSession. Link	Enables or disables the link for joining a session from the CA SDM Employee and Customer home page.
system.use. WebChat	Specifies to use the Web Client instead of the End-User Client.
system. SDM. create. abandon. Incident	Enables or disables the option of creating a CA SDM Incident when the end user disconnects while waiting to be served on a Support Automation queue.
system. SDM. analyst.JRE. Location	Specifies the URL of the JRE installation page.
system. dataRoutin gServers	Enables or disables the Message Routing Server option.

Create a Privacy Level

Privacy levels determine the actions that are allowed to be performed on different end users to protect user privacy. Privacy levels are associated with Support Automation Access Control. Three default permissions exist: High, Medium, and Low, but more can be defined if necessary. You can add, update, and delete the privacy levels that are available to the end user.

You can set the privacy level name and its description. You can define permissions for specified tools (File explorer, Remote registry, Run program) that are enabled for this privacy level.

Follow these steps:

1. Select Settings, Privacy Levels from the Support Automation menu.
   The Privacy Levels List page appears.

2. Click Create new.
   The Create New Privacy Level page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **Privacy Level Name**
     Specifies the privacy level name.

   - **Privacy Level**
     Specifies the privacy level.

   - **Privacy Level Description**
     Describes the privacy level.

4. (Optional) You can define permissions for specified tools (File explorer, Remote registry, Run program) that are enabled for this privacy level. When an analyst is assigned this privacy level, these tools are available for use. On the Permissions tab, select the Function name and click Yes or No from the drop-down list.

5. (Optional) You can modify the privacy level name and its description. You can also define which functions are enabled for this privacy level. On the Localization tab, select the Localization name to modify the name and description.

6. Click Save.
   The privacy level is created.

Create a Request/Incident Template Association

You can specify which Request/Incident ticket templates are available for the Analyst interface. You can also set the template as default or inactive.

Follow these steps:

1. Select Service Desk Integration, Request/Incident Templates Association from the Support Automation menu.
   The Request/Incident Templates Association List page appears.

2. Click Create New.
   The Create New Request Template Association page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **Name**
     Specifies the template name.

   - **Set Ticket Status to**
     Specifies the ticket status that is set for the association.

   - **Default**
     Specifies if the template is the default template.

   - **Active**
     Specifies if the template is active.

   Click Save.
   The request template is created.

Create an Issue Template Association

You can specify which Issue ticket templates are available for the Analyst UI. You can also set the template as default or inactive.

Follow these steps:

1. Select Service Desk Integration, Issue Templates Association from the Support Automation menu.
   The Issue Templates Association List page appears.

2. Click Create New.
   The Create New Issue Template Association page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **Name**
     Specifies the template name.

   - **Set Ticket Status to**
     Specifies the ticket status to set for the association.

- **Default**
  Specifies if the template is the default template.

- **Active**
  Specifies if the template is active.

Click Save.
The issue template is created.

Create a Support Automation Hour Configuration

You can set Support Automation to operate at specific hours or to operate always. You manage these hours of operation that is based on the needs of end users in your support environment. The end users cannot access Support Automation functionality when operation hours are over. You can make quick changes to several workshifts in a single step.

Important! You can assign workshifts to both your Support Automation hours and individual live assistance queues. Different workshifts that are assigned to Support Automation hours and individual queues can cause conflicts for analysts and end users in your support environment.

Each tenant can have one active configuration. A newly created configuration is active until another active configuration is defined.

Follow these steps:

1. Select Settings, Support Automation Hours from the Support Automation menu.
   The Support Automation Hours page appears.

2. Click Create New.
   The Create New Support Automation Hours page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **Label**
     Specifies the name that displays.

   - **Workshift**
     Specifies the hours.

4. Click Save.

The hours of operation are saved.

Create a Queue Summary

Queue summaries enable the support automation analyst to view the end-user information (for example, language) before starting a live chat. An administrator can configure the type of information that can be displayed from CA SDM. The Queue Summaries are public. You can add a queue summary for a specific tenant. If you want to select more than one queue summary, define the order in which they are supposed to appear.

Follow these steps:

1. Select Queues, Queue Summary from the Support Automation menu.
   The Queue Summary Fields List page appears.

2. Click Create New.
   The Add New Queue Summary Field page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant for the queue.

   - **Field**
     Specifies the field name.

   - **Order**
     Specifies the order that you want the field to display.

4. Click Save.
   The queue summary is created. For example, if the administrator has selected IP Address, Language, Questions, and Status, then the analyst will see the information (under End Users in Queue) on the analyst console.

Support Automation Connectivity

The analyst and end user never communicate directly with each other. You do not require a direct peer-to-peer connectivity between the two users. Data transfer is routed through the server, verifying that you can communicate even when the end-user computers are behind firewalls.

You can connect to end-user computers using the following connections:

- **Socket**
  Using a socket connection is the best way for you to connect. The socket connections are the fastest and the most efficient, with the least overhead, and minimal latency.

- **HTTP (or HTTPS)**
  Using an HTTP connection is better than a direct socket connection, because corporate firewalls can block direct socket connections. The HTTP connections generate a significant amount of network traffic overhead, when compared to direct socket connections. The number of simultaneous sessions is lower when the connections to the server are over HTTP. This happens due to the overhead and processing on the server,

- **Proxy**
  Socket Proxy is a mode of operation for the Support Automation server to off-load some of the CPU-intensive operations. For example, encryption or decryption from the main server, and a server component that can go into the DMZ within the logical network topology.

Typically, you attempt to connect through the direct socket connection first. If the direct socket connection fails, then connect through HTTP. However, you can specify custom connection settings on the client computer to alter this sequence.

How to Overcome Server Load

In large deployments, high server load can degrade the application performance. For this reason, you can off-load some of the processing to one or more Socket Proxy servers as follows:

- Offload encryption and decryption of the incoming and outgoing data for all analysts or clients. The clients must connect either through Direct Socket or through HTTP.
- Offload the processing of HTTP traffic from and to those clients connecting through HTTP to the Socket Proxy.

Use Socket Proxy Within DMZ

In some network environments, allowing direct socket access to the application servers that run Support Automation can be considered a security risk. In such environments, you can use Socket Proxy within the DMZ. Using Socket Proxy in this scenario offloads some of the processing from the main server. The Socket Proxy works as follows:

1. On the configured external port, the Socket Proxy listens for incoming connections from analysts or end users.
2. The Socket Proxy establishes a peer connection to the main server on the configured internal port for every connection. These two connections are named the end-user connection and the server connection, respectively.
3. The end-user connections are encrypted and the Socket Proxy encrypts or decrypts data coming in or going out. The server connection is not encrypted.
4. For each incoming data-packet, the protocol structure is verified and a checksum value is validated. This happens before the data is passed on to the main server through the server connection.
5. The main server off-loads the encryption and decryption processing.
6. The Socket Proxy closes the matching peer connection once the end user or server connection closes.

Create a Message Routing Server

Use Message Routing Servers (MRS) to manage multiple Remote Control servers, based on the geographical location of the local server. Using MRS helps improve performance during assistance sessions. When you enable MRS, the analyst interface and end-user client connect to the analysts preferred (local) server for sharing. If the connection is unsuccessful, the sharing session falls back to the main default server. The Live Log records which MRS you use during the assistance session.

You can create, search for, update, remove, enable, or disable a message routing server object.

Note: To use this option, the *system.dataRoutingServers* system property must be enabled in the Property List.

Follow these steps:

1. Select Settings, Message Routing Servers from the Support Automation menu.
   The Message Routing Servers List page appears.

2. Click Create New.
   The Create New Message Routing Server page appears.

3. Complete the following fields:

   - **Active**
     Specifies that the message routing server is active. When you enable the MRS, the analyst interface and end-user agent connect to the analysts preferred (local) server for sharing.

   - **Label**
     Specifies the name of the message routing server.

   - **Socket Server Host**
     Specifies the host for the socket server.

   - **Socket Server Port**
     Specifies the port for the socket server.

   - **HTTP Connection URL**
     Specifies the URL for the HTTP connection.

4. Click Save.
   The new Message Routing Server is saved.

Update a Support Automation Property

You can modify many of the ways in which Support Automation handles activities to differ from the default installation. You can use the property list settings to modify Support Automation behavior. For example, you can enable or disable some of the following Support Automation properties:

- Display the live chat link to employees and customers on the home page.

- Display the link that lets employees and customers join assistance sessions from the home page.
- Create a CA SDM incident when the end user disconnects while waiting to be served on a Support Automation queue.

You do not have to restart CA SDM after changing the Support Automation properties. However, some properties do require launching the Support Automation client or logging in to CA SDM. The Global properties cannot be tenanted and require restarting CA SDM.

Note: System properties are tenant optional. If a tenant has not defined its properties, Support Automation uses the public (shared) settings. The product installation creates the default public properties.

You can configure the Support Automation properties in the Property List node under Support Automation in the Administrator tab. Select and edti the property. The following properties are available:

Support Automation Properties	Description
system.art.fe.shownetworkdrives	Defines if network drives are displayed in File Explorer. This option is set to True by default, which allows the analyst to see the end-users network drives.
system.chat.agent.msg.color	Specifies the color of the analyst message in the Chat window.
system.chat.agent.showWhisperDialog	Displays the Whisper tab to analysts. When set to False, the whisper tab is removed.
system.chat.agent.url.color	Specifies the color of an analysts URL push in the Chat window, and by default is set to dark blue.
system.chat.agent.whisper.color	Specifies the color of the analyst whisper message in the Chat window and by default is set to blue.
system.chat.autoopen.pushed.urls	Automatically opens the end-users Internet Explorer with the pushed URL sent by the analyst. When you set this feature to False, it does not open the end-users Internet Explorer with the pushed URL. However, the pushed URL is shown in the Chat window and the end user can click it.
system.chat.cust.msg.color	Specifies the color of the end-users chat messages in the Chat window and is set to black by default.

Support Automation Properties	Description
system.chat.logging.removeCreditCards	Specifies that any credit card numbers in chat logs are cleared when they are written to the session log.
system.chat.notifyClientWhenConsultantJoins	Specifies the end user is notified when consulting analysts join or leave an Assistance Session.
system.chat.presets.hideUnusedLocalizations	Displays only the localized presets per the language of the end-user session.
system.chat.showChatPresets	Specifies the chat presets that can be selected in Chat.
system.chat.showTimestamps	Specifies a timestamp with each chat message received.
system.consult.restrictToSameRole	Displays the analysts having at least one Access Control in common with the consulting analyst when in consult.
system.customer.createRejoinLink	Set to False by default. When set to True, it creates a rejoin link on the end-users desktop in case of disconnection from the analyst.
system.customer.view.live.log	Allows the end user to view the Live Log for activities that are performed during their session. If the key is set to False, it removes the Live Log button from the end-users Assistance Session window.
system.log.consulting.inhibitCustomerNotification	Logs in the end-user Live Log when a consulting analyst joins or leaves an Assistance Session. When set to True, the end-user Live Log does not show that a consulting analyst has joined the Assistance Session.
system.security.forceFIPSCompliance	Forces the encryption to use FIPS Compliant libraries. This option requires a client-side download of 3.2 MB in addition to normal downloads.

Support Automation Properties	Description
system.security.prompt.autoallow	Indicates whether the end-user executable automatically allows the requested action to occur after the prompt timeout expires.
system.security.prompt.timeout	Specifies the duration of the countdown on the end-user security prompt.
system.selfServe.maxScriptsAllowed	Specifies the maximum number of scripts an end user can execute before they are offered Live Automation.
system.selfServe.maxSessionTimeAllowed	Specifies the maximum time (in minutes) a Self-Service Automation session can run.
system.sharing.countdown	Specifies the countdown that end users see before giving permission to the analyst to share a desktop.
system.sharing.countdown.defaultAction	Declines desktop sharing when the countdown has reached zero. If this key is set to True, desktop sharing initiates after the countdown has reached zero.
system.sharing.default.color	Sets the default color quality when the Remote Control starts.
system.sharing.drs.mainserver.enabled (Global Property)	Specifies the main server is a Message Routing Server. Setting this value to false off-loads MRS traffic (remote control, and so on) from the main server. It also improves performance for some larger deployments, depending on system configuration and usage patterns. Ensure that an MRS equivalent to the main server has been configured before you enable this setting. If it is not configure, you may experience a drop in remote control performance. **Note:** The Global properties cannot be tenanted and cannot require a CA SDM restart.
system.sharing.takecontrol.default	Gives the control of the mouse and keyboard to the analyst when sharing the desktop. The end user can enable or disable this check box whenever desktop sharing is requested.

Support Automation Properties	Description
system.sharing.takecontrol.prompt	Prompts the end user when the analyst tries to take control of the mouse and keyboard. If this key is set to False, the message is disabled and the end user is not prompted.
system.SDM.HomePage.LiveChat.Link	Enables or disables the link for live chat from the CA SDM Employee and Customer home page.
system.SDM.HomePage.JoinSession.Link	Enables or disables the link for joining a session from the CA SDM Employee and Customer home page.
system.use.WebChat	Specifies to use the Web Client instead of the End-User Client.
system.SDM.create.abandon.Incident	Enables or disables the option of creating a CA SDM Incident when the end user disconnects while waiting to be served on a Support Automation queue.
system.SDM.analyst.JRE.Location	Specifies the URL of the JRE installation page.
system.dataRoutingServers	Enables or disables the Message Routing Server option.

Create a Privacy Level

Privacy levels determine the actions that are allowed to be performed on different end users to protect user privacy. Privacy levels are associated with Support Automation Access Control. Three default permissions exist: High, Medium, and Low, but more can be defined if necessary. You can add, update, and delete the privacy levels that are available to the end user.

You can set the privacy level name and its description. You can define permissions for specified tools (File explorer, Remote registry, Run program) that are enabled for this privacy level.

Follow these steps:

1. Select Settings, Privacy Levels from the Support Automation menu.
   The Privacy Levels List page appears.

2. Click Create new.
   The Create New Privacy Level page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **Privacy Level Name**
     Specifies the privacy level name.

   - **Privacy Level**
     Specifies the privacy level.

   - **Privacy Level Description**
     Describes the privacy level.

4. (Optional) You can define permissions for specified tools (File explorer, Remote registry, Run program) that are enabled for this privacy level. When an analyst is assigned this privacy level, these tools are available for use. On the Permissions tab, select the Function name and click Yes or No from the drop-down list.

5. (Optional) You can modify the privacy level name and its description. You can also define which functions are enabled for this privacy level. On the Localization tab, select the Localization name to modify the name and description.

6. Click Save.
   The privacy level is created.

Integrate with Support Automation Tickets

Contents

You can integrate Support Automation tickets with CA SDM by specifying which ticket templates are available for the Analyst Interface. You can select the ticket templates for Incident/Requests and Issue ticket types.

You can define if the template is default or active. When you create a ticket template, you can select from existing CA SDM templates. The default template must be active.

You can have only one ticket template as a default per tenant.

Create a Request/Incident Template Association

You can specify which Request/Incident ticket templates are available for the Analyst UI. You can also set the template as default or inactive.

Follow these steps:

1. Select Service Desk Integration, Request/Incident Templates Association from the Support Automation menu.
   The Request/Incident Templates Association List page appears.

2. Click Create New.
   The Create New Request Template Association page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **Name**
     Specifies the template name.

   - **Set Ticket Status to**
     Specifies the ticket status that is set for the association.

   - **Default**
     Specifies if the template is the default template.

   - **Active**
     Specifies if the template is active.

   Click Save.
   The request template is created.

Create an Issue Template Association

You can specify which Issue ticket templates are available for the Analyst UI. You can also set the template as default or inactive.

Follow these steps:

1. Select Service Desk Integration, Issue Templates Association from the Support Automation menu.
   The Issue Templates Association List page appears.

2. Click Create New.
   The Create New Issue Template Association page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **Name**
     Specifies the template name.

   - **Set Ticket Status to**
     Specifies the ticket status to set for the association.

   - **Default**
     Specifies if the template is the default template.

- **Active**
  Specifies if the template is active.

Click Save.
The issue template is created.

Create a Support Automation Hour Configuration

You can set Support Automation to operate at specific hours or to operate always. You manage these hours of operation that is based on the needs of end users in your support environment. The end users cannot access Support Automation functionality when operation hours are over. You can make quick changes to several workshifts in a single step.

Important! You can assign workshifts to both your Support Automation hours and individual live assistance queues. Different workshifts that are assigned to Support Automation hours and individual queues can cause conflicts for analysts and end users in your support environment.

Each tenant can have one active configuration. A newly created configuration is active until another active configuration is defined.

Follow these steps:

1. Select Settings, Support Automation Hours from the Support Automation menu.
   The Support Automation Hours page appears.

2. Click Create New.
   The Create New Support Automation Hours page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **Label**
     Specifies the name that displays.

   - **Workshift**
     Specifies the hours.

   Click Save.
   The hours of operation are saved.

Create Queue Summary

Queue summaries enable the support automation analyst to view the end-user information (for example, language) before starting a live chat. An administrator can configure the type of information that can be displayed from CA SDM. The Queue Summaries are public. You can add a queue summary for a specific tenant. If you want to select more than one queue summary, define the order in which they are supposed to appear.

Follow these steps:

1. Select Queues, Queue Summary from the Support Automation menu.
   The Queue Summary Fields List page appears.

2. Click Create New.
   The Add New Queue Summary Field page appears.

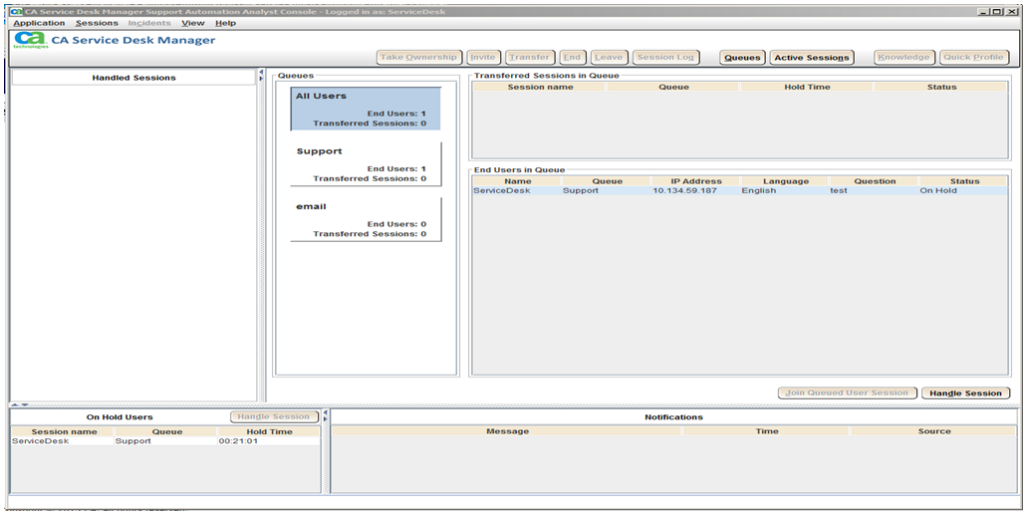
3. Complete the following fields:

   - **Tenant**
     Specifies the tenant for the queue.

   - **Field**
     Specifies the field name.

   - **Order**
     Specifies the order that you want the field to display.

   Click Save.
   The queue summary is created. For example, if the administrator has selected IP Address, Language, Questions, and Status, then the analyst will see the information (under End Users in Queue) on the analyst console, as displayed in the following diagram:



Queue Summaries

Manage Connnectivity

Support Automation Connectivity

The analyst and end user never communicate directly with each other. You do not require a direct peer-to-peer connectivity between the two users. Data transfer is routed through the server, verifying that you can communicate even when the end-user computers are behind firewalls.

You can connect to end-user computers using the following connections:

- **Socket**
  Using a socket connection is the best way for you to connect. The socket connections are the fastest and the most efficient, with the least overhead, and minimal latency.

- **HTTP (or HTTPS)**
  Using an HTTP connection is better than a direct socket connection, because corporate firewalls can block direct socket connections. The HTTP connections generate a significant amount of network traffic overhead, when compared to direct socket connections. The number of simultaneous sessions is lower when the connections to the server are over HTTP. This happens due to the overhead and processing on the server,

- **Proxy**
  Socket Proxy is a mode of operation for the Support Automation server to off-load some of the CPU-intensive operations. For example, encryption or decryption from the main server, and a server component that can go into the DMZ within the logical network topology.

Typically, you attempt to connect through the direct socket connection first. If the direct socket connection fails, then connect through HTTP. However, you can specify custom connection settings on the client computer to alter this sequence.

How to Overcome Server Load

In large deployments, high server load can degrade the application performance. For this reason, you can off-load some of the processing to one or more Socket Proxy servers as follows:

- Offload encryption and decryption of the incoming and outgoing data for all analysts or clients. The clients must connect either through Direct Socket or through HTTP.

- Offload the processing of HTTP traffic from and to those clients connecting through HTTP to the Socket Proxy.

Use Socket Proxy Within DMZ

In some network environments, allowing direct socket access to the application servers that run Support Automation can be considered a security risk. In such environments, you can use Socket Proxy within the DMZ. Using Socket Proxy in this scenario offloads some of the processing from the main server. The Socket Proxy works as follows:

1. On the configured external port, the Socket Proxy listens for incoming connections from analysts or end users.

2. The Socket Proxy establishes a peer connection to the main server on the configured internal port for every connection. These two connections are named the end-user connection and the server connection, respectively.

3. The end-user connections are encrypted and the Socket Proxy encrypts or decrypts data coming in or going out. The server connection is not encrypted.

4. For each incoming data-packet, the protocol structure is verified and a checksum value is validated. This happens before the data is passed on to the main server through the server connection.

5. The main server off-loads the encryption and decryption processing.

6. The Socket Proxy closes the matching peer connection once the end user or server connection closes.

Create a Message Routing Server

Use Message Routing Servers (MRS) to manage multiple Remote Control servers, based on the geographical location of the local server. Using MRS helps improve performance during assistance sessions. When you enable MRS, the analyst interface and end-user client connect to the analysts preferred (local) server for sharing. If the connection is unsuccessful, the sharing session falls back to the main default server. The Live Log records which MRS you use during the assistance session.

You can create, search for, update, remove, enable, or disable a message routing server object.

Note: To use this option, the *system.dataRoutingServers* system property must be enabled in the Property List.

Follow these steps:

1. Select Settings, Message Routing Servers from the Support Automation menu.
   The Message Routing Servers List page appears.

2. Click Create New.
   The Create New Message Routing Server page appears.

3. Complete the following fields:

   - **Active**
     Specifies that the message routing server is active. When you enable the MRS, the analyst interface and end-user agent connect to the analysts preferred (local) server for sharing.

   - **Label**
     Specifies the name of the message routing server.

   - **Socket Server Host**
     Specifies the host for the socket server.

- **Socket Server Port**
  Specifies the port for the socket server.

- **HTTP Connection URL**
  Specifies the URL for the HTTP connection.

Click Save.
The new Message Routing Server is saved.

Support Automation User Administration

This article contains the following topics:

System administrators and tenant administrators configure CA SDM contacts, role permissions, access levels, and privacy levels to define user permissions. The users that use Support Automation are as follows:

- **System Administrator**
  Defines system-wide access to add, edit, and modify all Support Automation defaults and functions in the Administration tab. The system administrator sets up tenants and analysts, modifies Support Automation system properties, and performs system password resets.

- **Tenant Administrator**
  Defines administrative rights at the tenant level. The rights do not include granting access to creating or editing other tenants or resetting user passwords. The Service Provider tenant determines permissions.

- **Analyst**
  Defines the rights for users that provide live assistance to end users in your support environment.

- **End User**
  Defines the rights for users that request live assistance from analysts in your support environment, such as employees and customers.

Support Automation Anonymous and Registered Users

The Support Automation server accepts registered or anonymous users, depending on CA SDM permissions. If permitted, the guest user lets anonymous users log in to CA SDM. You can authenticate with the server to gain access to the following tools and services:

- Live Assistance
- Self-Service
- Automated Tasks Editor
- End-User Client

Support Automation Access Level Administration

You manage Support Automation access levels and assign them to CA SDM roles in your support environment. Support environments vary in size and structure, so your implementation of access levels can vary.

In some cases, there can be a few analysts that are categorized within a single access level. For example, Analyst. In some cases, the tenant administrator sets up many analyst access levels, each with different privileges.

Important! If you are in a multi-tenancy environment, analysts that do not belong to the service provider only have write access to their own tenant and subtenants. You can give the write access to the analyst to other tenants and subtenants. To give the access, update the function access of the accessed tenant and include non-service provider tenants.

The following access levels are available:

- **Analyst**
  Specifies the contact type that provides live assistance to end users in your support environment. Access levels define which queues, automated tasks, and tools are available for the analyst to use.

- **End User**
  Specifies the contact type that receives live assistance from analysts, such as employee and customer.

You manage Support Automation access levels from the Administration tab. For more information about Support Automation access levels, see the Support Automation Access Control (see page 2864) article.

Support Automation Queue Administration

This article contains the following topics:

You use queues to route assistance session requests to the most appropriate analyst. The end user can select a category, or can enter a description of their computer problem. The ticket (such an as incident) is then routed to the appropriate queue.

After the initial product installation, the default queue is named Support. You can set up several queues to sort and track different support requests, according to your business needs. You can assign only one default queue per tenant. If a default is not set or it is unavailable, the public default queue is used. You set the working hours per queue.

The system automatically determines where to place the end user by mapping queues to incident areas. If mapped, and the end user selects a category, the end user is routed to the appropriate queue. The search capabilities are applied to the description of an incident or issue category to identify relevant queues. The end user is routed to the best matched queue.

You can perform the following queue management activities:

- Add (define) uniquely named queues to sort and differentiate between support requests.
- Specify the hours of operation for each queue.
- Deactivate a queue that is no longer needed.
- Assign a default queue for support requests to enter when no Issue category or Incident/Request Area is selected.
- Establish a session escalation process.

The Queue list page displays a list of queues containing information about each queue. You can manipulate the queue details.

Queue Management

You configure queues to help end users receive the appropriate live assistance from analysts. You manage queues to improve how end users are routed to assistance sessions as follows:

- Customize the queues for analysts and tenants in your live assistance environment.
  You can activate or deactivate queues and specify tenant and analyst permissions.
- Assign a default queue.
  You can route end users to the default queue when their queries do not match the queues in your environment. You can also customize queues for tenants in your environment.

  Note: If the default tenant queue is missing or unavailable, the public queue is used.

- Assign the hours of operation for your queues.
  You can manage queues that are based on the availability of users in your support environment. For example, you can enable Support Automation services during business hours.

  - **Important!** You can assign workshifts to both your Support Automation hours and individual live assistance queues. Different workshifts assigned to Support Automation hours and individual queues can cause conflicts for analysts and end users in your support environment.

Create a Queue

You can add or define a uniquely named queue to sort and differentiate between support requests.

Follow these steps:

1. Select Queues, Queue List from the Support Automation menu.
   The Queue List page appears.

2. Click Create New.
   The Create New Queue page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant for the queue.

   - **Queue Name**
     Specifies the queue name.

   - **End User Display Name**
     Specifies the name that displays for the end user.

   - **Default**
     Specifies if the queue is the default queue.

   - **Status**
     Specifies the status of the queue.

   - **Default Chat Preset**
     Specifies the default chat preset for the queue.

   - **Queue Hours**
     Specifies the queue hours.

   - **Issue Category**
     Specifies the Issue Category that is associated with this queue.

   - **Incident/Request Area**
     Specifies the Inciedent/request Area that is associated with this queue.

   - **Auto Transfer Users**
     Transfers the users to this queue automatically.

   Click Save.
   The queue is created.

Search for a Queue

You can search for queues by Name, Customer display name, and Status fields. You can view and edit queue details using the links on queue names.

Follow these steps:

1. Select Queues, Queue List from the Support Automation menu.
   The Queue List page appears.

2. Click Show Filter.

3. Complete the fields and click Search.
   The search limits the list to the information of interest.

Note: Click Export to export the list results to a Microsoft Excel (.xls) file.

Set Queue Hours of Operation

You can enable Support Automation for each queue for specific hours of the day, to accommodate the working hours of analysts.

Use the following procedure:

- Create a separate schedule for each queue and for all automated support services.

  Note: These settings do not limit self-service functions.

- Define support hours for the Support Automation server by a global open or close status. An entry for each hour of the week indicates a difference from the global status of the server.

- The server uses the first entry for each hour that is based on the rules you establish.
  This action effectively merges the support hour definitions from the parent tenant (or public) settings. This action can have counter-intuitive results if a mix of 'default-closed' and 'default-open' is used in the hierarchy.

You can set the hours of operation for each queue. The queues determine multi-tenancy, which is optional on the tenant. The queues are automatically filtered from the list page to the tenancy of the currently logged in user.

Follow these steps:

1. Select Queues, Queue List from the Support Automation menu.
   The Queue List page appears.

2. Click a queue.
   The Queue Detail page appears.

3. Click Edit to modify to the settings.
   The Update Queue page appears.

4. Click Queue Hours.
   The Workshift Search page appears.

5. Complete the information and click Save.
   The hours of operation are saved.

Deactivate a Queue

You can deactivate a queue that is no longer needed. You must have at least one queue active. If it is the only queue, you cannot make it inactive.

Follow these steps:

1. Select Queues, Queue List from the Support Automation menu.
   The Queue List page appears.

2. Click a queue.
   The Queue Detail page appears.

3. Click Edit to modify to the settings.
   The Update Queue page appears.

4. Select Inactive from the Status drop-down list and click Save.
   The queue is deactivated.

Assign a Default Queue

You can route end users to the default queue when their queries do not match the queues in your environment. You must have a default queue.

Note: You can configure only one default queue per tenant.

Follow these steps: Select Queues, Queue List from the Support Automation menu.

1. The Queue List page appears.

2. Click a queue.
   The Queue Detail page appears.

3. Click Edit to modify to the settings.
   The Update Queue page appears.

4. Select the Default check box and click Save.
   The queue is set as default.

Establish an Auto Transfer Process

You can establish an auto transfer process for each queue.

Follow these steps:

1. Select Queues, Queue List from the Support Automation menu.
   The Queue List page appears.

2. Click a queue.
   The Queue Detail page appears.

3. Click Edit to modify to the settings.
   The Update Queue page appears.

4. Complete the following fields:

   - **Issue Category**
     Specifies the Issue Category that is associated with this queue.

   - **Auto Transfer Users**
     Transfers the users to this queue automatically.

   Click Save.
   The auto transfer process is saved for the queue.

How to Configure Support Automation Role Permissions

This article contains the following topics:

You can configure the CA SDM roles to have Support Automation permissions. You can set role permissions by configuring Support Automation access levels for analysts and privacy levels for end users. You set role permissions in your live assistance environment as follows:

1. Configure the appropriate access levels for analysts (see page 2870) in your live assistance environment.
   You create access levels to manage permissions for analysts. The permissions could be enabling or disabling specific Support Automation Analyst Interface tools.

2. Configure the appropriate privacy levels for end users (see page 2872) in your live assistance environment.
   You create privacy levels to manage end-user access levels in your system.

3. Assign (see page 2872) access levels to roles.
   You assign end-user privacy levels and analyst access levels to roles in your environment.

For more information about Support Automation access levels for analysts and security levels for end users, see the Support Automation Access Control topic.

Create an Analyst Access Level

You can create access levels for Support Automation analysts. Access levels define which queues, automated tasks, and tools analysts use in the Support Automation Analyst Interface.

To create an analyst access level:

1. Select Security and Role Management, Support Automation Access Control from the Administration tab.
   The Support Automation Access List page appears.

2. Click Create New.
   The Create New Support Automation Access Level page appears.

3. Enter the analyst name, select Analyst from the drop-down list, and click Save.
   The Support Automation Access Level page appears.

4. Click Edit.
   The Update Support Automation Access Level page appears.

5. Assign the appropriate permission, queues, and tools for the access level.

   - Allow to Join Existing Session.

   - Allow to use Automated Tasks IDE.

   Note: In a multi-tenancy environment, enable the Update Public option for analysts that belong to the Service Provider tenant. This setting lets analysts upload task and library content.

6. Click Update Queues on the Queues tab.
   The Queues Assigned Update page appears. You can add the queues this access level can select.

   Note: You can select a queue and click Set Default Queue to set the desired queue as default. The default queue displays at the top of queue list in Support Automation Analyst client. If you do not set a default queue, the queue list displays in alphabetically order.

7. Click Update Tools on the Tools tab to modify the tools this access level can use.
   The Tools Assigned Update page appears.

8. Click Update Target Queues on the Transfer Target Queues tab to modify the queues this access level can select.
   The Target Queues Assigned Update page appears.

9. Click Update Tasks on the Automated Tasks tab to modify the automated tasks this access level can select.
   The Automated Tasks Assigned Update page appears.

10. Click Save.
    The analyst access level is created.

Create an End User Access Level

You can create access levels for end users to determine what actions the analyst can perform on the end-user computer.

To create an end-user access level:

1. Select Security and Role Management, Support Automation Access Control from the Administration tab.
   The Support Automation Access List page appears.

2. Click Create New.
   The Create New Support Automation Access Level page appears.

3. Enter the end-user name, select End User from the drop-down list, and click Save.
   The Support Automation Access Level Detail page appears.

4. Click Edit to assign the appropriate permissions and security levels.

   - Allow Editing Privacy Level
   - Default Privacy Level
   - End-User Client Launch Mode

   The Update Support Automation Access Level page appears.

5. Click Update Privacy Levels.
   The Privacy Levels Assigned Update page appears.

6. Modify the privacy levels for the end-user access level and click OK.
   The Update Support Automation Access Level page appears.

7. Click Save.
   The end-user access level is created.

Assign an Access Level to a Role

You can assign Support Automation access levels to existing CA SDM roles in your environment.

Follow these steps:

1. Select Security and Role Management, Role Management, Role List from the Administration tab.
   The Role List page appears.

2. Click the role that you want to assign the access level, such as Administrator.
   The Role Detail page appears.

3. Click Edit.
   The Update Role page appears.

4. On the Authorization tab, select the access level that you created from the SA Access drop-down list. Click Save.
   The Role Detail page appears. Verify that the Support Automation access is assigned to the role.

Session Log Administration

This article contains the following topics:

The session log lets you view all actions that the analyst performed during an assistance session. The actions include the tools that are used and chat details, but exclude whispers. You can print or Email the session log to the end user. The end users can also view and save the log, but they cannot modify the log.

View the Session Log

All actions that you perform during the assistance session are updated in the Session Log. The actions include chat dialog, automated task results, and using a specific Support Automation Analyst Interface tool. The Whisper conversations are not included in the log.

Follow these steps:

1. Open the active session view.
   The Active Session page appears.

2. Select the Session Log from the toolbar or Sessions menu.
   The Session Log page appears.

3. Click Refresh Now.
   The page refreshes.

4. (Optional) Select the Auto-Refreshing check box.

5. (Optional) Click Save Log to Disk.
   The save dialog appears. You can save the session log locally as an HTML file.

Support Automation Activity Notification Administration

You can use activity notifications to manage Support Automation activities. You can modify how end users, analysts, and administrators can track and receive notifications when an activity occurs. For example, you can modify the notification for the end of an assistance session.

Configure any of the following default notifications, as appropriate to your environment:

- **Queue Entry Notification**
  Notifies the analyst when an end user joins an assistance session queue.
  Notifies the analyst when the assistance session is transferred to another queue.

- **Analyst Notification**
  Notifies the analyst when end-user queue wait time expires. The event of expiration is recognized with a CA SDM Event conditional macro.

- **Invite End User to Assistance Session - Incident**
  Notifies the end user when the analyst invites them to an assistance session from an incident or request.

- **Invite End User to Assistance Session - Issue**
  Notifies the end user when the analyst invites them to an assistance session from an issue.

- **Session Ended Notification**
  Notifies the system when the assistance session ends.

Note: When using Support Automation functionality with an external system such as Star, System_SA_User is set to *Session Ended Notification*.

Message Routing Servers

This article contains the following topics:

Use Message Routing Servers (MRS) to manage multiple Remote Control severs, based on the geographical location of the local server. Using MRS helps improve performance during assistance sessions. When you enable MRS, the analyst interface and end-user client connect to the analysts preferred (local) server for sharing. If the connection is unsuccessful, the sharing session falls back to the main default server. The Live Log records which MRS you use during the assistance session.

You can create, search for, update, remove, enable, or disable a message routing server object.

Note: To use this option, the *system.dataRoutingServers* system property must be enabled in the Property List.

Create a Message Routing Server

You can create a message routing server to improve the performance of remote control during assistance sessions.

Follow these steps:

1. Select Settings, Message Routing Servers from the Support Automation menu.
   The Message Routing Servers List page appears.

2. Click Create New.
   The Create New Message Routing Server page appears.

3. Complete the following fields:

   - **Active**
     Specifies that the message routing server is active.

   - **Label**
     Specifies the name of the message routing server.

   - **Socket Server Host**
     Specifies the host for the socket server.

   - **Socket Server Port**
     Specifies the port for the socket server.

   - **HTTP Connection URL**
     Specifies the URL for the HTTP connection.

   Click Save.
   The new Message Routing Server is saved.

Search for a Message Routing Server

You can search for a message routing server to improve the performance of remote control during assistance sessions.

Follow these steps:

1. Select Settings, Message Routing Servers from the Support Automation menu.
   The Message Routing Servers List page appears.

2. Click Show Filter.

3. Complete the fields and click Search.
   The search limits the list to the information of interest.

Note: Click Export to export the list results to a Microsoft Excel (.xls) file.

Enable a Message Routing Server

After you create a Message Routing Server (MRS), you can enable it. When you enable the MRS, the analyst interface and end-user agent connect to the analysts preferred (local) server for sharing.

Follow these steps:

1. Select Settings, Message Routing Servers from the Support Automation menu.
   The Message Routing Servers List page appears.

2. Click a Message Routing Server.
   The Message Routing Server Detail page appears.

3. Click Edit.
   The Update Message Routing Server page appears.

4. Select the Active check box and click Save.
   The Message Routing Server is enabled.

Customizing Live Assitance Pages

This section contains the following articles:

Create a Branding

You can modify the header and footer of end-user facing pages, such as self-serve. You can change HTML code of the header and footer and can modify the location of the CSS file.

You can view a list of branding records, one for each tenant at maximum. Tenants can create their own branding. If branding is not defined for a tenant, they use the default system settings. You can also enable localization of branding and view a list of all localized branding for enabled localizations.

Important! Branding modifications from CA Support Automation r6.0 SR1 eFix5 do not migrate to CA SDM automatically. We recommend that you review the modified branding to verify that it corresponds to the CA SDM branding. If necessary, copy and paste the Header, Footer, and CSS URL data of each division to the corresponding tenant (or public) in CA SDM. This helps in migrating the branding data.

Follow these steps:

1. Select Adaptations, Branding from the Support Automation menu.
   The Branding List page appears.

2. Click Create New.
   The Create New Branding page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant that the branding displays for.

   - **Localization**
     Specifies the localization language.

- **CSS Location**
  Specifies the location of the CSS file.

- **Header Text**
  Specifies the text that displays for the header.

- **Footer Text**
  Specifies the text that displays for the footer.

Click Save.
The new branding is created.

Localization Administration

This article includes the following topics:

Localization lets you support multiple languages simultaneously on the same install. Multiple languages are supported by translating elements of the application to a particular language. These elements can include system messages, icons, and content. Information is presented in the best form for the end user, no matter their native language.

The localized versions of Support Automation meet the needs of your global environment. Each tenant can handle multiple languages, and the localizations are supported across multiple tenants. Each tenant shares the default system settings with its localization. You can configure what language the end user and analyst use, before launching Live Assistance. The analyst can use a different language than the end user within an assistance session.

You can edit localized text for disclaimers. You cannot create or remove localizations, but you can enable or disable localizations.

Note: The administrator interface is available in the default server localization only.

Localization IDs

Localization IDs are assigned to each localization installed with the software. You are assigned the appropriate localization ID when you log in to CA SDM. All file versions are retrieved using the localization ID. This localization ID determines the following properties:

- The versions of the automated tasks to download. The version is required to get the correct view of the automated task results in the Session Log.

- The version of the chat presets used.
  You can create a translated version of the text for every chat preset, for each of the localizations. The preset tree structure is duplicated for each language that is specified on the system. A default language preset must be created before you can add a localized version. If localized text is not created, the preset tree presents the default server language text.

- The version of the log display templates to use when displaying the Session Log.

- The end-user login pages and static content that are viewed.
  The Web Client is fully localized. The administrator interface is based in the default server language. It supports management of the localization properties that are presented to the end user. The Support Automation Analyst Interface is also in English, but supports chat communications with the end user in any language. You can override all or some of the localization properties available.

Enable or Disable Localizations

You cannot create or remove localizations, you can only enable or disable localizations. The server localization is the default and cannot be disabled. When a tenant is created, the tenant shares localization settings.

Follow these steps:

1. Select Adaptations, Localization Admin from the Support Automation menu.
   The Localization Admin List page appears.

2. Click Edit in List to select a localization name from the list.
   The name is displayed with a drop-down list.

3. Select Yes or No, and click Save.
   The localization is enabled or disabled.

Configure the Page Layout

Contents

When end users log in to Live Assistance from CA SDM, they view a default launch page. Likewise, when they are initially placed on-hold in a queue, they again view a default page.

If no special settings are specified for tenants, they default public settings. You can configure the following public settings for queues that do not have their own specialized settings:

- Wait Page

- End-user Post-Launch Page

- In Session
- Post-Logout Page
- Exit Survey Page

Each page has its own detail page. The detail page comprises a text field for entering the URL and a check box for marking this page as external.

Create a Default Layout Page

The default layout pages are public and not associated with a queue. You can create modified pages to override the default for a queue or a tenant to suit your business requirements.

Follow these steps:

1. Select Adaptations, Page Layout from the Support Automation menu.
   The Page Layout List page appears.

2. Click Create New.
   The Create New Page Layout Configuration page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant that the page displays for.

   - **Page Type**
     Specifies the page type.

   - **Page URL**
     Specifies the location of the page URL.

   - **Queue**
     Specifies the queue that displays the page.

   - **External URL**
     Select to define the URL as external.

   Click Save.
   The default page is created.

Define the Default Wait Page

Initially, the Wait Page advises end users that they are on-hold for the next available analyst. You can modify the Wait Page for a queue or a tenant.

Follow these steps:

1. Select Adaptations, Page Layout from the Support Automation menu.
   The Page Layout List page appears.

2. Click the Wait link.
   The Page Layout Configuration page appears.

3. Click Edit to modify the settings.
   The Update Page Layout Configuration page appears.

4. Modify any of the following fields:

   - **Page URL**
     Specifies the location of the page URL.

   - **External URL**
     Select to define the URL as external.

   Click Save.
   The configuration is saved.

Define the End User Post-Launch Page

The End User Post-Launch Page is displayed to the end users when they log in to Live Assistance and are placed on hold in a queue. This page can be closed after the end user has logged in and the software has been successfully launched. You can modify the End User Post-Launch Page for a queue or a tenant.

Follow these steps:

1. Select Adaptations, Page Layout from the Support Automation menu.
   The Page Layout List page appears.

2. Click the End User Post-Launch link.
   The Page Layout Configuration page appears.

3. Click Edit to modify the settings.
   The Update Page Layout Configuration page appears.

4. Modify any of the following fields:

   - **Page URL**
     Specifies the location of the page URL.

   - **External URL**
     Select to define the URL as external.

   Click Save.
   The configuration is saved.

Define the In Session Page

The In Session Page is the web page that the end user sees when the support session starts. You can modify the Post-Logout Page for a queue or a tenant.

Follow these steps:

1. Select Adaptations, Page Layout from the Support Automation menu.
   The Page Layout List page appears.

2. Click In Session link.
   The Page Layout Configuration page appears.

3. Click Edit to modify the settings.
   The Update Page Layout Configuration page appears.

4. Modify any of the following fields:

   - **Page URL**
     Specifies the location of the page URL.

   - **External URL**
     Select to define the URL as external.

   Click Save.
   The configuration is saved.

Define the Post-Logout Page

The Post-Logout Page is the web page that the end user sees when the support session has concluded. You can modify the Post-Logout Page for a queue or a tenant.

Follow these steps:

1. Select Adaptations, Page Layout from the Support Automation menu.
   The Page Layout List page appears.

2. Click the Post-Logout link.
   The Page Layout Configuration page appears.

3. Click Edit to modify the settings.
   The Update Page Layout Configuration page appears.

4. Modify any of the following fields:

   - **Page URL**
     Specifies the location of the page URL.

   - **External URL**
     Select to define the URL as external.

   Click Save.
   The configuration is saved.

Define the Exit Survey Page

The Exit Survey Page presents a feedback survey to the end user at the conclusion of the session. The survey helps you measure your effectiveness and customer satisfaction. You can modify the Exit Survey Page for a queue or a tenant.

Follow these steps:

1. Select Adaptations, Page Layout from the Support Automation menu.
   The Page Layout List page appears.

2. Click Exit Survey Location.
   The Page Layout Configuration page appears.

3. Click Edit to modify the settings.
   The Update Page Layout Configuration page appears.

4. Modify the configuration and click Save.
   The configuration is saved.

Note: By default, the Exit Survey Page is not displayed at the end of a Live Assistance session. The administrator must define the Exit Survey Page for it to display.

Create a Disclaimer

When end users launch self-service tasks, they are presented disclaimer text that they must agree to before they can continue. You can create, update, and delete the disclaimer business objects.

Follow these steps:

1. Select Tools, Disclaimers from the Support Automation menu.
   The Disclaimer List page appears.

2. Click Create New.
   The Create New Disclaimer page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **Disclaimer Name**
     Specifies the name of automated tasks classification.

   - **Disclaimer Text**
     Specifies the text that displays for the disclaimer.

   Click Save.
   The disclaimer is created.

4. (Optional) Click a localization link.
   The Localized Disclaimer Detail page appears.

5. Click Edit.
   The Update Disclaimer page appears.

6. Enter the localized text for the disclaimer and click Save.
   The localized text for the disclaimer is added.

Automated Tasks

Contents

An *automated task* is a collection of steps that define an automated process that the analyst or end user follows. The automated task steps are routines that are written in VBScript or JavaScript. The routines execute specific actions on the analyst or the end-user computer. You can create automated tasks and task steps using the Automated Task Editor. Some of the common routines include gathering telemetry information, diagnosing problems, and implementing resolutions.

When you execute an automated task, the log updates. This log is both linked and accessed from the assistance session log. Entries in the automated task log consist of a number of timestamped text entries. The entries are created by calling Functions.LogMessage() or WScript.Echo().

How to Configure Automated Tasks

You install and configure the Automated Tasks Editor to manage automated tasks that analysts use to provide support for end users. The end user can launch an automated task from a knowledge document and the self-service interface. An analyst can execute an automated task during an assistance session. The automated tasks provide analysts with detailed information about an end-user computer. You create self-service automated tasks that interact with the end user and process their input. These tasks can change the file system, registry, download install software, and so on. You configure automated tasks as follows:

1. Install the Automated Tasks Editor.
   You launch the installer from the following location on the installation media:

   ```
   casd.nt\SAScriptWriter
   ```

   Note: You can also copy the installer and deploy it to the appropriate users in your support environment.

   The Automated Task Editor is installed.

2. Open the Automated Tasks Editor.
   The Automated Tasks Editor installation creates a shortcut on your desktop.

3. Set the following connection parameters:

    a. Click **Tools, Server**.
    The **Server Configuration** dialog appears.

    b. Enter your hostname and port.
    Default Port: 8070

    c. Enter the user name and password of a user with read/write access to the Automated Task Editor. For example, enter the details of a Support Automation Analyst.

    d. Click **Test**.

    e. Click **OK**.

4. Create automated tasks and upload them to your server.
    You can upload public tasks or can assign them to specific tenants and subtenants.

    Important! Only the roles from the Service Provider tenant with the Update Public flag enabled can upload tasks and libraries to the server. All task library content and static content are stored as public data.

How to Implement Automated Tasks

You can use automated tasks to assist end users in your support environment. The automated tasks complete specific actions on the end-user computer, without the analyst or end user having to complete the process. These scripts can help you gather telemetry information, diagnose computer problems, and implement resolutions.

To implement automated tasks, do the following tasks:

1. Identify the opportunities for support automation.
    Identify common problems that end users encounter, and decide that you can automate some solutions to reduce your support costs.

2. Research automation of the potential solutions.
    Research resolutions to common problems and gather data about diagnostic processes you plan to use.

3. Design tasks to automate end-user support.
    Design the end-user experience that you want for each task with the Automated Task Editor.

4. Implement and test the automated tasks.
    Test the automated tasks to verify that they resolve common problems that are encountered in your support environment.

5. Deploy and monitor the automated tasks.
    Deploy the automated tasks to end users in your environment by allowing analysts to use them in assistance sessions. You can attach scripts to knowledge documents that end users can download and use.

Note: In a multi-tenancy environment, enable the Update Public option for analysts that belong to the Service Provider tenant. This setting lets analysts upload task and library content.

Note: CA Technologies can provide training in creating automated tasks and components. The training can include creating automated task step templates and libraries, which you can use in your environment. For more information about developing automated tasks, contact *CA Technologies Services*.

Automated Tasks Administration

You can create automated tasks and can associate them with the server. You need read/write access to all the automated task-related tables to use the Automated Tasks Editor. You can perform user management functions with the application, such as assigning automated tasks to roles and tenants.

Note: Service Provider analysts who have access to multiple tenants can select the tenant context of any task update operation against the server. Service Provider analysts can also assign an automated task as public.

Create an Automated Tasks Classification

You can classify the automated tasks that are displayed to differentiate between the types of automated tasks.

Follow these steps:

1. Select Tools, Automated Tasks, Automated Tasks Classification from the Support Automation menu.
   The Automated Tasks Classification List page appears.

2. Click Create New.
   The Create New Automated Tasks Classification page appears.

3. Complete the fields and click Save.
   The automated tasks classification is added to the list.

Update the Automated Tasks List

You can view the automated tasks that are available for use. You can configure the script to run for Live Assistance or Self-Service. You can also configure the script for the end-users even if they do not have system access rights.

Follow these steps:

1. Select Tools, Automated Tasks, Automated Tasks List from the Support Automation menu.
   The Automated Tasks List page appears.

2. Click an automated task.
   The Automated Task Detail page appears.

3. Complete the following fields:

   - **Classification**
     Specifies the classification or group the automated task belongs to.

   - **Description**
     Displays a description of the automated task.

   - **Disclaimer**
     Specifies the disclaimer that must be agreed to before the script can run.

4. (Optional) Click the Update Permissions button on the Configure script for the Live Assistance tab and select the permissions. Use the arrow buttons to move them from column to column and click OK.

5. (Optional) Select the Impersonate field and complete the Login name, Password, and Domain information about the Impersonation tab.

6. (Optional) On the Support Automation Access Level tab, click Update Tasks to add an access level. Click Edit in List to select the automated script for Auto Run and save.
   The automated task is added to the list.

Specify Default Credentials

Run automated tasks on the end-user computer even if the end user does not have access rights to perform such activities. If the end user does not have administrative rights to view system information, run a restricted automated task. Use the default credentials to gain access.

Follow these steps:

1. Select Tools, Default Credentials from the Support Automation menu.
   The Default Credentials List page appears.

2. Click Create New.
   The Create New Default Credentials page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **Label**
     Specifies the name that displays.

- **Domain**
  Specifies the domain.

- **Login**
  Specifies the login name.

- **Password**
  Specifies the password.

- **Confirm Password**
  Specifies the password was typed correctly.

- **Active**
  Specifies the default credentials is active.

Click Save.
Default credentials are saved.

Configure an Automated Task Script

You can view the automated tasks that are available for use. You can configure the script to run for Live Assistance, Self-Service, or on the end-users computer even if they do not have system access rights.

Follow these steps:

1. Select Tools, Automated Tasks, Automated Tasks List from the Support Automation menu.

   The Automated Tasks List page appears.

2. Click an automated task.

   The Automated Task Detail page appears.

3. Click the Update Permissions button on the Configure script for Live Assistance tab.

   The Permissions Assigned Update page appears.

4. Depending on the requirement, perform any of the following actions:

   - Select the permissions and use the arrow buttons to move them from column to column. Click OK.

   - Select the Impersonate field and complete the Login name, Password, and Domain information on the Impersonation tab.

   - Click Support Automation Access Level tab. Click Update Tasks to add an access level. Click Edit in List to select the automated script for Auto Run.

5. Click Save.

   The automated task is configured for Live Assistance.

Automated Task Deployment

This article contains the following topics:

After you author and test an automated task in the Automated Task Editor, you can deploy it to a classification on the CA SDM server. The task can then be used in assistance sessions or self-service. Some settings that are not part of the automated task definition are set when you deploy the task.

You can upload or download automated tasks directly to the server from the Automated Task Editor. You select the appropriate tenant when creating automated task classifications. If you upload scripts, select the classification or tenant for which you have access. Or, you can even set the script as public. You can also import automated tasks from XSDF files and export them to XSDF files.

Note: In a multi-tenancy environment, enable the Update Public option for analysts that belong to the Service Provider tenant. This setting lets analysts upload task and library content.

Upload an Automated Task

You can upload automated tasks that you created in the application. When you select a task, all dependent content automatically uploads, such as libraries and static content.

Follow these steps:

1. Open the Automated Task Editor.
   The Support Automation Task Editor appears.

2. Select the automated task that you want to upload.

3. Select the classification where you want to upload the task.

   Note: A user with right privileges in a multi-tenancy environment can select the appropriate tenant when the automated task is uploaded. Or, can make the task public.

4. On the toolbar, select the Upload Automated Task icon.

The Support Automation Task Editor uploads the task to the server.

Edit an Automated Task

You can download automated tasks from the server and can edit them in the Automated Task Editor. Any content that is newer in the version than the existing content on the server is imported into the database. The content is then made available to administrators of that tenant.

To edit an automated task:

1. Open the Automated Task Editor.
   The Support Automation Task Editor appears.

2. On the toolbar, select the Upload Automated Task icon.
   The Open Automated Task from Server pane appears.

3. Select the automated task that you want to download.

   Note: If you are a privileged user in a multi-tenancy environment, you can edit public or tenant-specific automated tasks.

4. Click Open Task.

The Support Automation Task Editor downloads the task to the client and opens it in the application. The download creates a text file on the computer of the task author that contains the dependent content.

Automated Task Credentials

You can execute an automated task that you need administrative privileges to run, such as performing a software installation. Use the following process to execute such a task:

- Define Default Credentials for the tenant and configure the automated task to use the default credentials in automated task administration.
- Define Default Credentials for the tenant and select that you use the Execute As dialog in the Assistance Session window.
- Define automated task credentials for the task and specify to use the Execute as dialog in the Assistance Session window.
- Specify the credentials in the Execute As dialog in the Assistance Session window.

Role Assignment

You assign the appropriate roles (for example, Analyst, Administrator) to use the automated task. You assign individual automated tasks to selected roles to limit the automated tasks to only those analysts in the assigned role. You can manage the different skill sets or levels of experience within the support organization.

You can manage the roles at a task level, selecting certain commonly executed tasks. The tasks include diagnostics that run automatically when the end user enters a session.

Assign an Access Level to a Role

You can assign Support Automation access levels to existing CA SDM roles in your environment.

Follow these steps:

1. Select Security and Role Management, Role Management, Role List from the Administration tab.
   The Role List page appears.

2. Click the role that you want to assign the access level, such as Administrator.
   The Role Detail page appears.

3. Click Edit.
   The Update Role page appears.

4. On the Authorization tab, select the access level that you created from the SA Access drop-down list. Click Save.
   The Role Detail page appears. Verify that the Support Automation access is assigned to the role.

Support Automation Reports

CA Business Intelligence installs a set of predefined Support Automation reports. CA SDM automatically deploys these reports to the BusinessObjects server during the installation.

The Support Automation Administrator and Support Automation Analyst roles can use Business Intelligence Launch Pad to view detailed and summary information about the following metrics:

- Analyst login metrics
- Assistance Sessions metrics
- Queue entries metrics
- Automated task execution metrics
- Tool usage per ticket category
- Real-time data about end users that are placed in support queues, active assistance sessions, and active (logged-in) analysts.

Employee or Customer Interface

This section contains the following articles:

Search for Existing Solutions

The Home page allows you to search for solutions using keywords. This section allows you to search for a solution using keywords and submit new solutions to the database.

Follow these steps:

1. Type your keyword(s) in the Search for a Solution section and click Go.

2. Click the document that addresses your issue.

3. Choose from the following options:
   Add/Remove Bookmark
   Stores a link to the document in My Bookmarks.
   Subscribe
   Allows you to receive updates if the document is modified.
   Rate & Comment
   Allows you to rate the usefulness of the document, based on the following questions:

   - Did this forum solve your problem?

   - How helpful was this forum?

   Email

   Allows you to email the document.

   New Incident

   Creates a new incident.

   New Incident based on this Document

   Creates a new incident based on the current document.

View Contact Information and Hours of Operation

You can view information about site hours of operation and how to contact your sites. Your administrator provides the content of this page so that you can see the hours of operation of each service desk site in your organization and details about how to contact the appropriate personnel at each site.

Follow these steps:

1. Browse to the Customer Service/Request Support section of your home page.

2. Click Service Desk contact information and hours of operation.

The Contact Information and Hours of Operation page appears.

Automating Support in Your Environment

This article includes the following topics:

You can implement a support strategy using a combination of processes and tools. CA SDM provides the tools to administer live assistance and develop automated tasks. The application also lets you deliver the tools through various channels.

Use the associated processes to create and maintain an environment that provides the following benefits:

- Reduced average support call duration
- Reduced overall support costs
- Increased resolution rates
- Improved end-user satisfaction

Live Assistance

Live Assistance provides end-user support through tools that enhance remote interaction between analysts and end users. You can use automated, predefined responses to communicate with the end user. You gather detailed information about an end-user computer and act to provide support.

You provide live assistance using the following interfaces:

- **Support Automation Analyst Interface**
  Lets the analysts interact with end users and provide support during assistance sessions.
- **End-User Client**
  Lets the end-user chat with the analyst, while the analyst provides support to their computer.

Support Automation Analyst Interface

You can provide Live Assistance to end users by using the Support Automation Analyst Interface. You monitor queues, manage multiple end-user assistance sessions, and interact with end users to resolve their computer problems.

You access Live Assistance from a ticket page, such as an incident, issue or request, or the Support Automation tab. You can also open a CA SDM ticket from Live Assistance.

Important! Analysts without read access to their tenant cannot launch the Support Automation analyst client. A warning message appears in CA SDM, such as from the main Support Automation tab or a ticket.

Use the following tools to provide live assistance to end users in your support environment:

- **Chat**
  Launches instant message to the end user or to use preset text and URLs. If the end user uses the web client, only chat is enabled in a browser. You can request to use the full Support Automation tools by selecting Sessions, Launch Full Tools.

- **Automated Tasks**
  Runs predefined diagnostic or repair scripts on the end-user computer.
  Note: Scripts are created and uploaded from the Automated Task Editor IDE and your administrator configures permissions.

- **File Explorer**
  Browses the files on the end-user computer and lets end users create, modify, rename, or delete files and directories.

- **File Transfer**
  Copies and transfers files and folders to the end-user computer. You can also copy and transfer files from the end-user computer.

- **Remote Registry**
  Performs the following registry management operations:

  - Create, edit, or delete registry records.

  - Export or import registry values from the end-user registry.

- **Screenshot**
  Captures the screenshots of the end-user computer when connection quality is not sufficient for remote control assistance.

- **Remote Control**
  Controls the end-user computer remotely.

- **Remote System Tools**
  Restarts or shuts down the end-user computer.

- **Run Program**
  Launches a program on the end-user computer without using the Remote Control tool.

- **Impersonate**
  Impersonates authentication credentials on the end-user computer, such as a privileged user. Impersonation credentials are configured in System Wide Credentials, Default Credentials.

Note: Your system administrator or tenant administrator can configure access levels, role permissions, and can disable any Live Assistance tools.

Support Automation Analyst Administration

Support Automation analysts monitor and manage multiple end-user requests in live assistance sessions in your environment. Analysts use Support Automation tools to interact with end users and provide live assistance.

Analysts access the interface from a CA SDM ticket, such as an incident, or the Support Automation tab. You can manage access levels to set permissions for tools that the analysts can use. You can enable and disable Support Automation tools for specific tenants. If a tool is disabled for a tenant, analysts cannot use that tool in assistance sessions.

Important! The Support Automation Analyst Interface only runs on Windows. For more information about supported operating systems, see the *Release Notes*.

Support Automation Connectivity

The analyst and end user never communicate directly with each other. You do not require a direct peer-to-peer connectivity between the two users. Data transfer is routed through the server, verifying that you can communicate even when the end-user computers are behind firewalls.

You can connect to end-user computers using the following connections:

- **Socket**
  Using a socket connection is the best way for you to connect. The socket connections are the fastest and the most efficient, with the least overhead, and minimal latency.

- **HTTP (or HTTPS)**
  Using an HTTP connection is better than a direct socket connection, because corporate firewalls can block direct socket connections. The HTTP connections generate a significant amount of network traffic overhead, when compared to direct socket connections. The number of simultaneous sessions is lower when the connections to the server are over HTTP. This happens due to the overhead and processing on the server,

- **Proxy**
  Socket Proxy is a mode of operation for the Support Automation server to off-load some of the CPU-intensive operations. For example, encryption or decryption from the main server, and a server component that can go into the DMZ within the logical network topology.

Typically, you attempt to connect through the direct socket connection first. If the direct socket connection fails, then connect through HTTP. However, you can specify custom connection settings on the client computer to alter this sequence. For more information about configuring communication settings, see the Online Help.

End-User Client

The end-user client connects end users to analysts in live assistance sessions. End users chat with analysts in WebChat. When you use the tools in the Support Automation Analyst Interface, the client is launched on the end-user computer. When the client launches, instructions appear for the end user specific to their web browser.

Server Load

In large deployments, high server load can degrade the application performance. For this reason, you can off-load some of the processing to one or more Socket Proxy servers as follows:

- Offload encryption and decryption of the incoming and outgoing data for all analysts or clients. The clients must connect either through Direct Socket or through HTTP.
- Offload the processing of HTTP traffic from and to those clients connecting through HTTP to the Socket Proxy.

DMZ Server Component

In some network environments, allowing direct socket access to the application servers that run Support Automation can be considered a security risk. In such environments, you can use Socket Proxy within the DMZ. Using Socket Proxy in this scenario offloads some of the processing from the main server.

How Socket Proxy Works

The Socket Proxy works as follows:

1. On the configured external port, the Socket Proxy listens for incoming connections from analysts or end users.
2. The Socket Proxy establishes a peer connection to the main server on the configured internal port, for every connection. These two connections are named the end-user connection and the server connection, respectively.
3. The end-user connections are encrypted and the Socket Proxy encrypts or decrypts data coming in or going out. The server connection is not encrypted.
4. For each incoming data-packet, the protocol structure is verified and a checksum value is validated. This happens before the data is passed on to the main server through the server connection.
5. The main server off-loads the encryption and decryption processing.
6. The Socket Proxy closes the matching peer connection once the end user or server connection closes.

How Live Assistance Works

This article includes the following topics:

How Analysts Launch Live Assistance

As an Analyst, you can launch Live Assistance as follows:

1. Perform *one* of the following tasks:
   - Log in to CA SDM and selects the Support Automation tab.
   - Open a CA SDM ticket and selects the Support Automation tab.
2. if it is not already installed, install the 32-bit Java Runtime Environment (JRE) version 1.6 or later. The Support Automation Analyst Interface does not support the 64-bit JRE.

Note: The Safari browser requires the 32-bit JRE 1.6.0_30 or later. The sa_login_session table creates a record every time an analyst launches the Support Automation Analyst Interface and when an end user launches the Web Client. For more information about the sa_login_session table, see the *sa_login_session Table* topic.

Configure Java Connection Options

Configure Java connection options to resolve an issue where Support Automation Analyst Interface cannot connect to the Support Automation server. The issue occurs when the browser of the analyst is not configured for your environment and the browser fails to launch Live Assistance. You can edit the analyst connection settings from a browser or the Java Control Panel.

Follow these steps:

1. Open your web browser, such as Internet Explorer.
   The browser appears.
2. Click Tools, Internet Options.
   The Internet Options dialog appears.
3. Configure the appropriate connection settings, such as a direct connection or proxy server.

4. Click OK.
   The connection opens are configured.

To configure connection options in the Java Control Panel

1. Open the Java Control Panel with the following command:

   ```
   javaws -viewer
   ```

   The Java Control Panel appears.

2. On the General tab, click Network Settings.
   The Network Settings dialog appears.

3. Configure the appropriate settings, such as a direct connection or proxy server.
   Click OK.
   The connection opens are configured.

How End Users Join Assistance Sessions

An end user requests assistance sessions from the CA SDM home page or by contacting the help desk. The Support Automation analyst invites the end user to a session from the CA SDM ticket.

1. As an end user, do one of the following tasks:

   - Request Live Chat from the CA SDM Home Page.
     The Live Chat Launch page appears asking you for the incident area and description. Click Continue, the session opens, and you are placed in the appropriate queue.

   - Click a link from an email notification and log in to the assistance session. Use the credentials and a session join code that the analyst has provided.
     If you join from the email notification, you bypass the queue.

   - Click Join Analyst Now and provide the session join code to bypass the queue.

     Note: When the Support Automation end-user client is launched, an executable is downloaded to launch the program. The end user starts it manually, however for security reasons there is a limited time to launch the executable. After the time expires, an error message appears on the end-user computer when they try to start the launcher executable.

2. The analyst provides live assistance through chat. You use the web browser to chat with the analyst, or launch the agent executable.

Note: If the analyst cannot resolve the session using WebChat, they can invite the end user from the Analyst Session window. The analyst can use the full tools available in the Support Automation Analyst Interface.

How Analysts Automate Support for End Users

As an Analyst, you use Live Assistance tools to perform the following tasks on end-user computers:

- Host live chat sessions.
- View file systems.
  - Create, modify, rename, or delete files and directories.
  - Copy and transfer files and folders to the end-user computer.
- View system registries
  - Create, edit, or delete registry records.
  - Export or import registry values from the end-user registry.
- Capture end-user screenshots when connection quality is not sufficient for Remote Control assistance.
- View the end-user computer desktop.
- Remotely control the end-user computer.
- Launch a program on the end-user computer.
- Restart or shut down the end-user computer.
- Run automated tasks.

How Analysts Provide Live Assistance

Analysts provide Live Assistance to end users by using the Support Automation Analyst Interface. Analysts handle end users that are routed to their queues, manage assistance sessions, and join sessions for which they have permission.

1. The end-user requests assistance from the CA SDM home page, or a ticket, such as an incident, a request, or an issue.
2. The end user joins a queue. If the end user joins the session using the link from the analyst email invitation, they bypass the queue.
   You configure CA SDM request areas and issue categories for queue routing.
3. The analyst selects the end user from the queue.
4. The assistance session begins and the analyst provides live assistance.

> **Note:** If the analyst launches the Support Automation Analyst Interface from the Support Automation tab, no CA SDM ticket is associated with the assistance session.

5. The analyst creates the ticket when closing the assistance session. The analyst defines the status or transfers the assistance session to another queue. The status can be as *SA-Open* or *SA-Resolved.*

6. The analyst closes the session and the end user receives an email notification with the Session Log.

How to Provide Live Assistance to End Users

This article contains the following topics:

The Support Automation Analyst Interface lets you provide live support to end users in your environment. Click the tab that corresponds to the tool you want to use.

Initiate a Chat with the End User

You can chat with the end user during a live assistance session. The chat displays inside the Support Automation Analyst Interface. The end users can see the chat in WebChat or in the end-user client executable.

To chat with the end user

1. Open an assistance session.
   The assistance session appears.

2. Do any of the following tasks:

   - Enter text in the chat window.

- Whisper a message to the end user.
  This message is private and not seen by the other analyst that is logged in to the assistance session.

- Push a specific URL to the end user.
  The end user can open the link, or you can open their browser, depending on the administrative settings.

- Send a preset response to commonly asked questions and common situations.
  Presets can consist of text messages or commonly pushed URLs.

The message appears in the chat window.

Support Automation Chat

The analyst, administrator, or tenant administrator creates chat presets that you can use in assistance sessions, such as greetings. You can chat with the end user during a live assistance session. While you use live assistance concurrently with telephone conversations, the chat tool lets you communicate using text messages.

The chat displays directly inside both the end user and Support Automation Analyst Interface windows. The chat notifies you when any of the following events occur:

- When someone joins your session
- When someone initiates a new chat
- When someone leaves a session that is still in progress with other participants
- When someone ends a session

You can also use the following chat functionality:

- **Whisper Messages**
  Sends private messages to selected members. Analysts that you invited to your assistance session cannot see these messages.
  Note: Whisper messages do not appear in the Session Log. You can only use whisper messages when more than one analyst handles the session.

- **Push URL**
  Directs the end user to a specific URL. The administrator sets whether the URL opens automatically or if the end user must open the URL manually.

- **Chat Presets**
  Sends preconfigured text messages to commonly asked questions and common situations. Presets can consist of text messages or commonly pushed URLs. Chat presets display in the Preset Tree area of the Chat Tool view.
  Chat presets include greetings and typical answers that can be populated automatically with information specific to the current assistance session. An example of a preset is the name of the participant.

Execute an Automated Task

You can execute predefined automated tasks that run on end-user computer. The automated tasks let you gather telemetry information, diagnose common problems, and implement resolutions. The administrator sets your automated task permissions.

To execute an automated task

1. Select Automated Tasks.
   The Automated Tasks page appears.

2. Select an automated task from the left pane.
   The script details appear, such as the name and description.

3. Click Execute.
   The automated task runs on the end-user computer.
   The Executed Tasks pane updates.

4. (Optional) Right-click the task in the Executed Tasks pane and click View Result.
   The results of the automated task execution appear.

Note: You can enable autorun and execute an automated task when the tool launches.

Browse the End-User File System

You can browse the end-user file system in a live assistance session. Use the File Browser to transfer from the end-user computer to your computer. The File Transfer tool can transfer files in both directions (see page 2901).

To browse a file system

1. Select File Explorer.
   The File Explorer page appears.

2. Browse the file system of the end user in the assistance session.

3. Use the context menu and select Download to transfer files.
   The File Transfer page appears.

Transfer Files with the End User

You can transfer files with the end-user computer. You can locate the appropriate file using the file explorer.

To transfer files

1. Select File Transfer.
   The File Transfer page appears.

2. Select the appropriate transfer option, such as Local to Remote.
   Locate the Source File.
   The Source File field populates.

3. Select the appropriate destination folder, such as Desktop.

4. Click Add to Transfer Queue.
   The Transfer Queue updates with the file transfer status.

Modify the End-User Registry

You can modify the registry of the end-user computer.

To modify the registry

1. Select Remote Registry.
   The Remote Registry Tool appears.

2. Navigate through the end-user registry and modify the appropriate registry entries.
   The registry is modified.

Capture a Screenshot

You can capture a screenshot of the end-user desktop when the connection quality is poor for remote control.

To capture a screenshot

1. Click the Screenshot tab.
   The Screenshot page appears.

2. Click Get Screenshot.
   The screenshot file transfers to your computer and displays in the right pane.
   The screenshot pane stores your capture history.

3. Click the picture to view it in original size.

4. (Optional) Save the picture as an external file.

5. Complete the assistance session.
   You can handle another end user from the queue.

Impersonate the End User

You can impersonate CA SDM login credentials during an assistance session. By default, you perform actions on the end-user computer with the end-user rights. You can also impersonate user rights with more privileges, such as an administrator.

Use impersonation when attempting to use tools that require higher privileges. For example, when modifying the end-user registry, or executing an automated task.

To impersonate the end user

1. Click Session, Impersonate.
   The Impersonation dialog appears.

2. Select an available impersonation login or use other credentials.

3. Click Impersonate.
   You impersonate the end-user rights.

Control the End-User Computer Remotely

You can take full control of the end-user computer, to perform diagnostic and repair functions remotely. You can see and manipulate everything on the end-user computer, as if you were physically sitting at the end-user desk.

Note: Your administrator establishes security levels for end users.

To control the end-user computer

1. Select Remote Control.
   The Remote Control page appears.

2. Wait for the end user to click Accept.
   The end user accepts your request for control.

Note: Remote Control uses Message Routing Servers to locate the best connection. If the connection quality is poor, you can use screenshots and can chat to diagnose the end-user computer. Connection quality symbols appear on the interface. For example, an excellent connection appears as green, yellow as fair, and red as poor.

3. (Optional) You can modify the behavior of remote control. Open the session as full screen, set the scrolling option and switch between the viewing and full control mode.

4. Control the computer and provide live assistance.
   The assistance session completes.

5. Disconnect from the computer.
   The Session Log updates to contain a record of which Remote Control server was used during the session.

Run a Program on the End-User Computer

You can run a program on the end-user computer without using Remote Control.

To run a program

1. Select Remote System Tools.
   The Remote System Tools page appears.

2. Enter a command to run on the end-user computer.
   The command executes and the program runs.

3. Click Run Program.
   The Run Program dialog appears.

Restart or Shutdown the End-User Computer

You can restart, restart and reconnect, or shut down the end-user computer.

To restart or shut down a computer

1. Select Remote System Tools.
   The Remote System Tools appear.

2. Select the appropriate action from the drop-down list, such as Restart and Reconnect.

3. Click Proceed.

4. The end user is prompted with your selection and confirms your selected action.
   The action performs and the end-user computer restarts or shuts down.

View the Session Log

All actions that you perform during the assistance session update the Session Log. The actions include chat dialog (excluding Whisper conversations), automated task results, and using a specific Support Automation Analyst Interface tool.

Follow these steps:

1. Open the active session view.
   The Active Session page appears.

2. Select the Session Log from the toolbar or Sessions menu.
   The Session Log page appears.

3. Click Refresh Now.
   The page refreshes.

4. (Optional) Select the Auto-Refreshing check box.

5. (Optional) Click Save Log to Disk.
   The save dialog appears. You can save the session log locally as an HTML file.

Configuring Support Automation Tools

This section contains the following articles:

Automated Tasks Administration

This article contains the following topics:

You can manage automated tasks as follows:

- View the automated tasks that are available for use.
- Update the automated task list to select from.
- Add, modify, or delete automated tasks classifications.

Create an Automated Tasks Classification

You can classify the automated tasks that are displayed to differentiate between the types of automated tasks.

Follow these steps:

1. Select Tools, Automated Tasks, Automated Tasks Classification from the Support Automation menu.
   The Automated Tasks Classification List page appears.
2. Click Create New.
   The Create New Automated Tasks Classification page appears.
3. Complete the following fields:
   - **Tenant**
     Specifies the tenant.
   - **Automated Task Classification Name**
     Specifies the name of automated tasks classification.

   Click Save.
   The automated tasks classification is added to the list.

Search for an Automated Tasks Classification

You can search for the automated tasks classifications that are displayed to differentiate between the types of automated tasks.

Follow these steps:

1. Select Tools, Automated Tasks, Automated Tasks Classification from the Support Automation menu.
   The Automated Tasks Classification List page appears.

2. Click Show Filter.
   Complete the fields and click Search.

3. The search limits the list to the information of interest.

Note: Click Export to export the list results to a Microsoft Excel (.xls) file.

Search for an Automated Task

You can search for the automated tasks that are available for use. You can configure the script to run for Live Assistance or Self-Service. You can also configure the script for the end-users even if they do not have system access rights.

Follow these steps:

1. Select Tools, Automated Tasks, Automated Tasks List from the Support Automation menu.
   The Automated Tasks List page appears.

2. Click Show Filter.
   Complete the fields and click Search.

3. The search limits the list to the information of interest.

Note: Click Export to export the list results to a Microsoft Excel (.xls) file.

Update the Automated Tasks List

You can view the automated tasks that are available for use. You can configure the script to run for Live Assistance or Self-Service. You can also configure the script for the end-users even if they do not have system access rights.

Follow these steps:

1. Select Tools, Automated Tasks, Automated Tasks List from the Support Automation menu.
   The Automated Tasks List page appears.

2. Click an automated task.
   The Automated Task Detail page appears.

3. Complete the following fields:

   - **Classification**
     Specifies the classification or group the automated task belongs to.

   - **Description**
     Displays a description of the automated task.

   - **Disclaimer**
     Specifies the disclaimer that must be agreed to before the script can run.

   (Optional) Click the Configure script for Live Assistance tab (see page 2907).
   (Optional) Click the Impersonation tab (see page 2907).
   (Optional) Click the Support Automation Access Level tab. (see page 2908)
   Click Save.
   The automated task is added to the list.

Configure an Automated Task Script for Live Assistance

You can view the automated tasks that are available for use. You can configure the script to run for Live Assistance or Self-Service. You can also configure the script for the end-users even if they do not have system access rights.

Follow these steps:

1. Select Tools, Automated Tasks, Automated Tasks List from the Support Automation menu.
   The Automated Tasks List page appears.

2. Click an automated task.
   The Automated Task Detail page appears.

3. Click the Update Permissions button on the Configure script for the Live Assistance tab.
   The Permissions Assigned Update page appears.

4. Select the permissions and use the arrow buttons to move them from column to column. Click OK.
   The Permission Assigned Update page closes.

5. Click Save.
   The automated task is configured for Live Assistance.

Configure an Automated Task Script for Impersonation

You can view the automated tasks that are available for use. You can configure the script to run for Live Assistance or Self-Service. You can also configure the script for the end-users even if they do not have system access rights.

Follow these steps:

1. Select Tools, Automated Tasks, Automated Tasks List from the Support Automation menu.
   The Automated Tasks List page appears.

2. Click an automated task.
   The Automated Task Detail page appears.

3. Select the Impersonate field and complete the Login name, Password, and Domain information about the Impersonation tab.
   Click Save.
   The automated task is configured for impersonation.

Configure an Automated Task Script for Access

You can view the automated tasks that are available for use. You can configure the script to run for Live Assistance or Self-Service. You can also configure the script for the end-users even if they do not have system access rights.

Follow these steps:

1. Select Tools, Automated Tasks, Automated Tasks List from the Support Automation menu.
   The Automated Tasks List page appears.

2. Click an automated task.
   The Automated Task Detail page appears.

3. Click Support Automation Access Level tab.
   Click Update Tasks to add an access level.
   Click Edit in List to select the automated script for Auto Run.
   Click Save(Y).

4. Click Save.
   The automated task is configured for access.

Chat Preset Administration

This article contains the following topics:

You can create common responses to commonly asked questions and situations. Instead of repeatedly typing the same information, you can save a response and can use it in other chat sessions.

You can send the presets to end users at the beginning of each session automatically, such as a greeting. You can also automatically populate the presets with information specific to the current session, such as the analyst name.

You can use the following types of presets in an assistance session:

- **Chat Preset**
  Identifies a commonly used text response to an end-user question.

- **URL Preset**
  Identifies a commonly used URL that the end user can access.

You can localize each chat preset. The chat preset is synchronized with the end-user localization so that the end user receives correct localized presets.

Create a Chat Preset Group

You can manage chat presets responses into categories (groups).

Follow these steps:

1. Select Tools, Chat Presets, Chat Preset Group List from the Support Automation menu.
   The Chat Preset Group List page appears.

2. Click Create New.
   The Create New Chat Preset Group page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **Group Name**
     Specifies the Chat Preset Group name.

   Click Save.
   The chat preset group is created.

4. (Optional) Click Edit in List to modify the Chat Preset Group Localizations.
   The Localized Chat Preset Group List page appears.

Search for a Chat Preset Group

You can search for a chat preset group.

Follow these steps:

1. Select Tools, Chat Presets, Chat Preset Group List from the Support Automation menu.
   The Chat Preset Group List page appears.

2. Click Show Filter.

3. Complete the fields and click Search.
   The search limits the list to the information of interest.

Note: Click Export to export the list results to a Microsoft Excel (.xls) file.

Create a Text Preset

You can create a chat preset for commonly used text responses to end-user questions. When you save a response, you can use it in other chat sessions.

Follow these steps:

1. Select Tools, Chat Presets, Text Preset List from the Support Automation menu.
   The Chat Text Presets List page appears.

2. Click Create New.
   The Create New Chat Text Preset page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **Default Chat Preset for Session Join**
     Select to define as the default Chat Preset for Session Join.

   - **Text Preset Group**
     Specifies the text preset group.

   - **Text Preset Name**
     Specifies the text preset name.

   - **Preset Text**
     Specifies the text of the preset.

   Click Save.
   The text chat preset is created.

4. (Optional) Click Edit to modify the Localized Chat Text Preset List.
   The Update Chat Text Preset page appears.

5. Click a localization link.
   The Chat Text Preset Localization Detail page appears.

6. Click Edit.
   The Update Chat Text Preset Localization page appears.

7. Enter the localized name and text and click Save.
   The localized text for the text chat preset is added.

Search for a Text Preset

You can search for a chat preset for a commonly used text response to an end-user question. When you save a response, you can use it in other chat sessions.

Follow these steps:

1. Select Tools, Chat Presets, Text Preset List from the Support Automation menu.
   The Chat Text Presets List page appears.

2. Click Show Filter.

3. Complete the fields and click Search.
   The search limits the list to the information of interest.

Note: Click Export to export the list results to a Microsoft Excel (.xls) file.

Create a URL Preset

You can create a URL preset for a commonly used URL that the end user can access. When you save a URL, you can use it in other chat sessions.

Follow these steps:

1. Select Tools, Chat Presets, URL Preset List from the Support Automation menu.
   The Chat URL Preset List page appears.

2. Click Create New.
   The Create New Chat URL Preset page appears.

3. Complete the following fields:

   - **Tenant**
     Specifies the tenant.

   - **URL Preset Group**
     Specifies the URL preset group.

   - **URL Preset Name**
     Specifies the URL preset name.

   - **Preset URL**
     Specifies the URL of the preset.

   - **URL Title**
     Title for the URL Preset.

   Click Save.
   The URL chat preset is created.

4. (Optional) Click Edit to modify the Localized URL Chat Preset List.
   The Update Chat URL Preset appears.

5. Click a localization link.
   The Chat URL Preset Localization Detail page appears.

6. Click Edit.
   The Update Chat URL Preset Localization page appears.

7. Enter the localized URL information and click Save.
   The localized URL preset is added.

Search for a URL Preset

You can search for a URL preset for a commonly used URL that the end user can access. When you save a URL, you can use it in other chat sessions.

Follow these steps:

1. Select Tools, Chat Presets, URL Preset List from the Support Automation menu.
   The Chat URL Preset List page appears.

2. Click Show Filter.

3. Complete the fields and click Search.
   The search limits the list to the information of interest.

Note: Click Export to export the list results to a Microsoft Excel (.xls) file.

Default Credential Administration

This article includes the following topics:

Run automated tasks on the end-user computer even if the end user does not have access rights to perform such activities. If the end user does not have administrative rights to view system information, run a restricted automated task. Use the default credentials to gain access.

Specify Default Credentials

Run automated tasks on the end-user computer even if the end user does not have access rights to perform such activities. If the end user does not have administrative rights to view system information, run a restricted automated task. Use the default credentials to gain access.

Follow these steps:

1. Select Tools, Default Credentials from the Support Automation menu.
   The Default Credentials List page appears.

2. Click Create New.
   The Create New Default Credentials page appears.

3. Complete the following fields:

- **Tenant**
  Specifies the tenant.
- **Label**
  Specifies the name that displays.
- **Domain**
  Specifies the domain.
- **Login**
  Specifies the login name.
- **Password**
  Specifies the password.
- **Confirm Password**
  Specifies the password was typed correctly.
- **Active**
  Specifies the default credentials is active.

Click Save.
Default credentials are saved.

Search for a Default Credential

You can search for default credentials. Use the default credentials to run an automated task on the end-user computer to view system information. You can also use the credentials to gain access to the end-user computer.

Follow these steps:

1. Select Tools, Default Credentials from the Support Automation menu.
   The Default Credentials List page appears.
2. Click Show Filter.
3. Complete the fields and click Search.
   The search limits the list to the information of interest.

Note: Click Export to export the list results to a Microsoft Excel (.xls) file.

Service Catalog Management

CA Service Catalog provides system forms for users to complete as part of their requests. A service consists of hardware, software, or other resources that users request from the catalog. Administrators can manage services to meet the needs of their users and organization. You can use events, rules, and actions to automate the processing of requests, users, and accounts in the CA

Service Catalog system. All rules are initially disabled. A rule must be enabled to be used. You can add a dashboard, configure content elements, manage outages, create business hours, news, content packs as shown in the following:

Manage Forms

CA Service Catalog provides the following system forms for users to complete as part of their requests:

- General Information Form
- Request Information Form

These forms request user-related information that is typically required to complete a request. For example, basic personal data and shipping address.

General Information Form

The General Information form asks the user to provide the required details for completing any checkout process. This form is not modifiable and therefore does not appear in the Form Designer. This form appears on the checkout page and other pages of the request.

Request Information Form

By default, the Request Information form asks the user to provide any custom descriptive information about the request. This form appears in any checkout process for services. The default version of the form appears in the Forms, System folder in the Form Designer.

You can optionally customize the Request Information form. Click the Customize button in the Component Tree when the form is selected. After confirming that you want to customize the form, you can edit it.

Use caution when modifying this form: Changes apply to all checkout-process for services in your business unit and all sub-business units. Even past (fulfilled requests, no archiving), present, and future are affected.

A tenant can have *one* active custom copy of this form.

Search the Forms

You can search for a specific form using either the Form Display name or Folder name option. You can use the Search Form UI option to modify or view an existing form. The search mechanism provides auto suggestion as the user types search terms in the form search text box. Search terms are case insensitive. The search results are displayed in a hierarchical manner.

Note: This capability is available only if you have installed the CA Service Catalog 14.1.01 patch updates available on CA Support.

Delete the Forms

After you customize this form, you can optionally delete the customized version to revert to the parent form.

The Delete function is disabled for the Service Provider (SP) business unit, because deleting the parent form is prohibited.

Hide the Forms

You can hide the Request Information form. Doing so ensure that the form does not appear to users or administrators during the request life cycle. By default, the request information form appears.

To hide it, open Catalog, Configuration, Request Management Configuration, and change the setting *Access Control: Show Request Information* to include no roles. Hence, no users or administrators can view or edit the Request Information form during request processing.

Restrictions

Keep in mind the following restrictions:

- Copying and pasting the Request Information form creates a copy that does *not* become the system form.
- You cannot move the Request Information form out of the Forms, System folder.
- You cannot alter the Forms, System folder, other than customizing the forms that can be edited.

Pre-Defined JavaScript Functions for System Forms

Customize the pre-defined JavaScript functions to update fields in the request information form when the general information form is changed. This optional customization helps integrate the request information form with the checkout and request edit pages. The pre-defined JavaScript functions are as follows:

- **custom_onPriorityChange(newPriority)**
  This function is invoked when the priority of the request is changed in the general information form. You can add code to update the customized request information form to reflect the priority change. By default, this function does nothing.
  newPriority is a string that corresponds to the new priority.

- **custom_onDateRequiredChange(newDateRequired)**
  This function is invoked when the date required is changed in the general information form. You can add code to this function to update the request information form. By default, this function does nothing.
  newDateRequired is a JavaScript date object set to the new required date.

- **custom_onRequestedForChange(type, id, name, shippingAddress)**
  This function is invoked when the requested for user or account for a request is changed. You can add code here to update values in your request information form. Example: Changing the shipping address fields in the request information form to have the address of the requested for user or account.
  By default, this function updates the shipping address of the request information form with the shipping address of the new user or account.

  Important! If you change the shipping address section of the request information form, update this code to reflect those changes.

type is the user when a user is selected and account when an account is selected.

id is the CA Service Catalog ID of the selected user or account.

name is the display name of the selection.

shippingAddress is a JavaScript map with the following keys: address_1, address_2, city, state, zip code, and country. If the user or account has no address, shippingAddress can be null or empty.

Elements of a Form

You can drag and drop the form element to Form Preview section. For each form element, the _id value is auto generated. This value is a combination of text and numbers and depends upon the element you are creating. The first element of the form always begins with 1. For example, in a form the _id for the first text field element is txtf_1 and the _id for the first text area element is txta_1. In the same form, the _id for the second text field element is txtf_2 and the _id for the second text area element is txta_2.

You can modify this auto generated _id value of the form elements, if required.

Important! We recommend that you do not specify the same _id value for the different form elements in the same form. Having multiple form elements with the same _id value can cause validation errors.

To reuse the elements that you have customized, copy and paste the elements from one form to another.

The Form Designer provides the following elements for you to create and modify forms:

Check Box

Enables the user to select or decline a single option.
You can optionally use multiple check boxes to group related choices, of which users can select two or more. For example, you can add one check box each for the peripheral devices that are associated with a laptop computer. These devices include a mouse, docking station, carrying case, and external backup drive.

Column Layout

Enables the user to organize the components on the form for maximum efficiency. The column layout includes two vertical columns, Column 1 and Column 2, aligned next to each other. You can place form components in one or both of these columns. You cannot insert one column inside another, and you are not allowed to add more than two columns per Column Layout place holder. However, you can place multiple column layouts in a form.

Date

Sets the format of the date and time. The date and time that appear on the Form Designer match the date and time of the browser that you are using to access CA Service Catalog. The date and time that appear to other users accessing the form match the date and time of their browsers. The date and time of form settings -- even on the same forms -- can differ between users in different time zones. This principle applies whether users access the form through the Form Designer or while requesting a service.

- **Date**
  Use the date portion of this field whenever date information is required. **Example:** Start Date, Date Required, Estimated Date of Arrival. Users can select a date from the calendar.
  By default, the date format for the Date Time field matches the date format of the current business unit.

  Note: As an administrator, you can optionally change the default format for the business unit to a different format: Edit the profile of the business unit on the Administration, Business Units page and select a new date format. Examples include M/d/yyyy, d-M-yyyy, or yyyy/M/d.

  Specify date formats in Date Time fields on your forms according to the following rules:

Letter	Meaning	Format	Example
y	year	Number	2009
M	month in a year	Text or Number	July or 07
d	day in a month	Number	10

  CA Service Catalog supports the date format attributes supplied with the Google Web Toolkit (GWT) 1.6. For more information about these attributes, see the Google website, www.google.com (http://www.google.com).

- **Time**
  Use the time portion of the Date Time field whenever time information is required. **Example:** Start Time, End Time, and Estimated Time of Arrival. When you use the time portion of this field, a drop-down list of time values appears next to the calendar. Users can select a time from this list. **Default:** The time format for the Date Time field matches the time format of the business unit of the user.

  Note: As an administrator, you can optionally change the default format for the business unit to a different format: Edit the profile of the business unit on the Administration, Business Units page and select a new time format.

  Specify time formats in Date Time fields on your forms according to the following rules:

Format	Separator
HH:mm	colon
HH.mm	period

  If the Hide Time attribute is set to *true*, then the time portion of the field is hidden. This time format is ignored. The drop-down list for selecting the time does not appear on the form. Otherwise, the field accepts valid values that are separated by a space. CA Service Catalog

supports the time format attributes supplied with the Google Web Toolkit (GWT) 1.6. For more information about these attributes, see the Google web site, www.google.com. (http://www.google.com.) You can add literal values that are enclosed in quotation marks (such as "hours" or "minutes") before or after the hour and minute values.

The HTML attributes (see page 2928) named *hidetime* and *increment* control whether and how incremented time values appear in each Date Time field.

Dual List

Displays two columns in a box: The left column lists available options, and the right column lists the selected options.
A toolbar of arrows appears between the columns. For example, to select an option, highlight it in the left column. Then, you click the arrow to move the option to the right column.
Users can highlight multiple options in one column and click the arrow to move them as a group to the other column. Users can click the double arrows to move all options from one column to another. This action selects or deselects *all* options.
While you are designing the form, you can perform the same actions as the user to select and clear options.
By default, the dual list field contains *no* available options. To populate the dual list with available options, use *one* of the following methods:

- Specify a report data object (see page 3232) for the dual list: Enter the HTML attributes (see page 2928) named Report/Plug-in Id and Report/Plug-in Variables.
- Create a static list of individual options for the dual list: Add options to the dual list. You can add, move, and delete options to the dual list. The default dual list element in the Component Tree includes one option. You can copy and modify this option to create more options.

To enable users to specify the order of the selected options, specify *true* for the HTML attribute named ordered. When you do so, the toolbar is updated to include up and down arrows. Users can highlight selected options and click these arrows to move the options up or down in the list. When you are designing the form, you can order the selected options in the right column. The available options in the left column always appear in the order that you arrange them on the Component Tree.

Field set

Enables the user to group multiple elements as a set. Examples include the following groups:

- Accessories for a laptop such as battery charger, carrying case, and docking station.
- Telephone numbers for a user such as home, work, cell, and fax.

Elements in a field set have a box around them to show that they are related. For maximum accessibility, do *not* place one of the following elements immediately after a field set: check box, Date Time field, radio group, and radio buttons.

Image

Enables the user to provide a picture representing an item that can be included in an associated service or service option. The image that you specify must reside in the filestore, the central location for CA Service Catalog files. Use the following format:

FileStore/*path*/*filename.ext*

Important! The folder name *FileStore* is case-sensitive. Use the correct case in path names and all other references.

Label

Identifies a form or an area of the form. **Example:** A title in a form, such as Medical History Form. Within the form, you can have other labels, such as Family History, Eating Habits, and Illnesses. If you use a multiple-column format in your form, it can be helpful to use a label as a heading for each column.

Use the HTML attribute (see page 2928) that is named Label Text to configure the label that users see on the form. You can optionally perform the following tasks for labels:

- Use the HTML attribute (see page 2928) that is named Hidden to hide the label when the conditions you specify are met.
- Use the JavaScript attribute (see page 2940) named onClick to run a JavaScript function (see page 2967) when the user clicks the label.

Lookup Field

Works with the JavaScript function ca_fdDoFieldLookup(fieldId, reportId) to populate fields based on user input to a report data object (see page 2970).
You configure the lookup field to prompt the user to enter the data for the query of the data object. **Example:** user ID, asset ID, or city. The data object queries the data source, which is based on the user input. The results are used to populate the fields you specify.
The user clicks the search icon for the lookup field and enters the requested data. The query runs and returns the search results in rows. Each matching value appears in a row. Users review the rows and select one. When the user selects a row, the results from that row populate the matching fields on the form.
For example, the lookup field can prompt the user to enter a user ID. The query then searches the database for the first name and last name of the user ID. The user can select one row to populate the corresponding First Name and Last Name fields on the form.

Radio Group

Presents a list of options to the user. A radio group contains radio buttons *only*. A radio group cannot contain any other element. The user must select only one. **Example:** A radio group that is named Size with three buttons: one each for Small, Medium, and Large. In contrast to options in select boxes (see page), radio group buttons *always* appear on the form. To save space, you can use a radio group only for fields having four or fewer options.

Select

Presents a list of options, of which the user select either one (the default) or multiple options.
A select box contains select options *only*. A select box cannot contain any other element. **Example:** You can create a select box that is named Width with two options: Narrow and Standard.
The options for select boxes appear on the form only when the user clicks the drop-down list box.

Therefore, you can use a select box rather than an option group to save space on a form. Doing so is especially relevant when the number of options is four or more.
Optionally change the default setting of a select box to enable users to select more than one option. To do so, change the Multi-Select attribute of the select box from False (the default) to True. If you change this setting to True, the select box changes from a drop-down list to a sequential list or list box. Hence, all the options are always displayed and more screen space is required. The user sees multiple lines in the select box and can select multiple options.
When this attribute is set to false, the select box appears as a combo box on the form: The user sees a list box and can select only one item from the list. The Catalog users cannot enter a *custom* value in a select box. However, users can type inside a select box. As they type, the drop-down list is populated with the options that begin with the typed text. Users can then select an option from this "auto-complete" list.
To set specifications for the auto-complete list, use the Minimum Search Characters attribute. For more information, see HTML attributes for select boxes only (see page 2934).

Slider

Enables the user *slide* a control forwards or backwards to increase or decrease the selected value. Each slide updates the selected value according to the increment that you set. Specify the unit of measure for the slider in a message that appears each time that the user increases or decreases the selected value. Sample messages include *0 CPUs, 1 CPU, 2 CPUs, and 3 CPUs*.

To configure the contents and behavior of the slider, use the following attributes:

- Attributes for most or all elements (see page 2929)
- Attributes for sliders only (see page 2935)

Spinner Field

Enables a user to select a numerical value from a range of incremented values. **Example:** 100, 200, 300, and 400. The user clicks the up or down arrows to increase or decrement the selected value. Use the HTML attributes for spinner fields only (see page 2928) to configure the contents and behavior of the spinner field.

Table

Enables the user to create tables. You can create either a Static Table or a Dynamic Table.

Static Table

A static table is a type of container, like a field set, that can contain certain elements of a form. You can use the columns in the table to organize the data from each type of element. In contrast to a dynamic table, a static table consists of fixed data that you specify manually.

You can create a static table to enter structured data into a form.

Follow these steps:

1. Edit or create the form in which you want to add the table. Expand the form.
2. Add the table element to the form:

a. (Optional) Create a field set to contain the table.

b. Expand the System folder, drag the Table element, and drop it on the form. If applicable, drop the table onto the field set that you created in the previous step.

c. Specify an _id value for the table and save the form.

3. Add an element to the table:

a. Expand the table and display the Row field.

b. Drag one of the following elements (see page 2916) from the System folder and drop it on the Row field:

- Date Time field
- Label
- Select field whose Multi-Select attribute is set to false. This setting allows only a *single* selection.
- Spinner
- Text

The name of the element that you drag-and-drop becomes the name of the first column. For example, if you drag-and-drop a Date element, the name of the first column becomes Date.
Similarly, the data that you enter in the column must match its element. For example, in a Date column, you can enter only dates.

c. Specify an _id value for the column and save the form.
After you save the form, you can optionally rename the element that you dragged and dropped. If you rename the element, the name of the column changes accordingly. For example, if you rename the element to Start Date, the name of the column also changes to Start Date.

d. Configure each element that you add to a table. The steps are the same as adding the element to the form without a table.
For date fields, the value returned must be a long or appropriately formatted string. For label columns, the value is converted to a string. For spinner columns, the value must be an integer or double. For text columns, the value is converted to a string.

4. To add rows to the table, perform the following steps:

a. Select the Row field on the Table element on the System folder.

b. Drag-and-drop it on the Table element on the form.

c. Repeat these steps until you have added all the rows that you want. You cannot move, copy, cut, or paste rows.

5. Define the values for each row in the table, as follows:

a. In the first row, specify the static values of each cell, using their value attribute.

b. In the remaining rows, specify values using the column attribute.
The Form Designer does *not* validate any data or the data format that you enter in the table rows. When users display the form in a request, the Catalog system validates the data and displays it *only* if you use the correct format. Thus, any invalid values that you specify do *not* appear when users view the form in a request. **Example:** If you specify a string value for a date column, the corresponding table cell appears empty to the user.

c. Perform this step if applicable; otherwise, skip it.
If you are using a Select field (see page) whose Multi-Select attribute is set to false, then the Select field does *not* contain the value attribute. In that case, perform the following actions:

- For the first row: Enter the value of the Selected Index attribute of the Select field. For example, to specify the first option, enter 0. To specify the second option, specify 1, and so on.
- For the remaining rows: Copy the value of the *value* attribute from the select option of the Select field. Paste this value into the column attribute of the row.

6. Specify any of the following attributes:
   - HTML attributes (see page 2928)
   - Attributes for tables only (see page 2937)
   - JavaScript functions for tables only

Dynamic Table

A dynamic table is also a type of container that can contain certain elements of a form. You can use the columns in the table to organize the data from each type of element.

You can create a dynamic table to enter structured data from a report data object into a form.

Follow these steps:

1. Create or edit the report data object or API plug-in that you plan to use to populate the dynamic table.
   The variables in the report data object or API plug-in must return data in the format that the table columns require. Otherwise, users do not see this data when they open the form in a request.
2. Edit or create the form in which you want to add the table. Expand the form.
3. Add the Table element to the form, as follows:
   a. (Optional) Create a field set to contain the table.
   b. Expand the System folder, drag the Table element, and drop it on the form. If applicable, drop the table onto the field set.

c. Specify an _id value for the table and save the form.

4. Add the report data object or API plug-in to the table, as follows:

   a. Select the Table element.

   b. If you are using an API plug-in, specify the values of the following attributes:

      Report/Plug-in Id: Enter the ID of the API plug-in that you want to use. You can find values for these attributes on the Administration, Tools, Plug-ins page. Report/Plug-in Variables: Open the API plug-in that you selected to display its details, including variables. On the details page, the Inputs section lists the ID values and descriptions of the input variables for the plug-in.

   c. If you are using a report data object, specify the values of the following attributes:

      - Report/Plug-in Id: Enter the ID of the report data object that you want to use. You can find values for these attributes on the Administration, Report Builder, Data Objects page.

      - Report/Plug-in Variables: Click the Edit icon for the report data object that you selected to display its properties, including variables. On the properties page, the input variables for the report data object appear as follows:
        For a Query: The input variables appear as *%expression%* statements.
        For Plug-in: The input variables appear in the Arguments field.
        For CSV: The input variables do not apply.

      For both attributes, enter variables as a JSON expression, for example:

```
$({'<variable name>' : '<variable value>', ...})
$({'userid':_.user.id,'rm_orgunit':ca_fdGetSelectedOptionValues(ca_fd.f
```

> **Important!** Specify the variables carefully. If you specify *no* variables, unpredictable results can occur.

5. Save the form.
   When users complete this form, the report data object or API plug-in runs and returns the data that you specified.

Next, you configure the dynamic table (see page 2924).

Configure the Dynamic Table

After you create a dynamic table, you configure it to contain the data and use the format that you require.

Follow these steps:

1. Review the following requirements for adding elements to the table. Each element that you add becomes a column in the table.

- Add one element for each variable that you specified in the Report/Plug-in Variables attribute of the table element.
- (API plug-ins) The value of the _id attribute of each element (column) in the table must match a value of an Output Id of the plug-in.
- (Report data objects) The value of the _id attribute of each element (column) in the table must match a value of a Field of the data object.

2. Add an element to the table, according to the requirements in the previous step, as follows:

   a. Expand the table to display the Row field.

   b. Drag the element from the System folder and drop it on the Row field. You can drag-and-drop the following elements:

      - Date Time field
      - Label
      - Spinner
      - Text
      - Select the field whose Multi-Select attribute is set to False. This setting allows only a *single* selection.

   c. Perform this step if applicable; otherwise, skip it.
   If you are using a Select field (see page) whose Multi-Select attribute is set to false, then the Select field does *not* contain the value attribute. In that case, you can populate the Select field using *either* a static list *or* a report data object.
   To populate the Select field *using a static list,* perform the following actions:

      - For the first row: Enter the value of the Selected Index attribute of the Select field. For example, to specify the first option, enter 0. To specify the second option, specify 1, and so on.
      - For the remaining rows: Copy the value of the *value* attribute from the select option of the Select field. Paste this value into the column attribute of the row.

   The name of the element that you drag-and-drop becomes the name of the first column. For example, if you drag-and-drop a Date element, the name of the first column becomes Date.
   You cannot move, copy, cut, or paste rows.

   d. Specify an _id value for the column and save the form.

   Important! The _id value for the column must meet the requirements noted in the previous step. Also, the data type and data format must also be the same. Otherwise, the column is not populated with data.

Example: You are using an API plug-in, and you want a table column to specify the start date of an event. You drag-and-drop a Date Time element onto the table and specify an _id value of start_date. This element becomes a column in the table. Therefore, the Output Id of a variable of the API plug-in must also be start_date. The sequence does not matter. This variable must also return the required date and time data in the format that matches the Date Time element.

3. Configure each element that you add to a table. The procedure is the same as if you were adding the element to the form without a table.
   Each one is a basic element (see page), except the Date Time field (see page) and the Select field (see page). The data that you enter in the column must match its element. For example, in a Date column, you can enter only dates.

4. (Optional) Specify a custom value for pagination for the table, as follows:

   a. Specify the value of the Page Size attribute of the Table element.

   b. For API plug-ins, configure sorting and pagination parameters. For report data objects, further action is necessary.

5. (API plug-ins only) Enable users to sort the results in the table, as follows:

   a. Specify a value of True for the Sortable attribute of the Table element.

   b. Configure sorting and pagination parameters. Sorting does not apply to report data objects.

6. Specify any of the following attributes:

   - HTML attributes (see page 2928)
   - Attributes for tables only (see page 2937)
   - JavaScript functions for tables only

Text Area

Enables the user to enter more than one line of input. **Example:** A free-form description of the offering.

Text Field

Enables the user to enter free-form text. **Example:** Fields for the user to enter a name, address, telephone number, or multiple-digit numeric entries. Use text fields when only one line of input is required.

Page Layout

Enables the user to place the form components within a page layout for maximum efficiency. You cannot place one page layout inside another and you can have only one page layout in a form.

You can have any number of pages within a page layout.

Page layout element can be one of the following:

- Card layout - Displays the element as pages with next and back button if there are multiple pages. This is the default page layout.
- Tab layout - Displays the element as tabs on top of the page layout.

Default page height: 400 pixels

Form Attributes

Form attributes apply to the *entire* form rather than to one field only.

- **name**
  Specifies the name of the form.
  Specify this attribute for each form, and verify that this attribute is unique for each form.
- **_id**
  Specifies the identifier of the form.
- **class**
  Specifies the CSS class name to use for the form.
  Define the new CSS class in the formdesigner.css file in the folder named USM_HOME\view\webapps\usm\gwt\fdBase\css.
  For example, to apply a class that changes the form to a 12-point, blue, boldface font, Follow these steps:

  1. Back up the formdesigner.css file before you edit it.
  2. Append the following class statement to formdesigner.css, as follows:

```
/* custom class by author-name, date for purpose */
.blue12-class {
color: blue;
font-size:12px;  /* Make sure to mention font size in pixels(px) */
font-weight:bold;
}
```

  > **Note:** Text fields have a preset height limit and therefore ignore the font-size attribute.

  3. Enter blue12-class as the value for CSS class attribute.
  4. Verify your updates by using the form in a request.

- **Form Type**
  Specifies whether the form is a configuration form type, as follows:
  - Request - for a request of a service from the catalog

- Configuration - for a content configuration form (see page 3070)

Default: Request
This attribute *cannot* be written using JavaScript expression.

- **Label Align**
  Applies to labels *only*. This attribute specifies the alignment of the label in relation to the fields on the form. Select top, right, or left (default).

- **Label Width**
  Specifies the width in pixels of the field labels in the form.
  You can also specify Label Width as an HTML attribute (see page 2928) for the column layouts and field sets on the form.

- **onLoad**
  Specifies the JavaScript function to run when the user opens the form in a request.
  Multiple forms having an onLoad attribute can appear on a single page. In that case, each JavaScript function (see page 2966) runs when the user opens the form that includes the function.
  An alert appears if an onLoad function fails to run correctly. For example, if the function cannot be found.

  If you receive an alert, verify that function is correctly defined and referenced to ensure that it runs without errors.

  Note: Use the Script dialog on each form to create and maintain the custom JavaScript functions for the form.

- **onSubmit**
  Specifies the JavaScript function to run when the user submits the request that contains the form. This function must return a Boolean value. If the function returns any value except *true*, the form is not submitted.
  Multiple forms having an onSubmit attribute can appear on a single page. In that case, each JavaScript function runs when the user submits the form that includes the function.
  The information about alerts for the onLoad function also applies to the onSubmit function.

HTML Attributes for Elements

You can use HTML attributes to configure the appearance and behavior of the elements of a form. For more information on how to use the JavaScript Functions, see JavaScript Function APIs (see page 2928).

Keep in mind the following principles:

- Not all HTML attributes apply to all elements (fields). Click an element to see which attributes apply to it.

- Required HTML attributes appear in **bold** in the Item Inspector. When you add an element to a form, complete the required attributes and save the form immediately after adding the element. Afterwards, you can add optional HTML attributes and JavaScript attributes.

- The HTML attributes are primarily internal, in that they regulate the appearance and behavior of the form. They *typically* do not supply literal text that appears to the administrator in the Design Area or to the user in a request.
- You view and modify the names and values of the HTML attributes in the Item Inspector as needed. However, you generally do not see the changes as literal text in the Design Area. The exceptions are:
  - The Checked attribute for radio buttons and check boxes
  - The Value attribute for labels, text fields, and text areas
- For an HTML attribute, you can optionally enter a JavaScript expression, but you cannot call a JavaScript function.
- For most elements, you specify the literal text that appears to end users by adding and configuring elements (see page 2951) on the form. Specifically, you rename the elements on the form in the Component Tree, and you verify their appearance in the Preview Area.

For more information about the different HTML Attributes, see the following sections.

- Attributes for Most or All Elements (see page 2929)
- Attributes for Date Time Field Only (see page 2932)
- Attributes for Dual List and Select Boxes Only (see page 2932)
- Attributes for Field Sets Only (see page 2932)
- Attributes for Labels Only (see page 2933)
- Attributes for Radio Groups Only (see page 2933)
- Attributes for Select Boxes and Tables Only (see page 2933)
- Attributes for Select Boxes Only (see page 2934)
- Attributes for Sliders Only (see page 2935)
- Attributes for Spinner Fields Only (see page 2936)
- Attributes for Tables Only (see page 2937)
- Attributes for Text Fields and Text Areas Only (see page 2940)

Attributes for Most or All Elements

Some HTML attributes apply to *all or most* elements (fields) of a form. The following attributes of that group may require explanation:

- **_id**
  Specifies an auto-generated unique identifier for the form field.
  If the _id is not unique, a warning message appears.

  Important! The Form Designer *warns* you if the _id attribute values are duplicated for multiple fields; however, it does *not* prevent you from saving them. Therefore, change any duplicate _id attributes a soon as you become aware of them. If the form contains duplicate _id attributes, JavaScript functions can run on the wrong form field and cause errors. If you change the value of the _id attribute, verify that you also change any references to it, especially in JavaScript functions.

- **CSS Class**
  Specifies a space-separated list of CSS classes. This class is associated with style information.

- **Empty Text**
  Provides extra description of a field to the user.
  The value that you specify for this attribute appears inside the field when the user opens the form. This text disappears when the user begins entering a value in the field. A sample value follows, for a password field: You can optionally use the Empty Text, Hint, and Tool Tip attributes together to assist the user.

- **Name**
  Specifies the name of the element.

- **Value**
  Specifies the value of the input component. This attribute is often useful for entering sample data or instructions. For example, for the value attribute of a text field named Address, you can specify something like "123 my street" or “Enter your address here.” In both examples, the value suggests that users replace the default text with their actual addresses.

- **Disabled**
  Specifies a value of true or false.

- **Hidden**
  Specifies whether to hide a field, including the label. Specify true or false. When the value is set to true, the field is *not* visible.
  You can use JavaScript expressions to specify this value as a condition, as follows: If the condition is met, hide the field. Otherwise, display the field.
  For example, you can hide a fulfillment-related field before the request reaches the Pending Fulfillment status. Similarly, you can hide a salary-related field from any user other than the manager of the user and the Human Resources user group.
  You can specify all the same conditions (see page) that apply for the Policies. Similarly, you can use the JavaScript expressions to specify the value as a condition for the **Include in Email Notification** attribute too.

- **Include In Email Notification**

  Specifies whether to display a field or component value, including the label. Specify the value as true or false. When the value is set to true, the field or component value is visible in the email. To set or edit this attribute, you must have admin rights. Navigate to **Catalog**, **Forms**, select the Form Component and click on the **Include in Email Notification** attribute.

  When you set the **Hidden** and **Include In Email Notification** element attributes to true/false in the CA Service Catalog UI, the following is reflected in UI and email notifications:

Hidden Attribute	Include In Email Notification Attribute	Result
true	true	Form component is not displayed anywhere.
true	false	Form component is not displayed anywhere.
false	true	Form component and value is displayed in the Form Designer, the Request Form while raising a request, and in the email notification.

Hidden Attribute	Include In Email Notification Attribute	Result
false	false	Form component appears in the Request Form UI, the Form Designer UI, but the component value is not displayed in Email Notifications.

- **Hide Label**
  Specifies whether to hide *only* the name of a field. The field remains visible regardless of whether you name the label. This attribute provides flexibility when space is a concern.
  Specify true or false. When the value is set to true, the name for this field is *not* visible.
  You can use JavaScript expressions to specify this value as a condition, as follows: If the condition is met, hide the name. Otherwise, display the name. You can specify all the conditions (see page) that apply for the Policies.
  For example, you can hide the names of obvious fields, such as Name, Address, and Telephone Number, after the user submits the request. Doing so can be helpful to save space on the form when the additional fields become visible for approval and fulfillment statuses only.

  Note: The Hide Label attribute does *not* apply to the Label element. Instead, the Hide Label attribute applies to the *name* of certain other fields that you enter in the Component Tree of the Form Designer. After you enter the name of a field in the Component Tree, the name appears in the Preview Pane.

- **Hint**
  Specifies help text for a field. This text *always* appears below the field, regardless of the position of the mouse.
  For example, for a password field, you can specify the following hint: "Passwords must be six to eight characters and must include both letters and numbers."
  You can optionally use the Empty Text, Hint, and Too tip attributes together to assist the user.

- **Required**
  Specifies whether this field is required. Enter a value of true or false.
  When a user submits the form, the system verifies that all the required fields are not empty. A required field is a field whose required attribute is set to true. If any required fields are empty, the system prompts the user to complete them.

- **Style**
  Specifies associated style information.

- **Tab Index**
  Specifies the position in the tabbing order. Enter numeric value only.

- **Tool Tip**
  Specifies helpful text appears *only* when the user hovers the mouse over the field.
  You can optionally use the Empty Text, Hint, and Tool Tip attributes together to assist the user.

- **Text Direction**
  Specifies the supported values for left-to-right and right-to-left for the direction of the text.

Attributes for Date Time Field Only

The following HTML attributes apply to the Date Time field (see page) *only*.

- **Hide Time**
  Applies *only* to the time portion of the Date Time field; this field is an optional element of a form (see page 2916).
  Specifies whether to display the drop-down list for users to select the time. Specify *true* to hide this list or *false* to display it.

- **Time Increment**
  Applies *only* to the time portion of the Date Time field; this field is an optional element of a form (see page 2916).
  Specifies the increment (in minutes) of the times that appear in the drop-down list for users to select the time. Specify any positive integer greater than zero.
  For example, if you specify 15, the following values appear in the list: 9:00, 9:15, 9:30, 9:45, 10:00, and so forth. Similarly, if you specify 30, the following values appear in this list: 9:00, 9:30, 10:00, 10:30, 11:00, and so forth.

Attributes for Dual List and Select Boxes Only

The following HTML attributes apply to dual lists (see page 2919) and select boxes (see page) only.

Additional attributes (see page 2934) apply to select boxes only.

- **Height**
  (Dual List) Controls the height of the dual list. Using this attribute displays the entire list of options *without* a scroll bar.
  (Select Box) Controls the maximum height of the drop-down list that appears when the user clicks the arrow to display the options.
  For select boxes that allow users to select multiple options, using this attribute displays the entire list of options *without* a scroll bar.

See also:

- attributes for select boxes only (see page 2934)

Attributes for Field Sets Only

The following HTML attributes apply to field sets *only*. Fields sets are basic elements of a form (see page).

- **Collapsed**
  Applies *only* to the field set element.
  Specifies whether the label of the field set is initially collapsed (true) or expanded (false).

- **Label Width**
  Specifies the width in pixels of the column layout and field set.
  You can also specify Label Width as a form attribute (see page 2927).

Attributes for Labels Only

The following HTML attributes apply to labels *only*. Labels are basic elements of a form (see page)
.

- **Label Text**
  Specifies the text for a label.
  A label identifies a form or an area of the form. For example, you can use a label at the top of the form to provide the title, such as Medical History Form. Within the form, you may have other labels, such as Family History, Eating Habits, and Illnesses. If you use a multiple-column format in your form, it may be helpful to use a label as a heading for each column.
  The Label Text attribute of a label contains the text that users see on the form, for example, as a title or heading. This Label Text attribute can contain HTML tags, which are especially helpful for highlighting purposes. For example, to specify the Family History label in bold, enter the following data in the Label Text field:

  ```
  <b>Family History Form</b>
  ```

Attributes for Radio Groups Only

The following HTML attributes apply to radio groups *only*. Radio groups are basic elements of a form (see page).

- **Orientation**
  Lets the user control the orientation of the options for the group.
  Specify horizontal or vertical (default).

Attributes for Select Boxes and Tables Only

The following HTML attributes apply only to select boxes (see page) and tables (as noted).

- **Report/Plug-in Id**
  Specifies the ID of the report data object (data object). This data object is used to pre-populate a combo box (see page 2972) or to pre-populate rows in a dynamic table (see page 2923).
  The data object returns two fields:

  - The first field returns the list of values in the combo box. Users can select one or more of these values, depending on the setting of the multiple attribute.
  - The second field returns the label for the combo box.

  The data object represents a stand-alone MDB query that does not require a JavaScript function to run.

- **Report/Plug-in Variables**
  Specifies the attribute to use user input to pre-populate a select box (see page 2973) or to pre-populate rows in a dynamic table (see page 2923).
  For example, you can specify this attribute to use the selection in one select box to determine the values in a second select box.

- **Page Size**
  Specifies the number of options that appear on one page in a drop-down list. The drop-down list appears when a catalog user performs one of the following actions:

  - Clicks the arrow of a drop-down list
  - Types text in a field and activates the auto-complete feature

  The Page size attribute applies *only* to the following elements:

  - Select boxes whose Multi-Select attribute is set to False.
  - Static table (see page 2921)
  - Dynamic table (see page 2923)

  The Page size attribute is optional and accepts *only* positive integers.
  This attribute is useful when report object returns too many options to list on a single page. In such cases, the drop-down list contains a scroll bar and page numbers. To view the values in the list, users can either scroll or click a page number.
  A blank (empty) value effectively disables pagination.
  The default is 50.

See also:

- attributes for select boxes only (see page 2934)
- attributes for tables only (see page 2937)

Attributes for Select Boxes Only

The following HTML attributes apply to select boxes only.

- **Eager**
  Applies *only* when both of the following settings are used:

  - The value of the Multi-Select attribute of the select box is False.
  - The Report/Plug-in Id attribute is set.

  Specifies a value of true or false.

  - **True**
    Loads the data from the Report/Plug-in Id attribute into the select box as soon as the user requesting the service displays the form.
  - **False**
    Loads the data from the Report/Plug-in Id attribute into the select box when the user requesting the service clicks the select box.

- **List Width**
  Specifies the minimum width of the drop-down list for a select field.
  The Form Designer uses the *larger* of the following values:
  - The width of the select field
  - The value of the List Width attribute
- **Multi-Select**
  Specifies a value of true or false.
  - **True**
    Specifies that the select box appears as a list box on the form. The user sees multiple options in the select box and can select multiple options.
  - **False**
    Specifies that the select box appears as a combo box on the form. The user can select one item from the list. The user cannot enter a custom value for this attribute.
- **Minimum Search Characters**
  Applies *only* when the value of the Multi-Select attribute of the select box is False. When this value is False, the select box appears as a combo box on the form: The user sees a list box and can select only one item from the list. Catalog users cannot enter a *custom* value in a select box. However, users can type inside a select box. As they type, the drop-down list is populated with the options that begin with the typed text. Users can select an option from this "auto-complete" list.
  The auto-complete list starts to populate after the user types the *n*th character, where *n* is the value you set for Minimum Search Characters attribute. For example, if you specify a value of 7, the auto complete options appear after the user types the seventh character.
- **Selected Index**
  Specifies the default selection.
  For example, the select box contains 10 values. If you specify 0 for the Selected Index attribute, the first value in the list becomes the default. Similarly, if you specify 5 for the Selected Index attribute, the fourth value in the list becomes the default.
  You can use a select box in a static table.

See also:

- attributes for select boxes and tables only (see page 2933)
- attributes for dual list and select boxes only (see page 2932)

Attributes for Sliders Only

The following HTML attributes apply to sliders only.

- **Increment**
  Specifies the increment by which the selected value increases or decreases with each forward or backward slide, for example, 1, 5, 10, 25, or 100.

- **Value**
  Specifies the initial value of the slider, for example, 10.

- **Maximum Value**
  Specifies the maximum value of the slider, for example, 100.

- **Minimum Value**
  Specifies the minimum value of the slider, for example, 1.

- **Message**
  Specifies the message that appears as the user slides the control. Use the following format:

  - **{0}** ***text***
    {0}displays the selected value. As the user slides the control, this value is automatically replaced with the selected value.
    text specifies the unit of measure, for example, CPU, RAM, or another meaningful unit.

For best results, specify values for these parameters and test the slider until you obtain the results that you want.

Note: You can optionally use JavaScript functions to set the values of these attributes. For details about predefined JavaScript functions, including slider-specific functions, select Administration, Tools, Links, Form Designer JavaScript API. The values are not saved if both of the following conditions exist: You use JavaScript functions to set the minimum and maximum values of these attributes, and the value is dynamic. Therefore, use the JavaScript functions to apply the values individually on each page.

Attributes for Spinner Fields Only

The following HTML attributes apply to spinner fields *only.* Spinner fields are basic elements of a form (see page).

This field enables users to select one of many values by clicking the up or down arrow. Each time the user clicks an arrow, the selected value increases or decreases by the amount that the Increment attribute specifies.

Typically, the values for a spinner field appear in meaningful, equal increments. An example is 50, 100, 150, and so forth.

- **Allow Decimals**
  Specifies whether to use decimal values, for example, in the rate or cost.

- **Allow Negative Numbers**
  Specifies whether to use negative values.

- **Increment**
  Specifies the amount by which the selected value increases or decreases each time that the user clicks the up or down arrow. For example, suppose you want to use the following values: 100, 200, 300, and 400. In this example, the increment is 100. If the selected value is 200 and the user clicks the up arrow, the selected value increases to 300.

- **Minimum Value *and* Maximum Value**
  Specify the minimum and maximum values, respectively.
  In the example for the previous attribute (Increment), the minimum value is 100 and the maximum value is 400.

- **Number Format**
  Specifies the format of the number that appears to the user, for example, 1, 2, 3, and so forth. The Form Designer uses the number format of the Google Web Toolkit. For details, see the Google Web Toolkit website. At publication time, the website is www.google-web-toolkit.googlecode.com.

Attributes for Tables Only

The HTML attributes in this topic apply to tables *only*.

Table elements have the following types of attributes:

- Table attributes apply to the entire table, that is, to *all rows* in the table.
- Row attributes apply only to the selected row.

Table Attributes

The following table attributes require explanation:

- **Report/Plug-in ID and Report/Plug-in Variables**
  Apply to dynamic tables (see page 2923).

- **Allow Edits**
  Specifies whether catalog users can manually update the data that is dynamically inserted into a row by a JavaScript function. The use of a JavaScript function for this purpose is described in the Note for the next attribute, Allow Inserts.
  If the value of Allow Edits is true, users *can* manually update this data in a form as they request a service.
  If this value is false, users *cannot* manually update this data in a form as they request a service.
  The Allow Edits attribute takes effect *only* if the Allow Inserts attribute is set to false.
  If the Allow Inserts attribute is set to true, users can *always* update data in a row, regardless of the following settings:
  - Whether you populate the row with default text, a JavaScript function, or not at all
  - Whether you set Allow Edits to true or false

- **Allow Inserts**
  Specifies whether catalog users can manually add rows to tables in a form when they are requesting a service.
  When this value is false, users *cannot* add rows.
  When this value is true, users *can* add rows by clicking an Add icon in the table. For example, you can design a service that contains a table with several predefined options. You can also enable

the user to add custom values to the table. The advantage of using such a table over a text box is that the table stores the data in *structured* format.
If Allow Inserts is true, the following conditions exist when users update the form as they request a service:

- Users can click the Add button in the table to add rows. The data that users enter must meet the validation criteria for each cell, such as minimum text length, and data format. For each cell, the type of element that you specify determines this validation criteria.
- Users *cannot* add, delete, move, or edit rows that you specify when you create the form. All rows that a user inserts are marked with red dots in their cells.
- When users add or update rows, JavaScript functions run *only* on the row being added or updated.
- User-created rows always appear at the *top* of the table, *before* all rows populated through a report data object, an API plug-in, or static data. Moreover, user-created rows always appear in the reverse order that they were added: The first rows in the table are the last rows added.
- Sorting does not apply to user-created rows. However, sorting does apply to the rows populated through an API plug-in or static data.

Note: As a form designer, you can use JavaScript functions to add rows to tables in a form while users are requesting a service. For example, use a JavaScript function to populate a row when a user clicks an option button in a radio group. This ability exists regardless of the setting of Allow Inserts. You can use either a custom JavaScript function or the predefined JavaScript function named ca_fdAddTableRow. For more information about predefined JavaScript functions, select Administration, Tools, Links, and view the *JavaScript API Reference*.

- **Auto Number**
  Specifies whether the first column of each row contains the row number.
  If the value is true, then the first column of each row displays the row number.
  The default is true.
- **Height**
  Specifies the height of the table, in pixels.
  The default is 125.
- **Maximum Selected Rows**
  Specifies the maximum of rows that users can select in the table while completing the form in a request.
  If the number of selections exceeds this value, an error occurs.
  If this value is not specified, then the number of rows that users can select is unlimited.
- **Minimum Selected Rows**
  Specifies the minimum of rows that users can select in the table while completing the form in a request.
  If this value is not specified, then the user is not required to select any rows.

- **Mode**
  Specifies whether the table functions in *selection mode* or *data mode* during the request life cycle, as follows:

  - In selection mode, the table automatically includes a check box in the first column, so that users can select one or more rows from the table. The user-selected rows appear in the request throughout the request lifecycle.

  - In data mode, the table does *not* include the check box. Therefore, users cannot select rows from the table.

  In *both* modes, if the value of the Allow Inserts attribute is True users *can* perform the following action: Configure the request by adding rows to the table and entering custom values. The catalog system automatically saves any rows that the user adds and displays them throughout the request life cycle. Users can remove each row that they added by clicking the row and selecting Remove.
  Selection mode is useful when you want users to select a set of related options for the request by selecting a row on the table. For example, you can specify the following table:

Check Box	Disk Space, GB	Memory, GB	Processor Speed, GHz	Operating System
_	700	4	2	Windows XP
_	900	6	2.4	Windows 7
_	1000	8	3	Windows 2008 Server
_	1400	8	4	Windows 7 Server

In this example, each row contains one set of configuration options for a computer reservation. Users cannot select each option individually, but they can select a set by selecting a row.

Row Attributes

The following table attributes apply to the selected row only, not the entire table:

- **Column Widths**
  Specifies a list of comma-separated values for the *widths* of each column in the table, from left to right.
  For example, if the table contains three columns, then the following points apply:

  - The first value applies to the first (left) column

  - The second value applies to the second (middle) column

  - The third value applies to the third (right) column

  Note: This attribute *applies* to the entire table, but *appears* only in the first row.

See also attributes for select boxes and tables only (see page 2933).

Attributes for Text Fields and Text Areas Only

The following HTML attributes apply to text fields and text areas *only*. Text fields and text areas are basic elements of a form (see page).

- **password**
  Specifies an attribute for text fields. Can have a value of true or false. When the value is set to true, this component becomes a password component.

- **Height**
  Specifies the number of rows in the text area. For example, if you specify 3, the text area contains three rows.

- **Maximum Length**
  Specifies the maximum number of characters that the user can enter in the field.

- **Pattern**
  In the value for this attribute, you specify regular expressions to validate numeric and address data (see page 2980). Such data includes credit card numbers, social security numbers, email addresses, IP addresses, and telephone numbers.

- **Pattern Message**
  Applies only when *pattern* (the previous attribute) is specified.
  You can specify an error message to appear when the user input violates the pattern attribute.
  You can optionally localize (see page 2987) this error message.

JavaScript Attributes for Elements

You can use JavaScript attributes to invoke JavaScript functions (see page 2966) while the user is completing the form in a request. JavaScript functions include predefined functions for validating user input into fields and any custom functions that you have written. All JavaScript attributes are named with the prefix *on*, such as onClick.

You can use the following JavaScript attributes in elements on forms. Not all attributes apply to all elements, however. Click an element to see which attributes apply to it.

Important! JavaScript attributes *must* have JavaScript functions but not JavaScript expressions as values. Conversely, HTML attributes can have JavaScript expressions but *not* JavaScript functions as values. Thus, JavaScript expressions apply to HTML attributes *only*, and JavaScript functions apply to JavaScript attributes only.

JavaScript functions in JavaScript attributes are validated when the user performs the action that the attribute specifies. Examples are clicking (for onClick) and mousing over (for onMouseOver). If the field does not validate, it is highlighted in red and an error message appears.

Note: Verify that the error messages (if any) returned by each JavaScript function are localized for the users of the form.

- **onFocus**
  Specifies the JavaScript function to run when the element comes into focus.

- **onBlur**
  Specifies the JavaScript function to run when the element loses the focus.

- **onChange**
  Specifies the JavaScript function to run when the element value is changed.

- **onClick**
  Specifies the JavaScript function to run when the component is clicked with the left mouse button.

- **onLoad**
  Applies to dual lists (see page 2919) and select boxes (see page) only.
  Specifies the JavaScript function to run when the data associated with the select is loaded. This attribute is ignored if the dual list or select box specifies static options.
  An alert appears if an onLoad function fails to run correctly, for example, if the function cannot be found. If you receive an alert, verify that function is correctly defined and referenced, and that the function runs without errors.
  Use the Script dialog (see page 2969) on each form to create and maintain the custom JavaScript functions for the form.

- **onMouseDown**
  Specifies the JavaScript function to run when a mouse button is pressed.

- **onMouseUp**
  Specifies the JavaScript function to run when a mouse button is released.

- **onMouseOver**
  Specifies the JavaScript function to run when the component is moused over.

- **onMouseMove**
  Specifies the JavaScript function to run when the mouse passes over the component.

- **onMouseOut**
  Specifies the JavaScript function to run when the mouse was moved away from the component.

- **onKeyPress**
  Specifies the JavaScript function to run when a key is pressed and released.

- **onKeyDown**
  Specifies the JavaScript function to run when a key is pressed.

- **onKeyUp**
  Specifies the JavaScript function to run when a key is released.

- **onValidate**
  Specifies the JavaScript function to run when the field is validated. The field is validated whenever the user navigates away from a field or when the user submits the form.
  If you specify a custom JavaScript function for the onValidate attribute, code that function as follows:

  - Specify an attribute that is named _val; this attribute is required to pass the current value of the field.
  - If no validation error occurs, return null.
  - If a validation error occurs, return a string with a helpful error message explaining the problem and solution. Localize error messages for each browser locale applicable to your users.

- **onLookup**
  Applies to lookup fields *only*. When the user clicks the magnifying glass for the lookup field, the JavaScript function for this attribute runs. You can use a lookup field to populate fields based on user input to a report data object (see page 2970).

Customize a Predefined Form

This scenario illustrates how Service Managers create a form by copying a predefined form and customizing the copy. You add fields and specify some fields to be auto-populated. You use spinner fields and radio buttons so that users can specify only valid options. You also show or hide fields according to the options selected by the user. Creating form in this manner helps reduce user errors and helps increase efficiency.

This scenario focuses on the onboarding of a new employee into the Lab Services group in your organization. You can use this scenario *as a model* to create a form using similar techniques.

For other use cases, search the **Catalog**, **Forms** folder for the form that most closely matches the form that you want to create. **Example:** To create a form for ordering hardware, review the Procure New Hardware form in the IT Support Services subfolder.

Note: Service Managers typically have one or more of the following roles in CA Service Catalog: Service Delivery Administrator, Services Manager, Super Business Unit Administrator, and Catalog Administrator.

Follow these steps:

- Step 1 - Review and Copy the Form (see page 2943)
- Step 2 - Add Fields for Contact Information (see page 2944)
- Step 3 - Configure Fields to be Populated Automatically (see page 2945)
- Step 4 - Copy and Modify Radio Buttons (see page 2945)
- Step 5 - Add Text Areas (see page 2946)
- Step 6 - Show and Hide Text Areas (see page 2947)
- Step 7 - Add Spinner Fields (see page 2949)

- Step 8 - Test the Form in a Service (see page 2949)

Important! We recommend that you do not create multiple forms with the same _id value for each form. If you already have multiple forms with the same _id value, do not associate such forms to a single Service Option. Having multiple forms with the same _id value in a single Service Option can cause validation errors.

Step 1 - Review and Copy the Form

All services include at least one predefined or custom form to record essential information from the user requesting the service. In this scenario, you review and copy the predefined form included with the standard New Hire Onboarding service. Afterwards, you modify the copied form for use by the New Hire Onboarding for Lab Services group.

Follow these steps:

1. Click **Catalog**, **Forms**.
2. Expand **Forms**, **CA Catalog Content** in the Component Tree.
3. Select **New Hire Onboarding**.
4. Click Copy.
5. Move the top level of the Forms folder and complete these actions:
   a. Click **Add** and create a subfolder and call it Custom.
   b. Select the Custom folder and click Paste.
   The form is copied, and its new name is "copy of *original name*." The copied elements under the copied form are *not* renamed.

      Note: If you copy the form from one business unit to another, the pasted form, including all elements under it, belong to the business unit of the destination folder.

   c. Select the form and click Rename.
   d. Enter the new name as New Hire Onboarding for Lab Services. Click OK.

Note: The name must be unique within its business unit.

6. Specify new_hire_onboard_labservices in the _id attribute for the form, press Enter, and click Save.

> **Note:** After you specify a new value for any attribute, press Enter to enable the Save button. This value of the _id attribute of the form is the form ID. Specify a unique ID for each form in a business unit.

Step 2 - Add Fields for Contact Information

Modify the form that you copied in the previous procedure by adding more contact information fields. These new fields increase the options for other employees to communicate with the Lab Services employees.

Follow these steps:

1. Expand the New Hire Onboarding for Field Lab Services form.
   The list of components in the form appear in the tree under the form name. This list matches the same named components in the middle pane.

2. Copy the Last Name field, to create another field, as follows:

   a. Select the Last Name field in the tree, and click the Copy icon.

   b. Select the name of the New Hire Onboarding for Lab Services form in the tree, and click Paste.

   c. In the _id attribute in the right pane, specify a unique ID. For example, employee_id. Press Enter and click Save.

3. Rename the new field, as follows:

   a. Select the field and click Rename.
      The Name dialog appears.

   b. Enter the new name as Employee ID. Click OK.

4. Move the Employee ID field, as follows:

   a. Select the name of the field in the tree.

   b. Drag it upwards until the horizontal line for the field appears above the Job Title field, and drop it.

   c. Verify that the First Name, Last Name, and Employee ID fields now appear sequentially in the tree.

5. Using steps 2-4 as a model, add the following new fields and move them under the Employee ID field:

- Email
- Phone number
- Address

You have added more fields for contact information.

Step 3 - Configure Fields to be Populated Automatically

Use JavaScript expressions to retrieve the data from the user database and populate the fields automatically to reduce errors and increase efficiency.

Follow these steps:

1. Expand the Forms tree to display the fields of the New Hire Onboarding for Lab Services Only form.
2. Specify the following JavaScript expressions in the Value attributes of the following fields. Press Enter and click Save after you specify each value.
   - First name: $(_.user.firstName)
   - Last name: $(_.user.lastName)
   - Employee ID: $(_.user.id)
   - Email: $(_.user.email)
   - Phone: $(_.user.phone)
   - Address: $(_.user.address)

When a catalog user opens this form while requesting a service, these fields are automatically populated based on the user ID specified at login.

Step 4 - Copy and Modify Radio Buttons

You can add radio buttons to the New Hire Onboarding for Lab Services Only form to allow users to select the type of server. Copying and modifying the radio buttons is more efficient than creating them. Therefore, you copy the radio buttons from the Procure Sun Server form and modify them for this form.

Follow these steps:

1. Expand **CA Catalog Content** in the Forms tree and perform these actions:
   a. Expand **Procure Server** and **Procure Sun Server**.
   b. Select the Choose Server Model field and click the Copy icon.
   c. Navigate the Forms tree to the New Hire Onboarding for Lab Services Only form. Select this form and click the Paste icon.

2. Move the Choose Server Model field, as follows:

    a. Select the name of the field in the tree.

    b. Drag it upwards until the horizontal line for the field appears above the Additional Info field, and drop it.

    c. Verify that the Hiring Manager, Choose Server Model, and Additional Info fields now appear sequentially in the tree, followed by the other fields.

    d. Verify that the Choose Server Model field includes these options Starter, Mid Size, and High End.

Note: The values for _id and other attributes for these fields are already set, because you copy them rather than create them. We use the same attribute values in this scenario because the values remain unique within the same form.

Step 5 - Add Text Areas

Add a text area to provide specifications for each type of server.

Follow these steps:

1. Verify that the New Hire Onboarding for Lab Services Only form is displayed in the Preview Pane.

2. Click **Components**, **System** in the Form tree.

3. Drag and drop the the Text Area element to your form directly above the Additional Info field.

4. Verify that the text area appears above the Additional Info field in the Preview Pane.

5. Select the Text Area in the tree and click the **Rename** button. Specify the new name as Starter.

6. Specify these values for the following attributes. After you specify each value, press Enter and click Save.

    - _id: starter_description
    - Value: 10K (ULTRA 10000, Starfire) UltraSPARC® processor
    - Disabled: true
      This setting means that this field is read-only, so that users *cannot* change the text that you specified.
    - Hidden: false

7. Repeat the previous steps for the next two text areas: Mid Size and High End. Use the following specifications for the attributes:
   Mid Size Text Area:

   - Name: Mid Size
   - _id: midsize_description
   - Value: 20K UltraSPARC IV & UltraSPARC III Processors
   - Disabled: true
   - Hidden: true

   High End Text Area:

   - Name: High End
   - _id: highend_description
   - Value: E25K UltraSPARC IV & UltraSPARC III Processors
   - Disabled: true
   - Hidden: true

8. Verify that the three Text Area fields appear on the form before the Additional Info field.

Step 6 - Show and Hide Text Areas

Add JavaScript functions to the form so that *only* the description of the selected server type (Starter, Mid Size, or High End) appears. If the user selects a new server type, the previous description is replaced with the description for the new selection. This enhancement helps save time for the user by eliminating the need to scroll through multiple static descriptions. This reduced scrolling is especially helpful for mobile users.

Follow these steps:

1. Select the New Hire Onboarding for Lab Services Only form in the Preview Pane.
2. Click the Script icon at the top of the form and proceed as follows:
   a. Delete the existing sample code.
   b. Copy and paste the JavaScript code from the section that is named JavaScript for New Hire Onboarding for Lab Services into the Script dialog.
   c. Save the script, and close the dialog.
3. Expand the form to show the fields for the Choose Server Model radio buttons.

4. Enter the following JavaScript function call in the onClick attribute of the Starter, Mid Size, and High End fields. After you update the attribute for each field, press Enter and click Save.

   ```
   ca_fd.js.onFormLoad();
   ```

   This call loads the JavaScript code that you copied earlier to the Script dialog for the form.

JavaScript for New Hire Onboarding for Lab Services

```
{
  onFormLoad : function() {
    ca_fd.js.clickStarter();
    ca_fd.js.clickMidSize();
    ca_fd.js.clickHighEnd();
  },

// ShowFields/HideFields either shows or hides the description field for Starter
servers when Starter radio is changed
// ResetFields will reset MidSize and HighEnd when selected and clicked away from
Starter
// This function is called in to Starter radio's onChange
  clickStarter : function() {
    if (ca_fdIsSelectRadio('new_hire_onboard_labservices','class','starter')) {
ca_fdShowField('new_hire_onboard_labservices','starter_description'); }

    else {
ca_fdHideField('new_hire_onboard_labservices','starter_description');

        ca_fdResetFields('new_hire_onboard_labservices',['starter_description']); }
  },

// ShowFields/HideFields will either show or hide the description field for Mid Size
servers when MidSize radio is changed
// ResetFields will reset the description field for Mid Size servers when selected
and clicked away from MidSize
// This function is called in to MidSize radio's onChange
  clickMidSize : function() {
    if (ca_fdIsSelectRadio('new_hire_onboard_labservices','class','midsize')) {
            ca_fdShowField('new_hire_onboard_labservices','midsize_description'); }

    else {
ca_fdHideField('new_hire_onboard_labservices','midsize_description');

        ca_fdResetFields('new_hire_onboard_labservices',['midsize_description']); }
  },

// ShowFields/HideFields will either show or hide the description field for High End
servers when HighEnd radio is changed
// ResetFields will reset hide the description field for High End servers when
selected and clicked away from HighEnd
// This function is called in to HighEnd radio's onChange
  clickHighEnd : function() {
```

```
    if (ca_fdIsSelectRadio('new_hire_onboard_labservices','class','highend')) {
        ca_fdShowField('new_hire_onboard_labservices','highend_description'); }

    else {
ca_fdHideField('new_hire_onboard_labservices','highend_description');

        ca_fdResetFields('new_hire_onboard_labservices',['highend_description']); }

  },
}
```

Step 7 - Add Spinner Fields

As a best practice, configure each form so that users can specify only a valid number of items. This practice helps reduce errors. To implement this practice, the form uses a spinner to field to let users request 0-10 servers of each type.

Follow these steps:

1. Verify that the New Hire Onboarding for Lab Services Only form is displayed in the Preview Pane.
2. Click **Components**, **System** in the Form tree.
3. Drag and drop the Spinner Field element to your form directly above the Additional Info field.
4. Verify that the Spinner Field appears above the Additional Info field in the Preview Pane.
5. Select the Spinner Field in the tree and click the **Rename** button. Specify the new name as Number of Starter Servers.
6. Specify these values for the following attributes. After you specify each value, press Enter and click Save.
   - Maximum Value: 10
   - Minimum Value: 0
   - Increment: 1
7. Repeat the previous steps for the next two fields: Mid Size and High End.
   Letting users specify 0-10 of each type of server provides flexibility for users. To prevent users from specifying 0 for all three types, specify a value of 1 or higher as the default value of one field.
8. Verify that the three spinner fields appear on the form before the Additional Info field.

Step 8 - Test the Form in a Service

Test the form before you make the form available in a service.

Follow these steps:

1. Select the service to which you want to add the form.
2. Add the form to a service option group in that service.
3. Verify that the service is available.
4. View the service in the catalog, complete the form, and submit the request.
5. Verify the specifications if you detect any errors.
   For example, if the text areas do not show or hide as planned, verify that the related JavaScript code and attributes (see page 2947) are correct.

Create and Customize a Form

This article contains the following topics:

Administrators add and configure elements on forms, including text fields, check boxes, radio buttons, and more. Each element of the form captures information for approving and completing a request for a service. All services include at least one

Important! We recommend that you do not create multiple forms with the same _id value for each form. If you already have multiple forms with the same _id value, do not associate such forms to a single Service Option. Having multiple forms with the same _id value in a single Service Option can cause validation errors.

Follow these steps:

1. Verify that the elements do *not* duplicate fields on other forms for the same service, including system forms (see page).
2. Decide which elements you want on the form and in which order. Verify that each part of the draft form has a matching element on the Form Designer.
3. Using the Form Designer, create a form (see page 2951).
   Alternatively, consider these options:
   - Use an existing Form Designer form.
   - Use an existing Form Designer form as a starting point, and modify it to include the changes you want.
     For both possibilities, see the forms in the predefined services and any custom services that you have. See also the forms in the content packs.

- Use the Customize a Predefined Form (see page 2942) scenario and create a form by copying and modifying the predefined form.

4. For each element, specify the HTML attributes and JavaScript attributes (see page 2954).
5. Attach the form to a service option group (see page 2954) and test it in a service.

Create a Form

You can create a form to include in a request. You can also capture user input that is required to complete the request. For example, a form typically lists options and records the ones that the user selects.

Note: The form level associations are showed only for the selected Business Unit level.

Follow these steps:

1. Click **Catalog**, **Forms**.
2. Click the **Forms** folder to select it.
3. Click the **Add** button above the **Components** folder and select **Form** from the drop-down list.
4. Enter the name of the new form and click OK.
   The new form appears in the Forms folder. The form attributes appear in the Item Inspector (the right pane).
5. Specify the required and optional form attributes (see page 2927). These attributes are for *the form itself*. These attributes are *not* the same as the HTML and JavaScript attributes of the *elements* on the form.

Add, Move, and Delete Elements

You can add and configure the elements (see page 2916), such as text fields, text areas with check boxes and radio buttons.

Follow these steps:

1. Click **Components** and expand **System**. Verify that the element you want to add appears in the tree view under the System folder.
   For example, to add a text field, verify that the System folder appears and is expanded to show the Text Field option. Similarly, to add a select box and its options, verify that the System, Radio Group folder appears and is expanded to show the Radio option.
2. Verify that the form to which you want to add the element already exists.
3. Expand the **Forms** folder. Scroll to the form to which you want to add the element.

4. Verify that both the element you want to add and the intended form are visible in the tree view simultaneously.

5. Click the element (for example, Text Field), drag and drop it on the intended form in the Component Tree.
   For example, you have a custom form named Model Options. Click Text Field under the System folder. Drag Text Field to Model Options, and drop it there. All these actions can be on the Component Tree or the Preview Pane.
   When you click and drag an element, both a checked circle and the message "1 object selected" appear next to the cursor.
   As you drag the element over a form or existing form element on which it can be dropped, the checked circle turns green. Also, the cursor changes to appear as a hand. Conversely, the checked circle turns red when the dragged element is not over a form or form element on which it can be dropped.

   Note: The element is not added if the attempted action violates a rule. Examples include attempting to drop a select option onto a radio group or to drop a select group onto another select group.

6. Specify the *required* HTML attributes (see page 2928) for the new element, and click Save.
   The required HTML attributes for each element appear in bold.

   Note: Attempts to perform a different action *before* completing this step fail. For example, attempts to drag-and-drop a new element *before* saving this element fail.

7. Check the form in the Preview Area (the middle pane) to verify that the element was added to the form as intended. If it was not, you can either rearrange the elements or delete the new element and try adding it again.

8. Specify the optional HTML (see page 2928) attributes (see page 2928) (if any) that you want for the new element, and click Save.

9. By default, components are organized in one column. You can optionally configure the form to use two columns, as follows:

   a. Drag Column Layout from the System folder and drop it onto a desired form.

   b. When you drop this layout, the tree updates with Column Layout and its two children, Column 1 and Column 2 automatically.

   c. Click the icon next to Column Layout to display the two columns, which are named Column1 and Column 2.

   d. Drag-and-drop other elements, such as text fields, radio groups, and select boxes, onto Column 1 and Column 2.

> **Note:** When you highlight the Column Layout or a Column, the corresponding sections in the Preview Area of form may be rendered gray and disabled, and the elements within the column may be highlighted with red border.

10. Specify the JavaScript attributes (see page 2940) (if applicable) for the new element, and click Save.

11. Specify a meaningful name for the new element, as follows:

    a. Select the new element in the Component Tree and click the **Rename** button at top of the Component Tree.

    > **Note:** Verify that you select the new element on *your* form in the Component Tree. Do *not* select the same-named element on the *System* folder in the Component Tree.

    b. Enter the new name and click OK.

    For example, perform these actions in a custom External Storage Drive Order Form:

    - Drag-and-drop a radio group and change its name from the default Radio Group to Capacity in GB.
    - Drag-and-drop three radio buttons onto that radio group. Change their names from the default radio button to Small (50), Medium (100), and Large (150), respectively.

    > **Note:** When you create a new element, a colon (:) is automatically included at the end of its name. The colon does not appear in the Name dialog when you rename the element. However, it does appear in the Preview Area after you click OK to close the dialog. Verify that you do not enter another colon in the Name dialog. Otherwise, the element has *two* colons after its name in the Preview Area.

12. Verify that the new element appears and functions as you intended. If necessary, refine any attributes to obtain the appearance and function you want.

13. (Optional) Move elements on the form by dragging and dropping them onto a different location in the form.

14. (Optional) Delete the elements that you no longer want on the form by selecting them and clicking **Remove**.

Specify Attributes for an Element

After administrators add an element to a form, they specify its required HTML attributes and any optional HTML attributes or JavaScript attributes. Specifying these attributes helps you modify the element to meet your requirements.

Follow these steps:

1. Click **Catalog**, **Forms**.
2. Open your form. For example, expand the Forms folder and select the form whose elements you want to configure.
3. Click the icon next to the form name to expand the folder for the form and display its elements.
4. Select the element whose attributes you want to set.
   The Item Inspector (the right pane) displays the names and values of all HTML attributes and JavaScript functions available for the selected element.
5. In the Item Inspector, search the Name column and locate the attribute, one of the following types:
   - HTML Attributes (see page 2928)
   - JavaScript Attributes (see page 2940)
6. Move your cursor to the adjacent field in the Value column and click.
7. Enter the value for this attribute and click Save.
   For example, you can set the value for Hidden attribute of a Label element.
8. Verify that all required attributes are set correctly.

Attach a Form to a Service Option Group

Administrators attach a form to one or more applicable service option groups. Users who select one of these service options in a request are prompted to complete the form. The form lets the user enter data to complete the request.

Follow these steps:

1. Click **Catalog**, **Service Offerings**,**Option Groups**.
2. Click the service option group name to which you want to add the form.
3. Click the **Edit** icon for the service option to which you want to add the form.
4. Click the **Add** button for the form.
5. Enter meaningful text that describes the purpose of this form, in the Display Text Field.

6. Click the magnifying glass icon in the Form Name field to select a form.
7. Navigate through the form tree and select the form that you want to attach.
8. Click the Select Form button.

   Note: You can add a form to a service option only once.

9. If you do *not* want to hide or disable the entire form at any point, leave the Hidden and Disabled fields blank. In that case, skip the remainder of this step.
   If you want to hide or disable the entire form according to a criteria, enter the corresponding JavaScript expression in the Hidden or Disabled field. Use the following format: $(_.*object*.*property*). The expression must return a value of true or false.
   Example:

   - To hide or disable the form when the request status is Pending Approval, enter: $(_.request.status == 400)
   - To hide or disable the form for end-user roles *only*, enter: $(_.user.role == 'enduser')

   You can also specify other JavaScript expressions in fields (see page 2957).

   Note: When a form is disabled, it is disabled but visible during all stages of the request life cycle *except* check-out. During check-out, a disabled form is both disabled and hidden.

10. Click the Options tab and complete the remaining fields on the Service Option Element Options Window--Options Tab (see page 3019).
11. Click Update and click Save.

Perform Automated Tasks in Form Fields

Administrators can use JavaScript expressions and JavaScript functions to perform automated tasks in form fields. At runtime, when the user fills out the form while completing a request, the JavaScript expression or function runs and performs the specified task.

Important! To use JavaScript expressions and functions, you must have a working knowledge of HTML, CA Service Catalog administration, and JavaScript.

Follow this process to specify automated tasks in fields, using one or more of the following options: JavaScript expressions, JavaScript functions, and report data objects.

1. Verify that you can represent the field or fields as one or more of the elements (see page 2916) available for creating forms. The elements can be text fields, check boxes, select boxes, or radio groups.

2. Determine whether to achieve the goal you intend for the field by one or both of the following methods:

   - Specifying a JavaScript *expression* for the value of an *HTML* attribute of the element
   - Specifying a custom or pre-defined JavaScript *function* for the value of a *JavaScript* attribute of the element

3. Consider specifying a JavaScript expression (see page 2957) for the value of an HTML attribute of the element. The JavaScript expression runs only once, as soon as the form appears. Examples:

   - Pre-populating user-related data in one or more fields on a form.
   - Disabling a field based on the request status, on the business unit or role of the user completing the form.
   - Hiding a field based on the request status, on the business unit or role of the user completing the form.

   JavaScript expressions retrieve the values of object properties from the CA Service Catalog database at runtime. These properties are grouped into the following categories: user, business unit, service, service option groups, and request.

   Note: To hide an *entire* form, you do not specify JavaScript expressions for any fields but for the entire form when you attach the form to a service option group.

4. Consider specifying a JavaScript function (see page 2966) for the value of a JavaScript attribute of the element. (For more information about *predefined* JavaScript functions, select Administration, Tools, Links, Form Designer JavaScript API.)
   This method is best suited for dynamic events that occur when the user performs an action while completing the form. The JavaScript function can run multiple times when a user checks a box, enters a value, or performs some other action. Thus, JavaScript functions are most useful when you want to create dynamic relationships between fields.

   - Enabling or displaying a list of options or fields under a check box when a user enables the check box.
   - Disabling or hiding a list of options or fields under a check box when a user clears the check box.

5. Test the JavaScript expressions and JavaScript functions to verify that they accomplish your goals for the fields on the form.

Use JavaScript Expressions in Fields

This article contains the following topics:

Administrators follow this process to use JavaScript expressions to perform automated tasks in fields:

1. Decide the fields on the form for which you want to specify a JavaScript expression. Also, decide the task that you want the JavaScript expression to perform. For example, you can pre-populate fields. You can hide or disable forms or fields under certain specific conditions. Another example is to pre-populate the value attribute of a field with the runtime value of one of many objects and properties from the CA Service Catalog database. To pre-populate a field for a user while the user is completing a form, specify a simple JavaScript expression for the value attribute of the field, using the following format: $(_.*object*.*property*), such as $(_.user.lastName)

2. Verify that you can represent the field as one of the elements (see page 2916) available for creating forms.

3. Verify that the purpose or goal you intend for the field is represented in one of the following HTML attributes (see page 2928). You can specify JavaScript expression for the values of the following HTML attributes *only*.

   - Value - Value is the only attribute for which you can use JavaScript expressions to pre-populate values in fields. The value attribute is most frequently used for this purpose, especially for pre-populating user-related data such as address, phone numbers, business unit, and other personnel-related data

   - Disabled - You can disable a field, according to the user's role or business unit, the request status, or other criteria that you specify.

   - Hidden - You can hide a field, according to the user's role or business unit, the request status, or other criteria that you specify.

   - Checked - Check boxes and radio buttons support the checked attribute.
     You can select a check box or a radio button, according to the user's role or business unit, the request status, or other criteria that you specify.

   - Required - You can set a field as required, according to the user's role or business unit, the request status, or other criteria that you specify.

4. Keep in mind these rules when coding JavaScript expressions for use in the HTML attributes:

- For the disabled, hidden, checked, and required attributes, the JavaScript expression must return a value of true or false.

- If the returned value is any value except true, CA Service Catalog automatically uses a value of false. The value attribute is the only attribute that is used for pre-populating fields.

5. Review the objects and properties that you can specify in JavaScript expressions (see page 2958) and determine which ones you need. These objects and properties are retrieved from the CA Service Catalog database at runtime, as noted earlier, and are grouped according the following categories: user, business unit, service, service option group, and request.

6. If the objects and properties that you need cannot be retrieved using a JavaScript expression, consider using the following pre-defined JavaScript function (see page 2967) to retrieve them: ca_reportQuery(reportId, variables, onSuccess, onFailure).

7. Review and follow the instructions for performing any of the following tasks or use them as a model for a similar task, if applicable:

   - Pre-populate fields (see page 2963)

   - Hide or disable a field (see page 2964) based on the request status, the business unit or role of the user completing the form, or on other criteria

   - Select options for fields by default (see page 2965) based on the request status, the business unit or role of the user completing the form, or on other criteria; you may select a check box or an option in a radio group by default, based on such criteria

   - Hide, enable, or disable an entire form under specified conditions (see page 2966).

8. Using all applicable information from the previous steps, construct and test the JavaScript expression to accomplish your goals for the fields on the form.

Objects and Properties that You Can Specify in JavaScript Expressions

You specify objects and properties in JavaScript expressions. You can use these expressions for the runtime values of the *value* attribute for the elements that you use as fields on forms. Typically, you specify these expressions in the following format: $(_.*object*.*property*).

For example, to capture the runtime value of the logged in user completing the form in a request, specify $(_.user.firstName). You can also concatenate strings, as explained later in this topic.

Forms

The form object contains the following property that you can use in JavaScript expressions or as a first parameter in JavaScript functions (see page 2967): ca_fd.formId.

formId refers to the *active* form. The form is in active when a field in the form triggers an event. The following are a few sample actions that activate forms:

- The user opens the form while working on a request, which activates the JavaScript attribute named onLoad.

- The user clicks a label or image, which activates the JavaScript attribute (see page 2940) named onClick.
- The user submits the form, which activates the JavaScript attribute named onSubmit.

User

The user object contains an array of user properties that you can access using _.user.

Each user object has the following properties, listed in related groups:

- id, uuid, status (0 = active, 1 = inactive)
- firstName, lastName, middleName, commonName, alias, title
- groups
  The _.user.groups property specifies the name of a user group in CA EEM. You can use this property to manipulate a field based on whether the user belongs to a specific CA EEM group. For more details, see the Example section.
  The _.user.groups property contains an array with all the CA EEM groups to which the user belongs.
- manager, delegate, description
- phone (an array: phone[0] = primary and phone[1] = secondary)
- mobile, fax, pager, email
- timezone, localeLanguage, localeCountry, defaultRole, defaultDomain, location.uuid, location.name, location.city, location.state, location.country, location.postalCode, location.phone, location.fax, location.description, location.address[0-5]
- roles.<domain>

Examples

You can use the _.user.groups property to hide a field from members of a CA EEM group, for example, the group named developers. To do so, set the value of the HTML attribute (see page 2928) named Hidden to the following:

```
_.user.groups.indexOf("developers") >= 0
```

In contrast, you can also make a field visible to users who are *not* members of a CA EEM group. To do so, set the value of the Hidden attribute to the following:

```
_.user.groups.indexOf("developers") < 0
```

Business Unit

The business unit object contains an array of business unit properties that you can access using _.bu.

Each business unit object has the following properties, listed in related groups:

- id, name
- type(business unit type where SP=service provider, ST=can have child business units, TE=cannot have child business units)
- singleAccountMode (true or false)
- status (0=inactive, 1=active)
- openedDate, description, timezone, federalTaxId, stateTaxId, taxRegion, currency, dateFormat, parent (parent bu id)
- email, website, primaryContact (contact userid), location.uuid, location.name, location.city, location.state, location.country, location.postalCode, location.phone, location.fax, location. description, location.address[0-5]
- data1, data2, data3, data4, and data5

Request

The request object contains an array of request properties that you can access using _.request.

Each request object has the following properties, listed in related groups:

- id, name, requestedFor, requstedForAccountId, requestedBy, requestedByAccountId
- description, priority, status
- dateCreated, completionDate, dateRequired, and lastModified
- newDateRequired, newName, and newPriority
  These properties reflect the new value of an object as soon as the user updates the object during the request lifecycle. (The user is typically a request manager or the requestor.)
  The user can update the object, for example, while approving, rejecting, or pushing through the pending action for the item associated with the property. The *new* value takes effect *immediately* when the user updates the property; saving is *not* required.
  When creating or editing forms, you can use these properties at your discretion. For example, you can use these properties in a custom JavaScript function for validation that you use in the JavaScript attribute (see page 2940) named OnSubmit. For example, if a user enters an invalid date such as a holiday, your custom JavaScript function can display text explaining the valid dates.

Service

The service object contains an array of services that you can access using _.service.

Each service object has the following properties, listed in related groups:

- id, bu, name, description
- status(0=deleted, 1=available, 2=unavailable, 3=created, 4=cancelled, 5=total)
- website, code, version, dateAvailable, dateUnavailable, dateCreated, dateCancelled

Service Option Groups

The service option groups object contains an array of service options that you can be access using _.sog.name.

Each service option group has the following properties, listed in related groups:

- id, bu, name, description
- status(0=deleted, 1=available, 2=unavailable, 3=created, 4=cancelled, 5=total)
- code
- dateAvailable, dateUnavailable, dateCreated, dateCancelled

Service Options

The service option object applies *only* to the predefined JavaScript function (see page 2967) named _.serviceoption.status( ).

The _.serviceoption.status( ) function contains a single property, which is named newStatus.

Note: This function does *not* take any parameters.

- **newStatus**
  Specifies the *new* value for the status when a user action updates the status of the service option. This property takes the new value for the status as soon as the user does one of the following:
  - Selects a new status value from the drop-down list in the Action column while managing requests pending action (see page 2205) . A request manager typically performs this action. The value of newStatus changes dynamically as soon as the user selects the new status of the service option.
  - Opens a page or dialog that changes the status to a fixed value when the user clicks OK. For example, when a user creates a request, the value of newStatus changes dynamically as soon as the user creates the request. In this example, the value of newStatus immediately becomes Submitted.

  In both cases, the value of _.serviceoption.newStatus() changes immediately. In contrast, the value of _.serviceoption.status( ) remains unchanged until the page is submitted and refreshed.

Examples

You can use the newStatus property to help your implementation process reservations efficiently. For example, suppose a user submits a main request for a computer and additional requests for related options. These options include extra memory, an upgraded keyboard, and so forth. You can create a custom JavaScript function so that if the main request is rejected, the onSubmit function runs for all optional requests. Examples of optional requests include accessories, extra memory, and so forth. For example, the following expression evaluates to True when the original status is 400 and the newStatus is changed to 800:

```
if (_.serviceoption.status() == 400 && _.serviceoption.newStatus == 800)...
```

Operators

The operators most commonly used for form design are described here. For complete details about standard operators, see the JavaScript standards reference that your organization uses, for example, www.developers.sun.com, or www.javascript.com.

You can specify all standard operators in your JavaScript expression *except* assignment operators.

The assignment operators are as follows: =, +=, -=, *=, /= .

For example, the folowing expression is invalid because it uses the = assignment operator:

```
$(var x = 1+2)
```

Required Return Values

Specify JavaScript expressions for the disabled, checked, and hidden attributes that return one of the following values:

- true or “true”
- false or “false”

If the expression returns any other value, CA Service Catalog replaces it with a value of false. Therefore, if you specify $(_.user.firstName) for the disabled attribute of a text field, the field is not disabled unless "true" is the first name of the user.

Concatenation Operators

You can optionally concatenate two strings together, using the + operator,

For example, $(‘Hello ‘ + _.user.firstName + ‘ ‘ + _.user.lastName) returns the following text: Hello *first-name last-name.* "Hello John Doe" and "Hello Jane Smith" are samples.

Comparison Operators

You can optionally use the following comparison operators:

- == is equal to
- === is exactly equal to (value and type)
- != is not equal
- > is greater than
- < is less than
- >= is greater than or equal to
- <= is less than or equal to

Logical Operators

You can optionally use the following logical operators:

- and (&&)
- or (||)
- not (!)

Pre-Populate Fields Based on JavaScript Expressions

When you use an element (see page 2916) that includes the *value* attribute as a field on a form, you can use a JavaScript expression to pre-populate the element's value attribute with the runtime value of one of many objects and properties from the CA Service Catalog database.

For example, in the text field for First Name on your form, you can specify the JavaScript expression $(_.user.firstName) to pre-populate the field with the first name of the logged in user ID who is creating the request and completing the form. Similarly, in the text field for Last Name, you can specify the JavaScript expression $(_.user.lastName) to pre-populate the field with the user's last name.

Follow these steps:

1. Design and create the form (see page 2951).
2. Review the guidelines for using JavaScript expressions in fields (see page 2957) and verify that you want to pre-populate the value attribute of an element in the field.
3. Verify that the data that you want to pre-populate is one of the objects and properties that you can specify in JavaScript expressions (see page 2958). These objects and properties are related to the logged in user's personnel data, to one or more business units, or to service, service options, status, or other data related to the request that contains the form.
4. Specify the JavaScript expression in the value attribute of the element for the field. When specifying the expression, follow all syntax rules in objects and properties that you can specify in JavaScript expressions (see page 2958), especially the rules related to using operators to link properties. The following examples are some valid expressions:
   - User's first name: $(_.user.firstName)
   - User's last name: $(_.user.lastName)
   - User's first name and last name, concatenated in a single field: $(_.user.firstName + ' ' + _.user.lastName)
   - User's physical address data, concatenated in a single field: $(_.user.location.address[0] + ' ' + _.user.location.address[1] + ' ' + _.user.location.city + ' ' + _.user.location.state)
     This example returns the street address, city, and state of the user, for an address in the United States.
   - User's role: $(_.user.roles[domainId])

- User's business unit, with parent: $(_.bu.id)
- User's business unit, without parent: $(_.bu.id.parent)

5. Test the JavaScript expression to verify that it accomplishes your goals for pre-populating the field on the form.

Hide or Disable a Field Based on Request Status, Business Unit, Role or Other Criteria

Decide to use JavaScript expressions to hide or disable a field based on the request status, on the business unit or role of the user completing the form, or on other criteria.

As an administrator, you typically disable fields that you want users to view but *not* update. Examples include options for a service that the user's manager selected or that the request manager selected based on available inventory.

In contrast, as an administrator, you can hide fields when you either do not want users to be aware of them at all, for some reason, or when the fields add distracting information that the user does not need. Examples include cost data, inventory options available to certain roles only or certain business units only, or data that does affect the end user, such as the estimated administrative cost of fulfilling the service.

To hide a field, specify the JavaScript expression that specifies your criteria in the hidden attribute of the field element. Similarly, to disable a field, specify the JavaScript expression that specifies your criteria in the disabled attribute of the field element.

Important! Hiding or disabling a *field* is not completely secure. While the field and its value are not displayed on the CA Service Catalog page, the data does still exist on the form's HTML page and can be accessed by viewing the source text of the browser. Therefore, to restrict sensitive data, create two versions of the form and hide the form that contains the sensitive data from users who you do not want to see it. For more information, see How to Hide, Enable, or Disable an Entire Form Under Specified Conditions (see page 2966).

Follow these steps:

1. Design and create the form (see page 2951).
2. View the field that you want to enable or disable and verify that it includes the HTML attribute (see page 2928) named disabled.
3. Determine the exact criteria that you want to use to disable or enable the field. Examples of the criteria are the request status, the business unit or role of the user completing the form. If the disabled attribute is set to true, users can view the field but cannot edit it. Conversely, if the disabled attribute is set to false, users can both view and edit the field.
4. Verify that the data that you want to use to determine whether to enable or disable the field is one of the objects and properties that you can specify in JavaScript expressions (see page 2958).
5. Review the guidelines for using JavaScript expressions in fields (see page 2957).

6. Specify the JavaScript expression in the value attribute of the element for the field. The following examples are some valid expressions:

- To hide or disable a field if the user has the end-user role, set the hidden or disabled attribute of that field to the following JavaScript expression: $(_.user.roles[_bu.id]==’enduser’).
  This expression returns a value of true and therefore hides or disables the field *only* if the user filling out the form has an enduser role in the current business unit.
  You can use this setting or a similar one to restrict users from either viewing or editing the text field that is named Memory in a form for a request for a new laptop computer. Conversely, this example displays or enables the field for all other roles in the business unit. Thus, when used with the disabled attribute, this example permits the request manager to edit the field, based on the available inventory.
  To display or enable a field for only request managers, hide or disable it for all other roles, by setting the hidden or disabled attribute of that field to $(_.user.roles[_.bu.id] != ‘requestmanager’).

- To hide or disable a field in a form that is shared by all business units *only* if the current business unit is PBJ222, set the hidden or disabled attribute of that field to $(_bu.id==’PBJ222’).

Select Options for Fields by Default Based on Request Status, Role, Business Unit, or Other Criteria

As an administrator, you can use JavaScript expressions to select a check box by default or select an option for a radio group by default,.Conversely, you can clear certain check boxes or radio group options by default according to such criteria. For example, select the check boxes related to publicly known managerial duties by default for managers only, while clearing them for other users.

Selecting or clearing the check box or radio group option by default does not prevent the user from changing the default that you specified before submitting the request that contains the form. Therefore, before using this feature, verify that permitting users to change the default is appropriate. Consider redesigning the form to either hide or disable the field (see page 2964) the options that you want to prohibit users from changing, according to the criteria specified in your JavaScript expression.

Follow these steps:

1. Design and create the form (see page 2951).

2. On the Form Designer, view the check box or radio group option that you want to select by default and verify that it includes the HTML attribute (see page 2928) named checked.

3. Determine the exact criteria that you want to use to select the check box or radio group option by default. The criteria can be based on the request status, on the business unit or role of the user completing the form, or some other criteria.

4. Verify that the data that you want to use to make the selection is one of the objects and properties that you can specify in JavaScript expressions (see page 2958). These objects and properties are related to the logged in user's personnel data, to one or more business units, or to service, service options, status, or other data related to the request that contains the form.

5. Review the guidelines for using JavaScript expressions in fields (see page 2957).

6. To select a check box or select an option for a radio group by default, specify the JavaScript expression that specifies your criteria in the checked attribute of the field element. When the user opens the form, the expression runs as follows:

   - If the criteria *are* satisfied, then value that is returned is true. Therefore the check box or radio group option is selected by default.
   - If the criteria are *not* satisfied, then value that is returned is false. Therefore the check box or radio group option is *not* selected by default.

   When specifying the expression, follow all syntax rules in objects and properties that you can specify in JavaScript expressions (see page 2958), especially those related to using operators to link properties. The following examples are some valid expressions: In these examples, the term *option* refers to both a check box and a radio group option.

   - To select an option by default if the user has the enduser role, set the checked attribute of that field to the following JavaScript expression: $(_.user.roles[_bu.id]==’enduser’). This expression returns a value of true and therefore selects the option by default *only* if the user filling out the form has an enduser role in the current business unit.
   - To select an option by default for request managers only, set the checked attribute of that option to $(_.user.roles[_.bu.id] != ‘requestmanager’).
   - To select an option by default in a form that is shared by all business units *only* if the current business unit is PBJ222, set the checked attribute of that option to $(_bu.id==’ PBJ222’).
   - To select an option by default in a form that is shared by all business units *only* if the parent of the current business unit is PBJ222, set the checked attribute of that option to $(_bu.id.parent==’PBJ222’).

Hide, Enable, or Disable an Entire Form Under Specified Conditions

To hide, enable, or disable an entire form under certain conditions, you attach the form to a service option group and enter the JavaScript expression you want in the Disabled and Hidden fields of the Service Option Group Definition dialog. You can hide, enable, or disable an entire form according to the request status, the role or business unit of the logged in user, or according to other criteria that you specify. For more information, see Attach a Form to a Service Option Group (see page 2954).

Use JavaScript Functions in Fields

This article contains the following topics:

Administrators follow this process to use JavaScript functions to perform automated tasks in fields:

1. Consider using the pre-defined JavaScript functions (see page 2967).
2. If none of the pre-defined functions meets your goals, then write your own custom function:
   - Follow the guidelines for custom JavaScript functions (see page 2968).
   - As a best practice, use the Script dialog (see page 2969) on each form to create and maintain the custom JavaScript functions for the form.

   Consider these examples:

   - Retrieving the values of one or more object properties from the CA Service Catalog database, the MDB, or other data source. This option especially useful when the value *cannot* be retrieved with a JavaScript expression. Consider all options to populate and pre-populate fields automatically (see page 2969).
   - Validating user input (see page 2980), specifically validating the format of numeric or address data entered by the users, including social security numbers, credit card numbers, telephone numbers, email addresses, and IP addresses.
3. As needed, specify JavaScript functions to link fields in two forms for simultaneous updates (see page 2983).
4. Using all applicable from the previous steps, construct and test the JavaScript function to accomplish your goals for the fields on the form.
5. As a best practice, ensure that you test the function in a form used with a service in a test environment before you use the form and the service in a production environment.

Pre-Defined JavaScript Functions

CA Service Catalog provides several options for performing automated tasks for fields (see page 2955) in forms, including report data objects, JavaScript expressions, and JavaScript functions.

Important! Information and documentation pertaining to Predefined JavaScript API functions, descriptions, and examples are available on the CA Service Catalog console. Select **Administration**, **Tools**, **Links**, **Form Designer JavaScript API, Components.** Click **Global, Checkbox, Date, Lookup, Radio, Select, Slider, Table,** and/or **Text options** to view the Javascript APIs, functions, and description**.**

Guidelines for Custom JavaScript Functions

Use the following guidelines for creating custom JavaScript functions in forms:

- Follow the instructions for using predefined JavaScript functions (see page 2967), as applicable.
- Follow the instructions for using JavaScript attributes (see page 2940).
- You can use either the Script dialog (see page 2969) or the custom_form_lib.js file to store your custom JavaScript functions, as follows:
  - As a best practice, use the Script dialog on each form to create and maintain the custom JavaScript functions for the form. If only one form uses the custom JavaScript function, the Script dialog is preferred over the custom_form_lib.js file for the following reasons:
    - The Catalog system loads the form most efficiently when the custom JavaScript function is in the Script dialog.
    - Using the Script dialog enables you to more efficiently move the form, custom functions, and related services or service option groups together. This consideration is important if you move these objects because of an upgrade, migration, or other event.

    Note: To move these objects, use the Import Export utility. For more information about the utility, see the Migrate Data between Catalog Systems (see page 1486) section.

  - Alternatively, store custom JavaScript functions in the custom_form_lib.js file in the filestore. This method is preferred *only* when two or more forms use the same custom JavaScript function.

    Important! If you use the custom_form_lib.js file, use a third-party JavaScript minification tool to *minify* this file on production sites. Minifying the file removes unnecessary characters from the file and reduce its size. As a result, the Catalog system loads the form more efficiently. Several third-party JavaScript minification tools are available on the Internet.

- Do not write excessively long custom JavaScript functions.
- Design your forms with usability as a high priority.
- Take into account the browser locale, to support other language users and to localize forms (see page 2987) as needed.

Use the Script Dialog to Maintain Custom JavaScript Functions

The Script dialog for each form lets you create and maintain JavaScript functions that apply to a form. The functions that you save in the dialog apply *only* to the form that you are editing. To use the Script dialog for a form, you require access rights to edit the form.

Follow these steps:

1. Click the name of the form in the Form Designer tree.
   The form attributes appear, and the Script button activates. The Script button appears on the toolbar with the Localize, Save, Restore, and other buttons.

2. Click the Script button.
   The Script dialog appears and displays the custom JavaScript functions already specified for the form, if any. You can enter new JavaScript functions before or after any existing ones.

   Note: To view a template for a function, click Show Help on the Script dialog. The template shows the product-specific implementation of a standard JavaScript function.

3. Write and save the custom function. Use the format shown in the sample functions that appear when you click Show Help on the Script dialog. This format is known as *JavaScript object literal notation*.

4. Save the form.

5. Specify the name of the function in the JavaScript attribute (see page 2940) from which you want to call it. Use the following format:

   ```
   ca_fd.js.function-name
   ```

   An example follows:

   ```
   ca_fd.js.calculateCostQty()
   ```

   Typically, you specify a custom JavaScript function in one of the following:

   - The onSubmit or on Load attribute of the form attributes (see page 2927)
   - The onChange or onValidate attributes of applicable fields

You have used the Script dialog to maintain JavaScript functions that apply to a form.

Options to Populate and Pre-populate Fields Automatically

Administrators have several options for using JavaScript functions to populate and pre-populate fields automatically. *Populating* fields means that the fields are filled with the results of a database query *based on* user input. The affected fields are empty when the user opens the form. When the user enters the requested input, the database query is run and the results are used to populate the fields.

Conversely, *pre-populating* fields means that the fields are filled with the results of a database query *without* any user input. As soon as the user opens the form, the data source query is run and the results are used to populate the fields. Thus, the affected fields are populated when the user opens the form.

Review the options and choose the one that best suits your needs. Use the pre-populating options when no user input is required for the requested information to be retrieved by the database query. Use the populating options when the user's input is critical for the requested information to be retrieved by the database query.

The options for using JavaScript functions to *populate* fields automatically follow:

- Use the pre-defined JavaScript function (see page 2967) named ca_fdDoFieldLookup with a lookup field to populate fields based on user input to a report data object (see page 2970).
- Use ca_fdDoFieldLookup with a lookup field, and use other pre-defined JavaScript functions like ca_fdSetTextFieldValue to set the values of elements in your form with a custom JavaScript function.

The options for using JavaScript functions to *pre-populate* fields automatically follow:

- Pre-populate a combo box based on a report data object (see page 2972).
- Use user input to pre-populate a select box (see page 2973).
- Use user input for personal data to pre-populate a select box (see page 2976).
- Pre-populate fields based on a report data object and JavaScript functions (see page 2978).

Populate Fields Based on User Input to a Report Data Object

This topic explains how to populate fields based on user input, by using a lookup field, a report data object (data object), and the pre-defined JavaScript function named ca_fdDoFieldLookup(fieldId, reportId). You use them together to run a data object and return the results in the matching field or fields on the form.

When the user clicks the magnifying glass icon for the lookup field on the form, CA Service Catalog prompts the user to enter the variable that you specified in your data object. An example is the user ID.

When the user answers the prompt or prompts in the lookup field, CA Service Catalog runs the data object and searches the data source for the data requested in fields of the data object; for example, the first name and last name of the user ID entered in the lookup field. In this example, you create matching First Name and Last Name fields on the form, and CA Service Catalog returns the results to the user. The user selects which result (if any) to use to populate the form fields.

To populate fields based on user input, by using a lookup field, a data object, and the pre-defined JavaScript function named ca_fdDoFieldLookup(fieldId, reportId), follow these steps:

1. In the Report Builder, create a data object (see page 3232) that queries the data source (such as the MDB) for the data you want (the data copied to the matching fields on the form). The query is based on the user input to the prompt or prompts that you specify, such as user ID. Record the name of the data object for later reference.
   The following sample query for the MDB matches the example started earlier in this topic:

   ```
   SELECT userid,first_name,last_name FROM ca_contact WHERE userid = '%use
   ```

   The ca_fdDoFieldLookup function processes this query as follows:

   - "WHERE userid = '%userid%" specifies that the user is prompted to enter this value, and this value is used in the SELECT clause.
   - "SELECT userid,first_name,last_name" specifies which values to return.
   - "FROM ca_contact" specifies that the data source is the ca_contact table in the MDB.

2. On the form, add the lookup field; it is one of the elements of a form (see page 2916).

   a. For the _id attribute, specify the first field returned by the query, and save the form. Thus, in the continuing example, you specify *userid* as the value of the _id attribute.

   b. For the value of the JavaScript attribute (see page 2940) named onLookup, specify the pre-defined JavaScript function (see page 2967) named ca_fdDoFieldLookup(fieldId, reportId) and save the form.
   This function runs the data object, associates it to the lookup field, and copies the data returned by the data object to the matching fields on the form.
   For fieldId, specify the value of the _id attribute of the lookup field.
   For reportId, specify the value of the _id attribute of the data object that you created earlier.

   c. For the tool tip attribute, optionally specify instructional text, such as "Click the magnifying glass and enter the requested data." Save the form.
   In the continuing example, for the tool tip attribute, you may optionally specify text such as "Click the magnifying glass and enter user ID."

   d. Optionally rename the default display text from the lookup field from "Lookup Field" to a more meaningful name, by selecting the element in the Component Tree and clicking the Rename icon at the top of the tree.
   In the continuing example, you may rename the display text to "User ID" or something similar.

   e. Leave value attribute empty. This value is populated with the first result returned by the query. The value appears on the form to the user as the value of the lookup field.

3. Also on the form, typically under the lookup field, add the fields that hold the results returned by the query. For each field, specify the value of the HTML Attribute (see page 2928) named _ic to match exactly the ID attribute of the corresponding object in the database.

> **Note:** To optionally disable a field so that users cannot change the result returned by the query, set the disabled attribute of the field to true. You can also set the disabled attribute to true only under certain conditions that you specify.

In the continuing example, create matching First Name and Last Name fields on the form, and specify first_name and last_name, respectively, in the _id attributes of these fields.
Thus, all matching values of userid are returned in the lookup field; each result appears as a row in the search results. Users can review the search results and select a row. When the user selects a row, the lookup field closes, and the form is populated with the results from that row. The user sees something like the following on the form:
User ID: johsmi515
First Name: John
Last Name: Smith

4. Test the form to verify that it works as you intended.

> **Important!** The lookup field displays *only* the first 25 matches in the search results. If your query returns more than 25 matches, refine your query to return fewer matches.

Pre-Populate a Combo Box Based on a Report Data Object

This topic explains how to pre-populate a combo box using a data object. On a form, a combo box appears as a single line item; the user clicks its arrow to open the entire list. You configure the combo box to specify whether the user can select only one option or multiple options.

On the Form Designer, you add and configure the select group element (see page 2916) to function as a combo box. To pre-populate the combo box with the results of the data object, you use the HTML Attribute (see page 2928) named reportobjid. When the user opens the form, the data object runs and return the results in the combo box. The user then selects one or more of the options in the combo box while completing the form.

This option is useful when you want to provide the user with multiple valid choices from your data source but do not want to enable the user to specify a custom selection. This option thus helps enforce the standardization and validity of users' selections while still typically providing users with multiple options from which to choose.

Follow these steps:

1. In the Report Builder, create a data object (see page 3232) that queries the data source (such as the MDB) for the data you want. The query must specify *two* fields from the data source, as follows:

   - The first field returns the list of all possible values and populates the combo box with this list.

   - The second field returns the label for the combo box.

When the form appears, the report data object runs and populates the combo box with the resulting data.
Record the name of the data object for later reference.
Consider the following sample query for a data object for the MDB. This example returns the list of available service option groups (rate plans).

```
SELECT rate_plan_id,rate_plan_name FROM usm_rate_plan
```

This query does the following:

- "SELECT rate_plan_id,rate_plan_name" specifies which values to return:
  - rate_plan_id returns the list of all service option groups. Each plan becomes an option in the combo box; for example, Budget, Standard, Deluxe, and so forth.
  - rate_plan_name returns the label for the combo box; for example, Service Option Groups.
- "FROM usm_rate_plan" specifies that the data source is the usm_rate_plan table in the MDB.

2. On the form, add a select box; it is one of the elements of a form (see page 2916).
   a. For the _id attribute, specify a meaningful name, and save the form.
   b. For the value of the HTML Attribute (see page 2928) named reportobjid, specify the id of the data object, and save the form.

Note: When you use a data object to populate a combo box, do not add any options to the select box, because they are ignored (not used) when the user opens the form. Any options for the select box are ignored, only the data object "matters."

Use User Input to Pre-Populate a Select Box

You can use input provided by the user in one or more fields in the form to determine the values in a select box. This technique is useful when you want to provide the user with two sets of multiple valid choices from your data source but do not want to enable the user to specify a custom selection. This option thus helps enforce the standardization and validity of users' selections while still typically providing users with multiple options from which to choose.

A common application of this technique occurs on a form with select boxes for both country and state. Using the reportobjid and reportobjvars attributes, you can configure the state select box to display only the states for the country selected by the user.

To use this technique of pre-populating a select box based on a user's selection in an earlier select box, follow this process. This process uses the country-state scenario as a running example.

1. In the Report Builder, create a data object (see page 3232) that queries the data source (such as the MDB) for the data you want in the first select box. The query must return the list of all possible values and populate the combo box with this list. This step is part of the process of

pre-populating a combo box based on a report data object (see page 2972).
In our running example, create a report data object to retrieve the list of countries from the database.
When the form appears, the report data object runs and populates the combo box with the resulting data.
Record the ID of the data object for later reference.
Consider the following sample query for a data object for the MDB. This example returns the list of available countries for the service or service option to which the form is attached

```
SELECT country_id,country_name from my_country_table
```

This query does the following:

- "SELECT " specifies which values to return. In this example, it returns the ID and the name of the country in the database.
- "FROM my_country_table" specifies the name of the database table.

2. On the form, add the first select box; it is one of the elements of a form (see page 2916).
    a. For the _id attribute, specify a meaningful value, and save the form. Record the value for later reference when you specify the reportobjvars attribute.
    b. For the value of the HTML Attribute (see page 2928) named reportobjid, specify the id of the data object, and save the form.

Note: When you use a data object to populate a combo box, do not add any options to the select box, because they are ignored (not used) when the user opens the form. Any options for the select box are ignored, only the data object "matters."

3. Create a second report data object to retrieve a list of values from the database, based on the user's selection in the first select box. In this report data object, specify some report variables in the query that are to be filled using the input provided by user in other fields in the form
In our running example, create a second report data object to retrieve the states from the database, based on the country that the user selected. Follow the guidelines in Step 1 to create the second report data object.

4. On the form, add the second select box. This box is to be pre-populated, based on the user's selection for the first select box. Follow the guidelines in Step 2 to create the second select box, but account for the following considerations:
    - The second query contains a report variable and is similar to the following:

      ```
      select state_id,state_name from my_state_table where country_id=%sele
      ```

    - The running example in this topic uses only one report variable (%selected_country%); however, your query may contain multiple report variables.
    - Record the names of all report variables for use when you specify the reportobjvars attribute for the second select box.

5. In the second select box, specify the reportobjvars attribute using the following format:
   $({'reportvar':*value*}).
   A valid *value* is one of the following:

   - A constant, such as 12, as in $({'reportvar':12})
   - A string, such as abc, as in $({'reportvar':'abc'})

     Note: Enclose strings in single quotation marks, as shown. Within a quoted string, if needed, use a backslash (****) as an escape character to specify a literal single quote or apostrophe. For example: $({'what\'s the status?'})

   - A JavaScript expression, such as the user's last name, as in $({'reportvar':_.user.lastName})
   - A JavaScript function of the following form: $({'reportvar':foo()})
   - Combinations of the previous values, delimited with commas, using the format shown in the following example:

     ```
     $({'reportvar':_.user.lastName,'reportvar1':'abc','reportvar2':12,'re
     ```

   In our running example, create a second select box to be populated with the states from the database, based on the country that the user selected. For the reportobjvars attribute of the state select box, specify the pre-defined JavaScript function (see page 2967) named ca_fdGetSelectedOptionValues, as follows:

   ```
   $({'selected_country':ca_fdGetSelectedOptionValues ('<form _id> ','coun
   ```

   - **form _id**
     Specifies the value of the _id attribute of the form containing the first select box. You reference this form in Step 2.
   - **country**
     Specifies the value of the _id attribute of the first select box. You create and record this value in Step 2.

6. In the first select box, set the onchange attribute to retrieve the data for the second select box as soon as the user makes a selection in the first select box. For the onchange attribute, specify the pre-defined JavaScript function named ca_fdFetchSelectData, using the following format:

   ```
   ca_fdFetchSelectData('<form _id>','<state field _id>');
   ```

   - **form _id**
     Specifies the value of the _id attribute of the form containing the second select box. You reference this form in Step 4.
   - **field_id**

Specifies the value of _id attribute of the form containing the second select box. You create and record this value in Step 4.
In our running example, set the onchange attribute for the country select box to the following:

```
ca_fdFetchSelectData('<form _id>','<state field _id>');
```

7. Test the form to verify that it works as you intended.

Use User Input for Personal Data to Pre-Populate a Select Box

You can use the first few characters provided by the user in a select box in a form to trigger an auto-complete function. A common application of this technique occurs on a form with a select box (an element of a form (see page 2916)) for the last name. For example, if the user types the letters *smit*, the field displays all valid options, such as Smittapopolous, Smitderski, Smitapunangala, and so forth. The user can select a valid value but cannot enter a custom value. This technique helps users find and specify valid data efficiently when the database is large.

Follow these steps:

1. In the Report Builder, create a data object (see page 3232) that queries the data source (such as the MDB) for the data you want. The query must return the list of all possible values and populate the select box with this list. This step is part of the process of pre-populating a combo box based on a report data object (see page 2972). For this example, do the following:

   - Create a report data object to retrieve the list of user IDs from the database. When the form appears, the report data object runs and populates the combo box with the resulting data.
   - Record the ID of the data object for later reference.
   - Verify that the variable you want to use exists and is of type *string*. If necessary, create or update the variable. For illustration, we use the last_name_prefix variable in the following example.

   For example, consider the following sample query for a data object for the MDB. This example returns the list of available last names that match the user input in the field.

   ```
   Select userid as id, last_name from ca_contact where last_name like '%la
   ```

   - **Select userid as id, last_name**
     Specifies which values to return. It returns the ID and the last name of all users that match the first few characters entered by the user.
   - **From ca_contact**
     Specifies the name of the database table.
   - **where last_name like '%last_name_prefix%%%'**
     Specifies the filter clause.
     The last_name_prefix variable filters on the last_name column (the display column of the query).
     The 'like '%last_name_prefix%%%' syntax filters the results so that the last_name starts with last_name_prefix.

2. Add the select box to the form.

   Note: When you use a data object to populate a select box, do not add any options to it, because they are ignored (not used). When the user opens the form, any options for the select box are ignored, only the data object is used.

   a. For the _id attribute, specify a meaningful value, and save the form.

   b. (Optional) Rename the default display text from the select group from "Select" to a more meaningful name, as follows: Select the element in the Component Tree and click the Rename icon at the top of the tree.

3. Specify values for the following attributes of the select box, and save the form.

   - Multi-Select: Specify False so that users can select only one option in the combo box.
   - (Optional) Title (tooltip text): Specify instructional text, such as "Click the arrow and scroll to select a last name.

     Note: You can optionally localize (see page 2987) the tooltip text or the name of the select box, if applicable.

4. Specify values for the following attributes of the select box, and save the form.

   - Report/Plug-in Id: Specify the name of the report data object that you created in Step 1.
   - Report/Plug-in Variable: Specify a JSON expression for the object that maps a key value pair, as follows:
     - The key is the variable for the report data object.
     - The value is a JavaScript expression that matches the data you want.

     For this example, specify the following:

     ```
     $({'last_name_prefix':_val})
     ```

     - last_name_prefix is a string constant, as noted in Step 1.
     - _val is a predefined variable that CA Service Catalog provides.
   - Minimum Search Characters: Specify a custom value, for example, 4 or 5. This attribute specifies the number of characters that users must type to trigger the auto-complete feature. The defaults is 4.

5. Test the form to verify that it works as you intended.

Pre-Populate Fields Based on a Report Data Object and JavaScript Functions

To pre-populate fields with data that is not accessible through JavaScript expressions (see page 2957), you can use a report data object (data object), custom JavaScript functions, and pre-defined JavaScript functions (see page 2967), especially ca_reportQuery(reportId, variables, onSuccess, onFailure). A representative case involves querying your organization's Human Resources database (not the CA MDB) for sensitive data, such as the banking account number and related information for a user.

For example, you may create a form for changing the bank account to which a user's pay check is automatically deposited. In this form, you may pre-fill fields with name of the current bank name and account number. Use later fields on the form for the user to enter the name of the new bank name and account number.

First, ca_reportQuery(reportId, variables, onSuccess, onFailure) retrieves from the data object the variables that match the fields queried by the data object. Next, the OnSuccess function is called, at which point you can use other pre-defined JavaScript functions (see page 2967) to pre-populate multiple fields in the form with the results of the query. For example, you may write a custom function that calls ca_fdSetTextFieldValue(formId, _id, text) multiple times, once for each field you want to pre-populate. This scenario is typically most suitable for pre-populating text fields, but can also be used to populate other types of fields.

Follow these steps:

1. Design and create the form (see page 2951), if you have not already done so.

2. In the Report Builder, create a data object (see page 3232) that queries the data source for the data you want (the data to be copied to the matching fields on the form).
   Record the ID of the data object for later reference.
   The following sample query for the MDB matches the example started earlier in this topic:

   ```
   SELECT bank_name,account_number FROM my_hr_db WHERE userid ='%userid%'
   ```

   CA Service Catalog processes this query as follows:

   a. "WHERE userid = '%userid% ’ specifies that a user id must be provided as input to this data object.

   b. "SELECT bank_name,account_number" specifies which values to return.

3. "FROM my_hr_db" specifies that the database is my_hr_db, a fictitious database for illustration.

4. On the form, add text fields (or other suitable form elements instead) to receive the retrieved data, as follows:

   - Add one text field for each variable queried by the data object.
     For the continuing example, add two text fields, one for bank name and one for account number.
     For the continuing example, add two text fields, specify bank_name and account_number, respectively.

- Rename each text field to have a meaningful name.
  For the continuing example, rename the fields to Bank Name and Account Number, respectively.

5. Select the form name to display the form attributes.

6. In the form attributes, in the JavaScript attribute named onload, enter the name of your function that calls ca_reportQuery. For illustration, these steps use getAcctData() as the name for this function. Substitute the name of your function if it is different.

7. Verify that getAcctData() is declared in a JavaScript file accessible by CA Service Catalog.
   For best results, use this location in the filestore: FileStore/scripts/custom_form_lib.js.

   Important! The folder name *FileStore* is case sensitive. Therefore, use the correct case in path names and all other programmatic references.

8. In the body of getAcctData, specify the call to ca_reportQuery function, to run the data object and return the results.

9. Use the results as input values to JavaScript functions such as ca_fdSetTextFieldValue to update the fields in the form.
   In this example, use the results to make two calls: one to update the bank name field and another to update the account number field.

10. Customize ca_reportQuery(reportId, variables, onSuccess, onFailure) to meet your requirements. This step uses the continuing example for illustration.

    - For reportId, specify the data object that you created earlier.

    - For variables, specify the JavaScript map with the variable names and values.
      For the continuing example, specify: {“userid”:_.user.id}.
      These variables *must* match the ones that you query in the data object, but they do not need to be ordered in the same sequence.

    - For onSuccess, specify the custom JavaScript function to run when the query returns successfully. The onSuccess function must take one operand. This operand is set with an array of maps, each representing a row, returned by the query. Within your custom onSuccess function, use ca_fdSetTextFieldValue(formId, _id, text) to return the results of each field, one at a time.
      For the continuing example, specify the following:

```
function updateFields(result) {
   if (result.length == 1) {
   ca_fdSetTextFieldValue(formId, 'bank_name', result[0].['bank_name'

   ca_fdSetTextFieldValue(formId,'account_number',result[0].['account

   } else {
      alert('could not find your bank account information')
   }
}
```

- For onFailure, specify the JavaScript function to run if the query fails.
  For the continuing example, specify the following:

  ```
  function onGetAcctDataFail() { alert("can't find your account");}
  ```

11. Finish creating the form to meet your requirements.

12. Test the form to verify that it works as you intended.

Validate User Input

You can configure Form Designer forms to verify that users entered the following types of data in the correct format: credit card numbers, social security numbers, email addresses, phone numbers, postal (zip) codes, and decimal numbers with two fractional digits.

This process does *not* guarantee that the data entered by the user is authentic but does assist in the validation process by verifying that the user entered the data in the correct format.

You can thus use the Form Designer to verify that the data you want and is recorded in the format that you want. For example, you can verify that phone number fields accept only numeric input, that date fields accept only your company's standard date format, and that credit card fields accept only numbers that are entered in the correct format for the credit card type specified.

Additionally, you can specify maximum length, minimum length, and other attributes used to validate user input.

Choose the task you want to perform:

- Use regular expressions to validate numeric and address data (see page 2980). In this case, you use regular expressions in the HTML attribute (see page 2928) named pattern to validate the format of credit card numbers, social security numbers, email addresses, phone numbers, IP addresses, postal codes, dates, and decimal numbers with two fractional digits.

- Use JavaScript functions to validate the format of credit card numbers. For example, you use the pre-defined JavaScript function (see page 2967) named ca_fdValidateCC(credit card number, credit card type) in a JavaScript attribute (see page 2940) such as onValidate to verify the credit card formats. Alternatively, you can create your own custom JavaScript function.

Use Regular Expressions to Validate Numeric and Address Data

This topic explains how to use regular expressions to configure Form Designer forms to verify that users entered the following types of data in the correct format: credit card numbers, social security numbers, email addresses, IP addresses, phone numbers, postal (zip) codes, and decimal numbers with two fractional digits. .

To verify the types of user input mentioned earlier, follow these steps. These steps use a continuing example for illustration.

1. Design and create the form (see page 2951), if you have not already done so.

2. For each type of user input, add a text field.

3. Rename each text field from Text Field to a meaningful name, such as Social Security Number, Credit Card Number, and so forth.

4. For the value of the HTML Attribute (see page 2928) named pattern, specify the regular expression for the type of data being validated, and save the form. Valid values follow:

   - Social security number: ^([0-6]\d{2}|7[0-6]\d|77[0-2])([\\d{2})\2(\d{4})$
   - Decimal number with two fractional digits: ^[1-9]\d*(\.\d{2})$
   - E-mail address: ^([0-9a-zA-Z]+([_.-]?[0-9a-zA-Z]+)*@[0-9a-zA-Z]+[0-9,a-z,A-Z,.,-]*(.){1}[a-zA-Z]{2,4})+$
   - IP Address: ^((25[0-5]|2[0-4][0-9]|1[0-9]{2}|[0-9]{1,2})\.){3}(25[0-5]|2[0-4][0-9]|1[0-9]{2}|[0-9]{1,2})$
   - Telephone number: ^(([0-9]{1})*[- .(]*([0-9a-zA-Z]{3})*[- .)]*[0-9a-zA-Z]{3}[- .]*[0-9a-zA-Z]{4})+$
   - URL: ^(http[s]?://|ftp://)?(www\.)?[a-zA-Z0-9-\.]+\.(com|org|net|mil|edu|ca|co.uk|com.au|gov)$
   - Postal Code (CAD): ^([A-Z][0-9]){3}$
   - For additional values, or to create your own expression, see your reference for regular expressions, such as www.regular-expressions.info or www.regexlib.com.

5. For the value of the HTML Attribute (see page 2928) named patternMessage, specify an error message to appear when the user input violates the pattern attribute.

   Note: You can optionally localize (see page 2987) this error message.

6. Finish creating the form to meet your requirements.

7. Test the form to verify that it works as you intended.

Use a JavaScript Function to Validate the Format of Credit Card Numbers

This topic explains how to configure Form Designer forms to use a JavaScript function to verify that users entered a credit card number in the correct format for the credit card type that they specified.

This topic explains how to present two credit card types: Master Card and Visa. For each type, you create a radio group option and a text field for the account number. Each account number field is disabled by design but is enabled if the user selects the matching credit card type.

You use the pre-defined JavaScript function (see page 2967) named ca_fdValidateCC(*number*, '*type*') to validate the format of the credit card number entered by the user, based on the credit card type that the user selected. This JavaScript function verifies the format according to the specifications set by the company issuing the credit card. Each company sets its own standard format.

To verify the credit card numbers entered by users, follow these steps. These steps use a continuing example for illustration.

1. Design and create the form (see page 2951), if you have not already done so.

2. Verify that the value of the form's HTML Attribute (see page 2928) named _id specifies a meaningful name, such as ccValdtnForm1.

3. Add a radio group; it is one of the elements of a form (see page 2916).

    a. For the value of the _id attribute of the radio group, specify a meaningful name, such as rgCCVal, and save the form.

    b. Rename "Radio Group" to a meaningful name or phrase, such as Select a Credit Card or Credit Card Type.

4. Add the first radio group option; these options are elements of a form (see page 2916) that apply only to radio groups.

    a. For the _id attribute, specify a meaningful name, such as mcard (signifying Master Card radio group option), and save the form.

    b. Rename "Radio" to a meaningful name, such as Master Card.

5. Add the second radio group option.

    a. For the _id attribute, specify a meaningful name, such as visa (signifying Visa radio group option), and save the form.

    b. Rename "Radio" to a meaningful name, such as Visa.

6. Add a text field onto the form

    a. For the _id attribute, specify a meaningful name, such as ccf.

    b. For the value of the JavaScript attribute (see page 2940) named onvalidate, specify cc_val(_val).

7. Use the Script dialog (see page 2969) to add the following function definition:

```
function cc_val(value) {
                var ccname = '';
                if (ca_fdIsSelectRadio('ccValdtnForm1', 'rgCCVal', 'mca

                                ccname = 'master';
                else
                                ccname = 'visa';
                ca_fdValidateCC(value, ccname);
}
```

    As a best practice, use the Script dialog on each form to create and maintain the custom JavaScript functions for the form.

8. Finish creating the form to meet your requirements.

9. Test the form to verify that it works as you intended.

Link Fields in Two Forms for Simultaneous Updates

You can optionally specify JavaScript functions to link two fields in two Form Designer forms. When a user updates a field in one form, the linked field is updated in the second form simultaneously. This technique essentially creates an automatic cross-reference between the fields in both forms.

Follow these steps:

1. Verify that the forms are in the same service option.

   Important! The forms *must* be in same service option.

2. Decide which fields in which forms you want to link. For example, you may want to ensure that a name, date, item, or phone number field has the same value in both forms in each request.

3. Specify the same exact function in both forms *except* that you switch the form IDs in each JavaScript function, as follows:

   - In the JavaScript function in Form 1, you specify the ID for Form 2.
   - In the JavaScript function in Form 2, you specify the ID for Form 1.
   - For ease of maintenance, use the same field name and same JavaScript attribute in each form.
     For example, you may decide to name the field Address in both forms and specify the JavaScript function in the onclick attribute in each form.

Important! Do *not* re-use either form in a different service. If one of the forms is re-used in a different service, the fields become un-linked. Consequently, both fields function correctly individually but are no longer cross-referenced. Therefore, they are no longer configured for simultaneous updates.

Example

This example illustrates how to use JavaScript functions to link two fields in two Form Designer forms for simultaneous updates.

In Form AA, whose form ID is form_aa, specify the following for the linked field:

- Name: Item Requested
- JavaScript function in the onclick attribute: ca_fdSetTextFieldValue ('form_bb','item_requested','New Laptop')

In Form BB, whose form ID is form_bb, specify the following for the linked field:

- Name: Item Requested
- JavaScript function in the onclick attribute: ca_fdSetTextFieldValue ('form_aa','item_requested','New Laptop')

Administer Forms

This article contains the following topics:

Understand Access Level Rules

Authorized users can access forms. Authorized users are users with the following roles: Super Business Unit Administrator, Catalog Administrator, Service Manager, and Service Delivery Administrator. Here, *access forms* means that the users can view, create, edit, copy, and delete forms, unless noted otherwise.

To configure access rights to forms, configure these Use Service Provider Catalog Only and Pass Through Catalog settings. Accept or change the default settings, as follows:

- By default, the *Use Service Provider Catalog Only* setting is No. Authorized users can access the forms in the current business unit and its child business units *only*. Authorized users can add forms to services and can delete forms from services in the current business unit and its child business units *only*.
  If the *Use Service Provider Catalog Only* is Yes, then authorized users can view and copy forms in the Service Provider business unit. They cannot perform any other actions on these forms. Similarly, authorized users cannot add forms to services and cannot delete forms from services in the Service Provider business unit.

- By default, the *Pass Through Catalog* setting is No. Authorized users can access forms in the current business unit and its child business units *only*. Authorized users can add forms to services and can delete forms from services in the current business unit and its child business units *only*.
  If the *Pass Through Catalog* is Yes, then authorized users can view and copy forms in the parent business unit. They cannot perform any other actions on these forms. Similarly, authorized users cannot add forms to services and cannot delete forms from services in the Service Provider business unit.

- If both the *Use Service Provider Catalog Only* and *Pass Through Catalog* settings are Yes, then the former setting takes precedence. Authorized users can view and copy forms in the Service Provider business unit, but not in any parent business unit. Similarly, authorized users cannot add forms to services and cannot delete forms from services in the Service Provider business unit.

To configure access rights to forms, proceed as follows:

- To configure the *Use Service Provider Catalog Only* setting, log in to the root (highest level) business unit as a Service Delivery administrator. Select Catalog, Configuration, System Configuration.

- To configure the *Pass Through Catalog* setting, log in to the business unit of interest as an authorized user. Select Catalog, Configuration, Catalog Configuration.

Note: Users cannot access forms in sibling business units under any circumstances.

Create and Maintain Forms

You can create forms in the Form Designer.

Follow these steps:

1. Verify that you have administrator rights to each folder that you want to access, in each affected business unit. To copy or move a form from one business unit to another, you must be an administrator in both business units. If you are an administrator in a parent business unit, then you are automatically an administrator in all its children business units.

   Note: You cannot create, copy, move, or delete any forms or elements within the System folder.

2. Use caution when modifying an existing form. If the form is included in an *active* request, you receive a warning message.
   Do *not* update the form (except trivial changes) if you receive this warning message. When you no longer receive this message, proceed with your change. To make important changes to the form, create a new version with the changes and use the new form.

3. Use extreme caution when deleting an existing form or moving an existing form from one business unit to another. If the form is included in an *active* request, you receive a warning message. Do *not* complete the move or delete operation if you receive this warning message. When you no longer receive this message, proceed with your change.

   Important! When you delete a form, all elements under it are also deleted. If you want to save the elements, store them in another form before deleting this form.

4. Click Catalog, Forms.

5. Click the icon next to the Forms folder in the Component Tree.

6. Create the form (see page 2951), if applicable.

7. Click the Associations tab to display the list of service offerings and service option groups that are associated with the selected form. It also provides the ability to view where a particular form has been used in the current Business Unit and also the capability to assess the impact of modifying or deleting a form. This functionality is also available in the Form Chooser UI when attaching a form to a Service Option.

   Note: The Associations tab is available only if you have installed the CA Service Catalog 14.1.01 patch updates available on CA Support.The form level associations are shown only for the selected Business Unit level.

8. Edit a form, as follows:

   a. Open the folder that contains the form you want to edit.

   b. Open the form to display its existing elements.

   c. Add, modify, and configure elements on the form (see page 2951).
   You can rename, move, copy, or delete a form.

      Note: The copied form, including all its elements, now belong to the business unit of the destination folder. The name of the copied form must be unique within the business unit. The form is copied, and its new name is "copy of *original name.*" The copied elements under the copied form are *not* renamed.

(Optional) Create and Maintain Folders

Create and maintain folders to organize your forms according to groups, categories, or business units. For example, you create and name folders that correspond to each business unit, department, owner, or service.

- If you delete a folder, all sub folders, forms, and elements under it are also deleted.
- If you move a folder from one business unit to another, the moved folder now belongs to the business unit of the destination folder. The names of each folder, form, and element must be unique within their new business unit.
- If you copy a folder from one business unit to another, the pasted folder now belongs to the business unit of the destination folder. However, the sub folders, forms, and elements under it are *not* renamed.
- If you want to delete a folder, first delete any sub folders or forms under it.

Import and Export of Forms

You can use the Import Export utility to perform the following tasks:

- Import and export Form Designer forms by themselves, without related services or service option elements.
- Import and export Form Designer forms associated to service option elements.

Localize Forms

You can use the Localization Editor to localize the element names and selected attributes in forms. You can do so for the supported languages.

When you edit the form in the Form Designer, you see localized names and values only if you are using the Localization Editor. However, when a localized form appears in a request, it displays all localized values. If no localized values exist, the form displays the default values for the form name, element names, and selected attributes.

For more information about how to set the Localization Attributes for a Form, see Localize a Single Service (see page 3031) section.

Manage Services

A service consists of hardware, software, or other resources that users request from the catalog. Administrators *manage* services to meet the needs of their users and organization. Here, *manage* means to create or update services, or to perform other tasks to manage services, as explained in the following steps.

Administrators (typically service designers) group one or more service option groups together as a single service. You can create services for several purposes, including requesting hardware or software, on boarding new employees, and reserving physical or virtual resources. You can optionally use Service Accounting Component to specify charges for each service.

You create and maintain services in folders in a service catalog. You make the catalog available either to all business units or only to a specific business unit. You can have multiple catalogs for multiple business units.

1. Verify that you are logged in to the correct business unit. If your role permits, you can change to another business unit to access its catalog instead of the catalog of your current business unit as follows:

    a. Click **Catalog**, **Service Offerings**.
    The Services page appears and displays the folders containing services, organized hierarchically according to category.

    b. Click **Change Business Unit**.
    The **Search Business Units** window appears.

c. Use the Expand and Collapse icons to navigate the business unit tree or search to locate the required business unit.

> **Note:** The list includes only the business units that the role of the user permits.

d. Select the business unit name in the tree.
The window closes and the catalog for that business unit is displayed. You have changed business units.

2. Click Catalog, Service Offerings.

3. Expand the tree and select the folder in which you want to manage services.

4. (Optional) Create a Simple Service (see page 2988).

5. (Optional) Add or Update a Service (see page 2996).
This task optionally includes specifying inheritance, setting featured and related services, and defining dependencies between services.

6. Perform Other Tasks to Manage Services (see page 3004):

   - Setting thresholds for quality-of-service (QoS) SLAs for services
   - Managing the folders that store services

As part of managing services, you Manage Service Option Groups (see page 3011) and Manage Service Options and Service Option Elements (see page 3017). You can also Localize a Single Service (see page 3031) or Localize Multiple Services (see page 3035).

Create a Simple Service

This scenario illustrates how service design managers create a simple service by copying predefined service option groups and forms and customizing the copied objects. Creating a service in this manner is more efficient than creating and configuring the objects that comprise the service. You can use this scenario *as a model* to create a simple service.

This scenario focuses on the onboarding of a new employee into the Field Services group in your organization. For a use case other than new hire onboarding, search the catalog for the service that most closely matches the service that you want to create. For example, to create a service for reserving a virtual machine using Reservation Manager, review services in the Reservation Services folder.

The predefined service in this scenario is a simple, on-premise enterprise service named New Hire Onboarding. You use it to create a similar service for the Field Services group. In this scenario, you optionally configure default options so that users can request the service with little to no effort or input. Creating simple services in this manner reduces user errors and increases efficiency, especially for users submitting requests from mobile devices.

Important! If you already have multiple forms with the same _id value, do not associate such forms to a single Service Option. Having multiple forms with the same _id value in a single Service Option can cause validation errors.

Follow these steps:

Step 1 - Create the Service Option Group for the Form

As a best practice, copy predefined objects and customize the copies, rather than changing predefined objects.

Follow these steps:

1. Click **Catalog**, **Service Offerings**.
2. Click the **Option Group** tab.
3. Select the group **New Hire Onboarding** and perform the following actions:
    a. Click the Copy icon.
    b. Click the Paste icon (*not* the Paste as Inherited icon).
    c. Specify New Hire Onboarding for Field Services Only in the prompt for the name of the new option group.
4. Select the copy of the service option group and perform the following actions:
    a. Click the Definition tab.
    b. Click the Delete icon to delete this form from the service option group.
    This action deletes the form from this service option group *only*. The form still exists in any other service option groups that include it, and in the Form Designer folder.

Step 2 - Review and Copy the Form

All services include at least one predefined or custom form to record and process essential information from the user requesting the service. In this scenario, you review and copy the predefined form included with the standard New Hire Onboarding service. Afterwards, you modify the copied form for use in the New Hire Onboarding for Field Services Only service.

Follow these steps:

1. Copy the New Hire Onboarding form, as follows:
    a. Click **Catalog**, **Forms**.
    b. Expand the **Forms**, **CA Catalog Content** folder in the Component Tree.
    c. Select the **New Hire Onboarding** form.
    d. Click the Copy icon.
2. Select the top level of the Forms folder and complete these actions:
    a. Click Add and create a subfolder named Custom.
    b. Select the Custom folder and click Paste.
    The new form appears; its name includes the "copy of" prefix. The copied elements under the copied form are *not* renamed.

    > **Note:** When you copy the form from one business unit to another, the pasted form, including all elements under it, belong to the business unit of the destination folder.

    c. Select the form and click Rename.
    d. Enter the new name as New Hire Onboarding for Field Services Only. Click OK. The name must be unique within its business unit.

Step 3 - Modify the Form

Modify the form that you copied by adding a unique field for Field Services.

Follow these steps:

1. Expand the New Hire Onboarding for Field Services Only form.
2. Copy the Additional Info field, as follows:
    a. Select the Additional Info field in the tree, and click the Copy icon. The Copy icon appears near the top left of the screen, in the row of form tools under the main menu and tab names.
    b. Select the name of the New Hire Onboarding for Field Services Only form in the tree. Click Paste.
    c. Enter a unique ID (for example, field_services_group_id) in the _id field in the right pane.

d. Click Save.

3. Rename the new field, as follows:

   a. Select the field and click Rename.

   b. Enter the new name as Field Services Group ID. Click OK.

The new field is renamed. The Field Services managers can use this field to assign new employees to a group in the organization.

Step 4 - Add the Form to the Service Option Group

Add the new, modified form to the New Hire Onboarding for Field Services Only service option group. Later, you add this service option group to the New Hire Onboarding for Field Services service.

Follow these steps:

1. Click **Catalog**, **Service Offerings**.

2. Click the **Options Group** tab.

3. Select the group named New Hire Onboarding for Field Services Only. Perform the following actions:

   a. Click the Definition tab.

   b. Click **Add Option**.
   The Service Option Details tab appears and lists the service option elements in the group.

   c. Enter a meaningful name for the service option. Example: New Hire Onboarding Form for Field Services Only.

4. Scroll to the Form field and click Add.

5. Complete the fields in the Service Option Element Definition, as follows:

   a. Specify meaningful text In the Display Text field. Describe the purpose of this form. This text appears to the user as a description for the form when administrators view this service option group in the catalog.

   b. Click the Search icon in the Form Name field.

   c. Navigate through this form tree and select the New Hire Onboarding for Field Services Only form.

   d. Click the Select Form button.

6. Click Update.
   The Service Option Element Definition dialog closes. You return to the Service Option Details tab.

7. Scroll to the bottom of the tab and click Save.

8. Scroll to the top of the tab and click Return to Service Option Group.

Step 5 - Create the Service and Customize the Details

You create a service to contain one or more service option groups. Specify the details of how and when catalog users can request the service. In this scenario, you create and configure a service to contain the service option group that you created previously (New Hire Onboarding for Field Services Only).

Follow these steps:

1. Click **Catalog**, **Service Offerings**.

2. Expand the **Personnel Services** folder in the tree and select the **New Hire Onboarding** service.

3. Click the Definition tab to view the service option groups. In this scenario, you use the same service option groups in your new service.

4. Select the **Personnel Services** folder, and click **Add**, **Offering**.

5. Enter the name of the new service as New Hire Onboarding for Field Services Only.

6. Complete the following fields on the Details tab of the new service, and click Save:

   - For Description, specify Onboards new employees in the Field Services group.

   - Complete the fields in the Availability section, and click Save.
     The service becomes visible and users can request it only on the date that you specify in the Available On field.

7. Complete the following fields as shown, and click Save:

   - For User Request Method, verify that One-Click Submit is selected.
     This setting lets users request the service quickly, without using a cart. This setting is ideal for simple services.

   - Select the option named Available from mobile device.

   - For the Approval Process drop-down list, either select No Approval or verify your selection with the catalog administrator. Catalog administrators typically configure either the Workflow driven approval process or the Policy driven approval process.

   - Accept the default values for the other fields.

8. Click the **Definition** tab, and perform the following actions:

   a. Click the Edit icon for the Overview field.

   b. Specify the following (or similar) text for the Overview, and click the Save icon:
      For onboarding new employees in the Field Services group only

Step 6 - Add and Customize the Service Option Groups

You can add several service option groups for onboarding Field staff. As you add each group, if applicable, you customize it for the Field staff by including only the deluxe option.

Note: The customizations in these steps affect this service *only*. You do not modify the service option groups or their service options. Instead, you customize this service to include only the service options that you select from each service option group.

Follow these steps:

1. Click the Edit Offering Selection button on the Definition tab for the New Hire Onboarding for Field Only service.
2. Scroll to the service option group named Business Cards. Perform the following actions:
    a. Click the Include checkbox.
    b. Select Order Business Cards - Embossed, and select the options for Include and Default. Leave both options *unchecked* for the service option named Order Business Cards - Standard.

    This action adds embossed business cards to the service and includes them by default.
3. Scroll to the service option group named Mobile Phone, and perform these actions:
    a. Click the Include checkbox.
    b. Select Mobile Phone- Deluxe, and select the option for Default.

    This action adds a deluxe mobile phone to the service and includes it by default.
4. Scroll to the service option group named Mobile Phone Accessories, and perform these actions:
    a. Click the Include checkbox.
    b. Select all the options for Include and Default.

    This action adds all mobile phone accessories to the service and includes them by default.
5. Scroll to the service option group named New Hire Onboarding for Field Services Only, and perform these actions:
    a. Click the Include checkbox.
    b. Select the options for Include and Default.

    This action adds the form that you created earlier to the service and includes it by default.

6. Scroll to the service option group named Procure Laptop, and perform these actions:

    a. Click the Include checkbox.

    b. Select Laptop - Deluxe, and select the options for Include and Default.

    This action adds a deluxe laptop to the service and includes it by default.

7. Scroll to the bottom of the dialog and click Save.
   The Catalog system adds the service option groups to the service, with your customizations.

Step 7 - Specify Automatically Chosen Selections

You can specify the service option groups that you added to the service as automatically selected (default). This technique helps to verify that Field Services personnel can see and request all required equipment efficiently, especially from mobile devices.

Follow these steps:

1. Perform the following actions on the Definition tab for the New Hire Onboarding for Field Only service:

    a. Click the Edit icon for the first service option group, Business Cards.

    > **Note:** When you mouse-over this Edit icon, the help text is "Edit Service Option Group." Other Edit icons for the header text and for the service option also appear near this Edit icon, but each one has different help text when you mouse over it.

    The Details tab for the service option group appears.

    b. Specify Automatically Chosen as the Selection Type. Click Save.
    This service option group is automatically included when the service is requested or subscribed to. This service option group contains one service option, embossed business cards. The embossed business cards option is automatically selected for Field Services staff, and is the only option for them.

    c. Click the Back button on the browser to return to the Details tab for the service.

    d. Click the Definition tab for the service.
    You return to the Definition tab for the New Hire Onboarding for Field Only service. The list of service option groups in the service appears.

2. Perform the following actions:

    a. Click the Edit icon for the next service option group, Mobile Phone.

b. Specify Automatically Chosen as the Selection Type. Click Save.
This service option group is automatically included when the service is requested or subscribed to. This service option group contains one service option, the deluxe mobile phone. The deluxe mobile phone option is automatically selected for Field Services staff, and is the only option for them.

c. Click the Back button on the browser to return to the Details tab for the service.

d. Click the Definition tab for the service.
You return to the list of service option groups on the Definition tab.

3. Use the previous steps as a model to edit the definitions for the following service option groups and to specify Automatically Chosen as the Selection Type:

   - Mobile Phone Accessories
   - New Hire Onboarding for Field Services Only
   - Procure Laptop

   These service option groups also contain a single, deluxe service option that is automatically included for Field Services staff.

Step 8 - Set the Permissions

You can optionally set the permissions for the service so that only specified roles or groups can request it. If a role or group has permission to access the service, the associated users can perform the following actions.

- View the service in the catalog.
- View, request, and subscribe to the service
- Access the service through searches and web service calls

Conversely, if a role or group does not have permission to access the service, the associated users do not have these rights.

Follow these steps:

1. Click the **Permissions** tab of the service named New Hire Onboarding for Field Only.
2. Clear the check box named **Grant All Access to All Roles in All Business Units**.
3. Select the Request/Subscribe box for Catalog User, and click Save.
This selection lets all Field staff request this service. In this scenario, all Field staff have the catalog user role. In your organization, another role may be more suitable.

Note: You can optionally define a user group for Field staff in CA EEM and use the Groups tab to restrict the permissions for the service to that group.

Add or Update Services

This article contains the following topics:

Service designers create or update services. They do so by grouping service option groups together as a single service that users can request from the catalog.

Follow these steps:

1. Click Catalog, Service Offerings.
2. Expand the tree and select the folder in which you want to manage services.

   Note: To add a folder at the top level (root folder), click Add and name the new folder.

3. Perform one of the following actions in the selected folder:
   - Create a service by clicking Add and naming the new service.
   - Edit a service by selecting it and updating its fields.
4. Complete the fields on the Details tab (see page 2997) for the service.

   Note: This step and the remaining steps apply *only* if you are adding or updating a service.

5. Define the service (see page 3001).
6. Click the Permissions tab, and set permissions for the service.
   Each role and group (if applicable) receives the access rights that you specify to the new service.
   Only if a role or group has permission to access the folder, the associated users can perform the following actions:
   - View the service in the catalog.
   - View, request, and subscribe to the service.

- Access this service through searches and web service calls.

7. (Optional) Click the Related Offerings tab, and perform the following tasks:
   - Review Service and folder inheritance (see page 3002). Specify other services to inherit (include) with this service.
   - Define dependencies (see page 3005) for this service, if applicable.
8. (Optional) Set Featured and Related Services (see page 3003).

Service Details Tab

When you add or edit a service, you complete the fields on the Details tab for the service.

The following fields on the Details tab for a service require explanation.

- **Image**
  Assigns an image to a service.
  To select the new image from the USM_HOME\FileStore\images\offerings folder, click the existing image.

  Important! The folder name *FileStore* is case-sensitive. Therefore, use the correct case in path names and all other programmatic references.

  The recommended size for an image is no larger than 48 x 48 pixels. However, the size of an image for a featured service is fixed at 32 x 32 pixels. So, the image is reduced or enlarged to 32 x 32 pixels, regardless of its original size.
  If you make this service a featured service, verify that the image is legible when viewed at 32 x 32 pixels. If you add images to several services in the same folder, verify that the sizes of the images are compatible. Verify that the images blend together to form a balanced layout that aligns with the Featured Item header.

- **Service ID**
  (read-only) Specifies the object ID of the service.

  Note: As part of importing or exporting objects using IXUtil or content packs, you specify the Service ID explicitly.

- **Name *and* Description fields**
  Specifies the name and description of the service for catalog users. You can optionally localize these fields for use in a multilingual catalog.

- **Code**
  Specifies the text value to represent the product code, subscription code, SKU number, or any other applicable value.

- **URL Info**
  Specifies an external URL for more information about the service. For example, a service for a new laptop can include the URL to the manufacturer specifications page for the laptop.

- **Date fields**
  The dates and times that you view and specify are based on the time zone on the CA Service Catalog server. These values can be different from your local time zone.
  The dates that you enter in any of the following fields affect the availability of the service to catalog users:

  - Available On
  - Unavailable After
  - Canceled After fields

  The changes that you make to these fields take effect immediately.
  The following date fields require further explanation:

  - **Unavailable After**
    Specifies the date when catalog users can *no longer* request or subscribe to the service.
  - **Canceled After**
    Specifies the cancellation date for all requests for this service and all accounts with subscriptions to this service.
    On this date, these subscriptions and requests are canceled. Requests and subscriptions that are in progress are canceled immediately.

- **Business Hour**
  Specifies the business hours for the service. The business hours are the regularly scheduled days and times of service. For example, Monday-Friday, 9:00 am to 5:00 pm. Business hours apply only when you use request SLAs to help measure the availability of a service.

- **Outage Calendar**
  Specifies the outage calendar for the service. The outage calendar specifies days, dates, and times when the service is not available. For example, weekends, holidays, and one-time outages. Outage calendars apply only when you use request SLAs to help measure the availability of a service.

- **User Request Method**
  Specifies whether users request the service by using the one-click submit method or by using a shopping cart.

  - **One-Click Submit**
    Allows users to request the service, using one click, without a shopping cart. This method submits a stand-alone request for the service.
    The one-click submit method is appropriate for the internal business and personnel services that are *not* related to shopping. Examples: Services for onboarding new employees and for setting up or accessing virtual computers.
    When you use this method for a service, users cannot include it in the same request as other services.

- **Shopping Cart**
  Allows users to request this service by adding it to a shopping cart. The cart can include multiple services. The user finishes shopping, verifies the cart, and submits it. This method is appropriate for services that are related to internet shopping, typically procurement requests. Example: Requests for new hardware or software.
  A catalog user who has added services to a shopping cart without submitting it can request a one-click submit service. The request for the one-click submit service is submitted immediately as a separate stand-alone request. The shopping cart is not affected.

- **Available from mobile devices**
  Enable the checkbox to raise a service request from the mobile application.

- **Display SOG Name**

  Note: This capability is available only if you have installed the CA Service Catalog 14.1.01 patch updates available on CA Support.

  Check or uncheck the checkbox to hide or display the Service Option Group name that has single or multiple options associated in an offering. This option is enabled only when you have a single Service Option Group in an offering. In case of multiple service option groups in an offering, this option is disabled or greyed out by default. Checking or unchecking this option will not alter the offering Preview.

- **Approval Process**
  Specifies the approval process to use for the service when a user requests it. This Approval Process setting does *not* apply to subscriptions.
  Select *one* of the following options:

  - **System approval process**
    To determine whether the request for a service requires further approval, the System approval process uses the following options:

    - The authorization level of the user requesting the service
    - The approval level of the service

    If the authorization level of the user is less than the approval level of the service, the request requires further approval. In that case, the Catalog system performs the following tasks:

    - Assigns the manager of the user to approve the request
    - Places the request in the Requests Pending Action queue of that manager

    This process repeats until the authorization level of the approver is at least equal to the approval level for the service.

  - **No approval process**
    Approves the service automatically.

- **Workflow Driven Approval Process**
  Uses a CA Process Automation process to determine the approval process.
  The process includes the business logic to determine the approver and the number of approval levels. CA Service Catalog provides sample processes for a single level of manager approval.
  For any service, if you use this approval process with a CA Process Automation process, you can optionally use policies. In that case, the approval process proceeds the same as with Policy driven approval process, except as follows:

  - The Workflow driven approval process uses the CA Process Automation workflow engine to evaluate and implement policies.

  - Policy driven approval process uses the Catalog Policy Engine to evaluate and implement policies. This option is typically more efficient for an approval process that uses policies, because this engine is internal.

  Verify that the rules and actions are enabled (see page) for the option that you specify.

- **Policy driven approval process**
  Uses policies to determine the approval process for requests. In policies, you specify conditions that are based on the attributes of service options, services, requested items, and users. If a policy is active and a submitted request meets the condition in the policy, then the following event occurs: The assignees in the policy receive a request pending action to approve, reject, or fulfill a service option, service, or request. Policy driven approval and system approval use a few common terms. Example: The *level of approval* refers to the authority of an approver in numeric terms. The higher the number, the greater the authority of the approver. However, in policy driven approval, the administrator assigns each approver and authority level uniquely, with no relation to system approval. If a policy does not apply to a request, the Catalog system uses the approval flow that is defined in the workflow driven approval process. Example: You are using the predefined workflow approval process and no predefined sample policy applies to a request pending action. In that case, the Catalog system assigns the request pending action to the manager of the Requested For user. If the user has no manager, then the system assigns the request pending action to the Default User for Request Actions. This user is specified in the Request Management Configuration.

- **Approval Level**
  Specifies the approver Authorization Level that is required for the service. Specify these values logically and consistently to verify proper approval operations in your organization. This setting applies *only* if you specify System approval process or Workflow driven approval process in the Approval Process field.

- **Status on Approval**
  Specifies the status of the request items in the service once the service is approved. Select *one* of the following options:

  - Fulfilled

  - Pending Fulfillment.
    Using Pending Fulfillment enables you to specify workflow processes that assign any additional tasks to fulfill the request, if necessary.

This setting applies *only* if you specify System approval process or No approval process in the Approval Process field.

- **Sort By**
  Arranges the service option groups to appear to the user according to the category you select. Categories include Name, Selection Type, Code, Date Created, and None. You can also select Custom - use Sort Number. This option uses the Sort Number field in the service option group details.

- **Sort Number**
  Sorts the service according to the value you specify.
  This field applies *only* when the parent folder uses a value of Custom - use Sort Number in the Sort By field.

Define a Service

After you create a service, define it. *Defining* a service primarily means adding one or more service option groups and specifying which service options to include.

Follow these steps:

1. Click Catalog, Service Offerings.
2. Expand the tree and display the service of interest and click the Definition tab.
3. Click Edit Offering Selection.
   - If no service option groups are already associated with this service, all service option groups appear.
     To add service options from a group to a service, select the group, expand it. Select the service options that you want to include.
   - If one or more service option groups are already associated with this service, the service options from those groups appear.
     - Expand the associated service option groups and select or remove service options for this service.
     - Click Show All to display all service option groups. Select the group that you want, and include the service options that you want in the service.
   - Verify that you have completed the following actions, as applicable:
     - Select the service options that are included in the service *by default*. To do so, select the check box for the service option in the Default column.
     - Select the service options that are *required* in the service. To do so, select the check box for the service option in the Include column.
     - Exclude any groups or service options that you do *not* want in the service.
4. Save your changes and close the Service Offering Selection dialog.

You can set thresholds for QoS SLAs for request fulfillment reports. You can also set permissions as part of managing the service.

Service and Folder Inheritance

You can configure the inheritance folders and services, as follows:

- Inherit folders and services from the catalog of one business unit to the catalog of another business unit.
- Inherit folders and services from one part of the catalog hierarchy to another.
- Copy a service or folder and paste it as inherited.

After you create the inherited folder or service, you can update both the parent and child (inherited) objects. The following tables list:

- The changes to the parent that the child inherits
- The changes to either the parent or child that break inheritance

Parent Object	Change	Change Inherited?	Breaks Inheritance?
Folder or Service	Update settings on the Details tab	Y*	N
Folder	Add subfolders or services	N	N
Folder or Service	Delete services or subfolders--Not permitted directly. To delete the service or subfolder, first break the inheritance by deleting the inherited service or subfolder. You can also break inheritance for a service by editing or deleting an inherited service option group or service option.	N	N
Service Option Group	Update settings on the Details tab	N	N
Service Option Group	Add a service option	N	N
Service Option Group	Delete a service option--Not permitted directly. To delete the service option, first break the inheritance by editing or deleting the inherited service option.	N	N
Service Option	Update a service option element**	Y	N
Service Option	Add a service option element	N	N
Service Option	Delete a service option element	N	N

*Your updates in the parent folder override any existing values (including any custom values) in the child folder. The only exceptions are as follows:

- For child folders, the folder name is not changed.
- For child services, the service name, dates, and status are not changed.

** A service option element is a part of a service option. Examples include forms, reservations, and rate elements. Service option elements appear as fields on the Service Option Details tab. When you update these fields, the Service Option Element dialog opens.

Child Object	Change	Breaks Inheritance?
Folder or Service	Update settings on the Details tab	Y or N*
Folder	Add subfolders or services	N
Folder	Delete subfolders or services	N
Service Option Group	Update settings on the Details tab	N
Service Option Group	Add a service option	N
Service Option Group	Delete a service option	N
Service Option	Update a service option element	Y**
Service Option	Add a service option element	Y**
Service Option	Delete a service option element	Y**

* For child folders, you can change the name without breaking inheritance. For child services, you can change the name, dates, and status without breaking inheritance. Any other change breaks inheritance of the folder or service details *only*. Inheritance of service options and service option elements is not broken.

** The inheritance of the service option is broken. Inheritance of the folder and service details remains.

Note: Inheritance applies only to the changes listed in the tables.

Set Featured and Related Services

For folders, you can specify *featured* services. Similarly, for services, you can specify *related* services. These specifications are helpful when the user viewing a service or folder considers requesting a featured or related service. **Example:** When you create an "onboarding" service for new employees, you can specify services for laptops and cell phones as related services. When new employees access the onboarding service in the catalog, they see summaries and links for these related services.

Follow these steps:

1. Click Catalog, Service Offerings.

2. Expand the tree. Perform one of the following actions for the service or folder of interest:
   - Select the folder and click the Featured Offerings tab.
   - Select the service and click the Related Offerings tab.
3. Expand the Catalog Tree and specify one or more services, as follows:
   a. On the left side of the tree, select the box next to the service name.
   b. Next to the Selected Offerings box, click the right arrow to add the selected service to the box.
   c. (Optional) Include the children (inherited services) with the featured service. You can specify this setting individually for each featured service.
4. Verify and save your updates.
5. Verify that the catalog is configured to display related services, as follows:
   a. Select Catalog, Configuration, Request Management Configuration.
   b. For the Browse Catalog Layout option, specify Request View.
   c. For the *Access Control: Show General Information* option, specify the roles that you want to see featured services.
   d. For the *Access Control: Show General Information* and *Selections in Catalog Item Details* option, specify the same roles that you specified in the previous step.

Perform Other Tasks to Manage Services

This article contains the following topics:

Administrators (typically service designers) can copy, cut and paste, delete, and cancel services. They can use a service as a template. Administrators can also manage the folders that store services, define dependencies, and set thresholds for quality-of-service (QoS) SLAs.

Perform or skip any of the following tasks, as needed.

1. Use a service as a template (see page 3006).
2. Copy a service *with or without* inheritance (see page 3002), as follows:

a. Select the service and click Copy.

b. Specify which *one* of the following options you want to include in the copy:

- All associated service option groups (preferred)
- Only the service, *without* the service option groups (primarily for backward compatibility with earlier releases of the product)

c. Expand the tree and select the folder to which you want to paste the copied service.

d. Click the Paste icon or the Paste as Inherited icon.
The folder (and its child folders and services) or service is pasted to the new location. The inherited services are named "Inherited from *parent service*." When the parent service is updated, the same updates occur in the child service automatically.

3. Cut and paste a service, as follows: Select the service and click Cut. Expand the tree to the new location and click Paste.

4. Delete a service by selecting it and clicking the Delete icon. Before you confirm the deletion, review the effects of deleting a service (see page 3007).

> **Important!** Deletion is permanent.

5. Cancel a service by selecting it and setting the Canceled After field on the Details tab. Before you confirm the cancellation, review the effects of deleting a service (see page 3007). Canceling a service has the same effects as deleting a service on the related subscriptions and requests.

6. Review thresholds for QoS SLAs (see page 3008) and set (see page 3009) them.

7. Manage the folders (see page 3009) that store services in the catalog.

Define Service Dependencies

A dependency in the catalog allows a service state to change depending on the state of another service. You can also set the availability of a service to a user based on the business unit of that user.

The ability to define dependencies of services allows you to define how one service behaves based on how you select or clear another service. For example, if you are subscribing to Service A, the following events can occur for Service B:

- Service B can become disabled. The selection check box is inactive and cannot be selected or cleared.
- Service B can become subscribed to. The check box displays selection whether it is enabled or disabled.
- Service B can become unsubscribed to. The check box is cleared whether it is enabled or disabled.

Follow these steps:

1. Click Catalog, Service Offerings.
2. Click Change Business Unit, if necessary, and select the business unit whose service dependencies you want to define.
3. Click Define Dependencies.
4. Select one of the following options, and click Save Dependency.
   - **Business Unit to Service Assignment**
     Specifies which services appear in the catalog of the child business unit.
   - **Service to Business Unit Assignment**
     Specifies which services appear in the catalog of the child business unit.
   - **Subscribe Services**
     Specifies which services are included automatically in a subscription to another service. When a user subscribes to the selected service, the Catalog system subscribes the user to the services that you specify.
   - **Un-subscribe Services**
     Specifies which subscribed services are canceled automatically with the cancelation of another service. When a user cancels the selected service, the Catalog system cancels the subscription (of this user) to the services that you specify.
   - **Disable Services**
     Specifies which services are made *unavailable* (disabled) automatically as a result of a subscription to another service. When a user subscribes to the selected service, the Catalog system disables (for this user) the services that you specify.
5. Click the Close icon.

Use a Service as a Template

You can create a service to use as a template for creating all services in your catalog. Creating a template service helps ensure that all services in your catalog have a consistent look-and-feel. To create a template service, follow this process:

1. Add a service, using the following guidelines:
   - Include the word "template" in the name.
   - Mark the service as unavailable by setting the Unavailable After date to the current date.
   - Select the service option groups that you want to be in the template service.
2. Inform other administrators about the template service. Tell them to follow the remaining steps to use it to add a new service:
   a. Copy and paste the template service to an appropriate "holding" folder.

b. Rename the service each time that you copy it to a different folder.

c. Add new service option groups to the service, if necessary.

d. Remove existing service option groups from the service, if necessary.

3. Perform one of the following steps to modify a service option group in a service that is created from your template service:

   - To apply your changes to all services that use the service option group, edit the service option group definition directly.
   - To apply your changes only to the new service that you are creating from the template service:

     a. Copy and rename the service option group.

     b. Modify the new service option group as required.

     c. Add the new service option group to your new service.

     d. Remove the original service option group from the service.

   Note: When you copy a service, specify whether the new service includes copies of the original service option groups or links to them. If you specify links, any changes to a linked service option group apply to all services that include it. That is, the original service, the new service that you copied, and any other service in the Catalog system that includes the link.

4. Define a service option element in a service option group, or update it, if necessary.

Effects of Deleting a Service

Deleting folders or services affects the subscriptions and requests for the deleted services, as follows:

- **Subscriptions**
  The account that is subscribed to the service being deleted no longer contains or lists that service.
- **Requests**
  The status of requested service options for the account change that is based on their original status, as follows:

Original Status	New Status
Not Submitted	The service is deleted from the request.
Submitted. An approval status, a fulfillment status, Pending Resource Assignment, or Resource Assignment	The service and its service options are set to Cancelled.
Completed	

Original Status	New Status
	The default cancellation status (Pending Cancelation or Cancel) if Service Accounting Component is installed. Cancelled if Service Accounting Component is not installed.
Pending Cancelation or Canceled	Same as original status.

Thresholds for QoS SLAs

Request Service Level Agreements (SLAs) are a feature of CA Service Catalog. Quality of Service (QoS) SLAs are available only if CA Service Catalog is integrated with CA Business Service Insight.

You can establish thresholds for QoS SLAs for use with Request Fulfillment reports. An SLA threshold specifies the following data:

- Starting status
- Ending status
- Duration (days, hours, and minutes) for warning status
- Duration for a violation status

If the request for the service option takes longer than the SLA duration, then the request reaches a warning or violation status.

The Request Fulfillment reports use the SLA threshold specification. By default, the report includes the following phases:

- The approval phase
- The fulfillment phase
- The combination of approval and fulfillment phases

The following table shows summary data for these items:

Starting Status	Numeric Value	Ending Status	Numeric Value
Submitted	200	Approval Done	999
Approval Done	999	Completed	2
Submitted	200	Completed	2

You can also configure the reports to display the following data:

- The time for the status of a service option to move from the starting to the ending phase.
- The average time in each phase.
- The violation time for the SLA phases.

- The color code of warnings and violations for the service options for which SLA thresholds have been set.

If you report on different SLA thresholds, alter the STATUS_RANGES values for the Request Fulfillment reports.

The SLA violation duration for the Submitted to Completed phase is used for the “estimated time to fulfill” value. This value appears in the catalog in the “fulfillment details” for a service option.

Set Thresholds for QoS SLAs

You can establish thresholds for QoS SLAs for use with Request Fulfillment reports. Doing so is an optional task when you define a service.

Follow these steps:

1. Select Catalog, Services Offerings.
2. Expand the tree, locate the service of interest, and click its Definition tab.
3. Select the service option of interest and click its SLA icon.
4. Click Add, specify the following parameters for the new SLA, and click OK:
   - The starting status
   - The ending status
   - The warning and violation thresholds

Manage Folders

Services exist in a folder structure. You can *manage* the predefined folder structure to meet your needs. *Manage* here means create, copy, delete, and move.

Follow these steps:

1. Click Catalog, Service Offerings.
2. Expand the tree and select the folder of interest.

   Note: To add a folder at the top level (root folder), click Add and name the new folder.

3. Perform one of the following steps in the selected folder:
   - Copy a folder *with or without* inheritance (see page 3002), as follows:
     Select the folder and click Copy.
     Specify which *one* of the following you want to include in the copy:

- All associated service option groups
- Links to these service option groups

Expand the tree and select the folder to which you want to paste the copied folder.
Click the Paste icon or the Paste as Inherited icon.
The folder (and its child folders and services) or service is pasted to the new location.
Inherited folders are named "Inherited from *parent folder*." When the parent folders or services are updated, the same updates occur in the child folders or services automatically.

- Delete a folder by selecting it and clicking the Delete icon.

Important! Deletion is permanent. Deleted folders *cannot* be recovered.

Deleting the folder deletes all services in it. Before you confirm the deletion, review the effects of deleting a service (see page 3007).
Do one of the following actions *if* the folder that you want to delete contains inherited services.

- Delete the child, inherited service.
- Break the inheritance by editing the child, inherited service.

4. Complete the fields on the Details tab (see page 3011) for the folder.

Note: This step and the remaining steps apply only if you are creating or updating a folder.

5. Click the Permissions tab, and set permissions for the folder.
   Each role and group (if applicable) receives the access rights that you specify to the new folder.
   Only if a role or group has permission to access the folder, the associated users can perform the following actions:
   - View the folders and its subfolders in the catalog.
   - View, request, and subscribe to the services in the folder and its subfolders.
   - Access this folder, its subfolders, and associated services through searches and web service calls
6. (Optional) Review featured services (see page 3003). Specify any services in this folder to feature in the catalog.
   (Optional) Review service and folder inheritance (see page 3002). Specify other services to inherit with this folder.

Details Tab for a Folder

When you add or edit a folder, you complete the fields on the Folder Details tab.

The following fields on the Folder Details tab require explanation.

- **URL**
  Specifies a URL that supplies more information about the services in the folder. For example, a URL to a manufacturer web site.

- **Display Subfolders**
  Specifies whether the top-level subfolders under this catalog folder appear in the Browse section of the Requests page. Select *one* of the following options:

  - **Use System Setting**
    Use the system or "global" setting to show or hide the subfolders that are specified in the Browse Catalog: Show Subfolders parameter in the Request Management Configuration section of the Configuration page of the Catalog tab.
    If the value of the Browse Catalog: Show Subfolders parameter changes, all catalog folders that use the system setting are automatically updated accordingly.

  - **Show Subfolder**
    Specifies that this catalog folder *always* displays its subfolders in the Browse section of the Requests page, regardless of the value of the system setting.

  - **Hide Subfolder**
    Specifies that this catalog folder *never* displays its subfolders in the Browse section of the Requests page, regardless of the value of the system setting.
    Hiding these subfolders is often helpful when the number of them is so high that the following condition exists: Users must scroll through the Browse Catalog several times to view them all or to see the remaining folders and subfolders

Default: Use System Setting

Manage Service Option Groups

This article contains the following topics:

Administrators (typically service designers) create, update, and otherwise manage service option groups, which are the main components of services. Here, *manage* means create, update, copy, edit, delete, and so forth. A service option group consists of hardware, software, or other resources that you can include in a service. Service option groups are bundled groups of service options (see page 3017). Each service option consists of individual service option elements. You can use the same service option group in multiple services. Each business unit can have its own set of service option groups.

Follow this process:

1. Click Catalog, Service Offerings.
2. Click the Option Groups tab and perform one of the following actions:
   - View the details (see page 3013) of a service option group by selecting it.
   - Edit a service option group by selecting it and updating its fields. Go to the next step.
   - Create a service option group by clicking the + sign below the Option groups tab and name it. The details page for the new service option group appears. Go to the next step.
   - Copy a service option group *with or without* inheritance (see page 3015), as follows:
     a. Select the service option group in the tree and click Copy.
     b. Specify a unique name for the new service option group.
     c. Click the Paste icon or the Paste as Inherited icon.
     On the service option group tree, the inherited options appear in green.
   - Delete a service option group by selecting it and clicking the Delete icon. Before you confirm the deletion, review the effects of deleting a service option group (see page 3016).

     Important! Deletion is permanent. Deleted service option groups *cannot* be recovered.

     Perform one of the following actions *if* the service option group that you want to delete contains inherited service option groups. Otherwise, skip to the next step.
     - Delete the child, inherited service option group.
     - Break the inheritance by editing the child, inherited service option group. You cannot delete a folder or service that contains inherited service option groups.
3. Complete the fields on the Details Tab for the service option group.

   Note: This step and the remaining steps apply only if you are adding or updating a service option group.

4. You can optionally use a tiered service option group (see page 3014).
5. Define the service option group by clicking the Definition tab and performing one of the following actions:
   - Create service options and add them to the group.
   - Edit a service option in the group.

- Delete a service option from the group.
- Copy a service option in the group, with or without inheritance.
- Organize the service options in the group.

After you define the service option group, you can add it to services that users can request from the catalog.

6. Publish a report layout (see page 3016) for a service option group.
7. Associate a CA APM model with a service option, if you have integrated with CA APM.

Service Option Group Details Tab

The following fields on the Details tab for a service option group require explanation:

- **Id**
  (Read-only) Specifies the object ID of the service option group. At times, you specify object IDs explicitly. For example, as part of importing or exporting objects using IXUtil or content packs.

- **Date fields**
  The dates and times that you view and specify are based on the time zone of the CA Service Catalog server, which can be different from your local time zone.
  The following date fields require further explanation:

  - **Available On**
    Specifies the date when this service option group becomes available for catalog administrators to include in a service when they define the service. The change that you make to this field take effect immediately.

  - **Unavailable After**
    Specifies the date when catalog users can *no longer* request or subscribe to the service option group. Catalog administrators can no longer include this service option group in a service when they define the service. The change that you make to this field take effect immediately.

- **Name *and* Description fields**
  Specify the name and description of the service option group for catalog users. You can optionally localize these fields for use in a multilingual catalog.

- **Type**
  Specifies the type of service option group. This value determines how you can include this service option group within other service option groups as a characteristic of a service option element. Select one of the following options:

  - Fixed - A fixed service option group presumes a fixed cost or a variable cost that is based on usage.

  - Tiered - A tiered service option group (see page 3014) presumes a variable cost value.

  Default: Fixed

- **Selection Type**
  Specifies how catalog users select the options in the service option group while requesting a service that includes the service option group.

- **Code**
  Specifies a text value for a code of your choice. Examples include the product code, subscription code, and SKU number.

- **Sort Number**
  Specifies how to sort this service option group when a service that includes it uses a Sort By setting of Custom - use Sort Number.

- **Offering Dependencies**
  Specifies the names and statuses (for example, Available) of the services that include this service option group.

- **Account Dependencies**
  Specifies the following data:

  - The names of the accounts that are subscribed to services that include this service option group. The accounts subscribe to the service option group by subscribing to the service.

  - The names and statuses of the services to which these accounts are subscribed.

Tiered Service Option Group

A tier is a single row in a tiered service option group. You can use a tiered service option group to produce a variable cost according to a lookup value. The lookup value from the referencing service option group is matched with the tier values in the tiered service option group.

An association into a tiered service option group starts at the first row and works its way down: The first tier has the lowest tier values. When an applicable tier is identified and the Quantity Specification is set to System Specified, this event occurs: The lookup value is multiplied by the rates in other service option elements in the tier row to determine the invoice amount. If the Quantity Specification is not set to System Specified, other rates apply.

When a service option element is associated with a tiered service option group, the tier type value determines how the tiered service option group is used. The following tier types are available, depending on the referencing service option element:

- **Lookup**
  Use the first tier that matches the value being passed to the tiered service option group.

- **Lookup Multiple**
  Use each tier that matches the value being passed to the tiered service option group.

- **Variable Lookup**
  Use each tier up to and including the tier that exactly matches the value being passed to the tiered service option group.

- **Fixed**
  Use the first tier that matches the value being passed to the tiered service option group. Once in that tier the tier is fixed and cannot change.

- **Fixed Incremental**
  Use the first tier that matches the value being passed to the tiered service option group. Increment to the next tier only if the value passed in exceeds the previously used tier. That is, a certain tier level is used; a lower tier level can never be used.

- **Variable Fixed**
  Is a merger between variable lookup and fixed tier types. Use each tier up to and including the tier that exactly matches the value being passed to the tiered service option group. Once in the tier that exactly matches, that tier is fixed and cannot change.

- **Variable Fixed Incremental**
  Is a merger between variable lookup and fixed incremental. Use each tier up to and including the tier that exactly matches the value being passed to the tiered service option group. Increment to the next tier only if the value passed in exceeds the previously used tier.

Inheritance of Service Option Groups

You can copy a service option group and paste it as an inherited service option group. The inherited service option group has the same characteristics as the parent service option group from which it was created. The Catalog system shows the inheritance in the inherited service option group, as follows:

- On the Details tab, a note indicates that the service options in this group are inherited.
- On the Definition tab, the inherited service options appear in green.
- If you click the Edit icon of an inherited service option, the Service Option Details tab includes the following information:
  - Text that the option is inherited.
  - A link to the parent service option.
- If you click the Edit icon of an inherited service option element on the Service Option Details tab, the resulting dialog includes:
  - Text that the service option element is inherited.
  - The ID of the parent service option element.

The following rules apply to the inheritance relationship:

- If you update a service option element in the parent service option group, the Catalog system automatically makes the same updates to the inherited service option element in the child service option group. The updated values of the parent replace the existing values in the child.
- If you make either of the following updates to the parent service option, the updates do not apply to the child service option:

- Adding a service option element
- Deleting a service option element

- If you make either of the following updates to the child service option, you break the inheritance relationship. If this relationship breaks, then changes to the parent no longer propagate automatically to the child.
  - Adding a service option element
  - Deleting a service option element
  - Editing a service option element

When you manually update an inherited service option element, the green color disappears. The color disappearance indicates that the element was changed after it was inherited.

Effects of Deleting a Service Option Group

Deleting a service option group affects the subscriptions and requests for the deleted service option groups, as follows:

- **Subscriptions**
  The account that is subscribed to the service option group being deleted no longer contains or lists that service option group.

- **Requests**
  The statuses of requested service options in the service option group being deleted change, as follows:

Original Status	New Status
Not Submitted	The service option group and its service options are deleted from the request.
Submitted. An approval status, a fulfillment status, Pending Resource Assignment, or Resource Assignment	The service option group and its service options are set to Canceled.
Completed	The default cancellation status (Pending Cancellation or Cancel) if Service Accounting Component is installed. Cancelled if Service Accounting Component is not installed.
Pending Cancellation or Canceled	Same as original status.

Publish a Report Layout

You can publish a report layout that appears as a service option in a special service option group. This service option group is created the first time that a report is published. This service option group is named *Published Reports*. You can manage it as you manage other service option groups.

Follow these steps:

1. Select Administration, Report Builder, Layouts.

2. Expand the folders and select the report of interest.

3. Click the Publish Layout to the Catalog icon in the Actions column.
   A new service option for the report layout is added to the Published Reports service option group. The new service option has a default cost of 0.
   The service option representing the published report contains the following data:

   - Two Text type service option elements that display the report name and comment values.
   - A Rate Type service option element that holds the report cost.

   You can edit this service option and can include it in services.

Note: You can remove a published report from the catalog, as follows: De-select the service option from a service that includes it, or remove the service option from the service option group.

Manage Service Options and Service Option Elements

This article contains the following topics:

Administrators (typically service designers) create, update, and otherwise manage service options, which are the building blocks of a service option group. A service option group must contain at least one service option. Similarly, each service option contains one or more service option elements.

Each service option element adds value to the service. Examples include an item that the user can request or a function to complete the request lifecycle. Examples include these elements:

- A form element provides a form that the user completes to customize the request and to obtain fulfillment.
- A rate element provides billing specifications for a service option.
- A reservation element helps provide required data in a service for reserving physical or virtual computers.

Service option elements can have the following characteristics:

- **Static**
  Provides fixed information about the service option.

- **Actionable**
  Specifies that a request, service, or service option follows a specific approval process, fulfillment process, or both.

- **Financial**
  Specifies fixed, tiered, or usage-based rates. You can optionally link these rates to budget and planning functions.

You create, edit, and delete service options as part of managing service option groups.

When you create or edit a service option, you complete the fields on the following tabs, as applicable:

- Policies & Actions (see page 3018)
- Options (see page 3019)
- Details (see page 3021)

After you finish creating a service option, click the Preview tab to see how it appears to users in the catalog. If necessary, update the service option after you preview it to achieve the results you want.

Policies and Actions Tab

You create *global* policies and global actions for general use with any service. In contrast, you create *attached* policies and actions for use with one or more specific service options only. You attach these policies and actions to each service option individually. You can create an attached policy or action *only* from the Policies & Actions tab of that service option. After you create an attached policy or action for that service option, you can optionally attach that policy or action to another service option. However, you cannot change an attached policy or action into a global policy or action. Similarly, you cannot change a global policy or action into an attached policy or action.

Note: On the Policies and Actions tab, you can use the link to access CA Process Automation.

By default, CA Service Catalog evaluates all global policies and all events, rules, and actions (see page 3040) (global actions only) for every requested *service*. However, for individual service options, you can replace this default behavior. From the Policies & Actions tab of a service option, you can specify that the Catalog system apply the following specifications to that service option:

- For policies, one of the following options:
  - Global policies only
  - Attached policies only

- Both global and attached policies

- For actions, one of the following options:
  - Global actions only
  - Attached actions only
  - Both global and attached actions

Important! Applying policies or actions at both the service and service option levels could produce conflicting, unintended, or unpredictable results. Use attached actions and policies *only* if you are using a discrete request life cycle (see page 2120) that includes discrete approval of service options. This precaution helps avoid the unintended application of policies and actions at *both* the service and service option levels.

Service Option Element Options Window--Options Tab

Several fields appear on the Options tab of the Service Option Element Definition dialog. These fields apply to all service option elements.

- **Change to Take Effect**
  Applies *only* if the Catalog Configuration item named **Default Effect of Service Option Element Changes** is set to *Allow User to Choose*. For more information about Catalog Configuration settings, see the Catalog Configuration (see page 1449) section.
  If applicable, this option appears when you create or update service options in a service option group that is already defined in a service (see page 3001). The setting for this field applies to *all* updates that you make to other fields on this tab.
  Select an option from the following list and specify when the changes take effect for existing subscribers or requesters:
  - **Beginning of Accounts' Current Billing Period - No Audit Trail**
    The change takes effect retroactively to the beginning of the current billing period for existing subscribers or requesters.
  - **Beginning of Accounts' Current Billing Period**
    The change takes effect retroactively to the beginning of the current billing period for existing subscribers or requesters.
  - **Beginning of Accounts' Next Billing Period**
    The change takes effect at to the beginning of the next billing period for existing subscribers or requesters.
  - **Immediately during Accounts' Billing Period**
    The change takes effect immediately for existing subscribers or requesters.
  - **Specify a Future Effective Date**
    The change takes effect for existing subscribers or requesters on the date specified.

- **Code**
  Specifies user-specified text value to represent the product code, subscription code, SKU # or any other applicable code.

- **URL Info**
  Displays a clickable URL with the service option element to the requesting or subscribing user.

- **Display Type**
  Specifies how the service option element appears in the request, subscription, and invoice (if Service Accounting Component is installed). This setting allows you to hide the service option element from view in special cases. Select an option from the following list:

  - Include in Request/Subscription and Invoice
  - Include in Request/Subscription, Exclude from Invoice
  - Exclude from Request/Subscription and Invoice

- **Include in services (offerings)**
  Applies only when you create a service option element in a service option that belongs to a service option group that is already defined in a service (see page 3001). In other words, one or more services already include this service option group.
  Select from the following list:

  - **Do not include**
    Specifies that the new service option element is not included in any existing (defined) services. However, newly defined services that include this service option do include the new service option element.

  - **That have this service option**
    Updates all existing services that include this service option to include the new service option element.
    The updated service definition includes the new service option element.

  - **That have this Service Option Group**
    Updates all existing services that include this service option group to include the new service option element, as follows:
    Did the original service definition include the service option that you updated by adding the new service option element?
    If yes, the updated service definition includes the new service option element in that service option.
    If no, the updated service definition includes a new service option that contains only the new service option element.

  If you select the second or third option, the following subscription (see page 3120) prompt appears
  Select from the following list:

  - **Do not subscribe**
    The new service option element is not included in any existing subscriptions.
    However, new subscriptions for this service that include this service option do include the new service option element.

- **That have this service option**
  Updates all existing subscriptions for services that include this service option to include the new service option element.

- **That have this Service Option Group**
  Updates all existing subscriptions for services that include this service option group to include the new service option element, as follows:
  Did the original service definition include the service option that you updated by adding the new service option element?
  If yes, the updated subscription to the service includes the new service option element in that service option.
  If no, the updated subscription to the service includes a new service option that contains only the new service option element.

Service Option Details Tab

Use this tab to add the service option elements that you want to this service option.

To add an element, click the Add icon and supply the following data. To update an element, click the Edit icon and update the following data.

- Fields that apply to all service option elements (see page 3019)

- Fields that apply to the element only.

Basic Information

- **Name *and* Description fields**
  Specify the name and description of the service option for catalog users. You can optionally localize these fields for use in a multilingual catalog.

- **Attachment Mandatory**
  Requires the user requesting the service to add an attachment for this service option. If the user does not add the attachment, the user cannot submit the request. Use this option to collect documents (such as certifications or proof of identity) or data that you cannot collect in a form. If selected, this option is activated *only* when the Allow Attachments at Service Option Level parameter is set to Yes. To set this parameter, select Catalog, Configuration, and click Request Management Configuration.

Reservation

- **Reservation Service Option**
  Associates a Reservation Manager reservation of a physical or virtual resource.
  This option and the related fields apply *only* if Reservation Manager or an external reservation system is installed and integrated with CA Service Catalog. The related fields are as follows: Reservation Display Text, Operation, Reservation Ready Status, Reservation Failure Status, and Reservation System

Form

- **Form**
  Associates the form or forms that you select with this service option. In the catalog, the form appears under the service option. Users complete the form when they request this service option.

This form is a service option element within this service option.
Complete the fields for Form Designer form elements (see page 3025).
You can create, customize, and use forms (see page 2950) with the Form Designer (the preferred method).

Contract

- **CA Business Service Insight Contract**
  Associates a CA Business Service Insight service level agreement (SLA).
  This option applies only if CA Business Service Insight is installed and integrated with CA Service Catalog.

Categorization

- **Category**
  Specifies the major category of the service option element from a list of categories.
  The Category value helps determine which rule actions execute approval and fulfillment business processes for a request for a service including this service option element.
  In addition, this value is used to determine the asset type for assigning an asset.
  If CA APM is installed and you select Track as an Asset, the following option applies: You can use the CA APM Assign Asset dialog to associate a request item with a software asset or other type of asset.

- **Category Class**
  Specifies a value from the list to categorize the class of this element within the selected category.

- **Category Subclass**
  Specifies a value from the list to categorize the subclass of this element within the selected class.

- **Keywords**
  Specifies a list of comma-separated list of keywords that are referenced during a catalog search.

- **External ID**
  A user-specified text value to represent the product code, subscription code, SKU # or any other applicable code.

- **Track as an Asset**
  Identifies whether the service option element is eligible to be associated with an asset.
  If CA APM is installed and you select Track as an Asset, the following option applies: You can use the CA APM Assign Asset dialog to associate a request item with a software asset or other type of asset.

- **Information Service Option Only**
  Indicates that this service option is for information only and cannot be subscribed to or requested.

Cost & Pricing

- **Rate**
  Associates a rate (price or cost) service option element with this service option. This price or cost is fixed; it is *not* based on application usage.
  Complete the fields for rate elements (see page 3025).

- **Adjustment**
  Adjusts the charge of an associated service option element. It can be a fixed value or a specified multiplier of the value of the associated service option element.
  Complete the fields for adjustment elements (see page 3029).

- **Usage Based Price**
  Specifies the charges for a service option or other item according to usage.
  Complete the fields for usage based costs elements (see page 3029).

Additional Elements

- **Text**
  Specifies the text and optional image file that appear to users when they select the associated service option.
  An example text string follows: Estimate: one week to complete the request. A sample image file is a detailed photograph of the item being ordered.
  You can optionally upload an image file and specify a text value for the image.

  - **Associate Service Option Group**
    Indicates that a service option group is associated with this service option element.
    Select this field to display a list of tiered service option groups. Associate a service option group and tier type.

  - **Rich Display Text**
    Converts the Display Text field to a rich text field, so that you can add images and special formatting to the Display Text field.
    The recommended size for a Service Option Element image is no larger than 48 x 48 pixels.

  - **Information Service Option Only**
    (Read-only) This field is automatically assigned the same value as the Information Service Option Only field on the Service Option Details tab.

- **Numerics**
  Specifies either a fixed numeric value or a numeric value that is entered by the user requesting the service that contains this service option element.
  Complete the fields for numeric elements (see page 3030).

- **Booleans**
  Specifies a true or false value.
  Note that some fields apply only if Service Accounting Component is installed.

  - **Display Text**
    Specifies the additional text that appears for this service option element.

  - **Boolean Value**
    Determines the value of the service option element. Select from: False or True.

  - **Associate Service Option Group**
    Indicates that a service option group is associated with this service option element.
    Select this field to display a list of tiered service option groups. Associate a service option group and tier type.

- **Date**
  Specifies the date values used with a service option.

  - **Date Type**
    Specifies the type of date. Select from the following list:

    - Specify Value - The Administrator specifies the date value that appears in the catalog. This setting displays the following field:

    - Date Value: The date value for the catalog.

    - Subscription Date - The system sets this value to the date of the request or subscription.

    - Invoice Date - The system sets this value to the date of the invoice if Service Accounting Component is installed.

  - **Associate Service Option Group**
    Specifies that a service option group is associated with this service option element.
    Select this field to display a list of tiered service option groups. Associate a service option group and tier type.

- **Day of Billing**
  Similar to a rate element but also allows a day of the week for weekly charges or a day of the month for monthly charges.
  A Day of Billing element specifies one of the following options:

  - For weekly charges: the day of the week on which to bill the item

  - For monthly charges: the day of the month on which to bill the item

  This element applies only if Service Accounting Component is installed.
  Most of the fields for a Day of Billing element have the same meaning as the fields for rate elements (see page 3025).

- **Numeric Range**
  Specifies a numeric range entered by the user requesting the service that contains this service option element.
  This element applies to tiered service option groups (see page 3014)*only*.
  Complete the fields for numeric range elements (see page 3031).

- **Date Range**
  Specifies a date entered by the user requesting the service that contains this service option element.
  This element applies to tiered service option groups (see page 3014)*only*.

  - **Lower Bound**
    Specifies the numeric value of the lower bound for matches when this service option group is referenced.

  - **Upper Bound**
    Specifies the numeric value of the upper bound for matches when this service option group is referenced.

- **Infinite Upper Bound**
  Specifies that the Catalog system uses this service option element for matches when the lookup value exceeds the value of the lower bound.

Fields for Form Elements

- **Display Text**
  Specifies the descriptive text to display for this form to administrators browsing the list of forms.

- **Form Name**
  Specifies the name of the Form Designer form that you want to define as a service option element for this service. Use the Search icon to view the list of forms and select one.

- **Hidden and Disabled fields**
  If you do not want to hide or disable the entire form under any conditions, leave the Hidden and Disabled fields empty.
  If you do want to hide or disable the entire form, enter the corresponding JavaScript expression in the Hidden or Disabled field. You can hide or disable the form according to the request status, the user role or business unit, or other criteria. Use the following format: $(_.object.property). The expression must return a value of true or false.
  You can specify JavaScript expressions (see page 2957) in the Hidden field, the Disabled field, or both. Examples follow:

  - To hide or disable the form when the request status is Pending Approval, enter the following JavaScript expression in the Hidden or Disabled field: $(_.request.status == 400).
  - To hide or disable the form for the end user roles only, enter $(_.user.role == ‘enduser’).
  - To hide or disable the form from all business units except ca.com, enter $(_.bu.id != ‘ca.com’).
  - To disable the form when the request status is Fulfilled, enter $(_.request.status == 2000).

  When an entire form is disabled, it is disabled but visible during all stages of the request lifecycle. The exception is checkout, when the form is both disabled and hidden.

- **Display Form Name**

  Note: This capability is available only if you have installed the CA Service Catalog 14.1.01 patch updates available on CA Support.

  Check or uncheck to show or hide the Form name. The **Display Form Name** option is also dependent on the System Configuration settings. If the administrator has disabled the form name display option at the System Configuration level, the form name is not displayed, even if the the **Form Name Display** option is checked.

Fields for Rate Elements

- **Cost Type**
  Specifies the type of cost for the Service Option Element. Select from the following list:

- **Specify Value**
  The Administrator specifies the cost value that appears in the catalog and the requesting or subscribing user cannot change the value.
  This setting displays the following field:
  - Unit Cost: The cost value that is to appear in the catalog.
- **User Specified**
  The Administrator specifies the default cost value that appears in the catalog. The requesting or subscribing user can change the value.
  This setting displays the following fields:
  - Default Unit Cost: The default cost value that is to appear in the catalog.
- **Allocate Cost**
  The cost is determined by using values that are associated to a Set as established in Accounting, Budgeting, and Planning worksheets. This setting applies only if you have Service Accounting Component installed.
  This setting displays the following fields:
  - Default Unit Cost: This value in this field is set to 0, as the cost is determined from the worksheet value for the associated set with the selected Allocation Method.
  - Set: List of Accounting Budgeting and Planning sets available for this cost type.
  - Allocation Method: The list of possible methods of allocating the cost that is tied to the service option element.
  - Assign: Use the value in the set for the total cost of this service option element for every subscription or request.
  - Distribute by Subscribed Account: Use the value in the set for this service option element that is divided by the number of accounts that are subscribed to this service option element.
  - Distribute by Subscription: Use the value in the set for this service option element that is divided by the number of subscriptions to this Service Option Element.
  - Weighted Distribution: Use the value in the set for this service option element that is allocated according to actual usage by the account.
- **Standard Cost**
  The unit cost is determined by pulling values that are associated to a Set value as established in Budgeting and Planning worksheets. This setting applies only if Service Accounting Component is installed.
  This setting displays the following fields:
  - Default Unit Cost: This value in this field is set to 0, as the cost is determined from the worksheet value for the associated set with the selected Allocation Method.
  - Set: List of Accounting Budgeting and Planning sets available for this cost type.

- Allocation Method: The list of possible methods of allocating the unit cost that is tied to the service option element.

- Assign: Use the value in the set for the unit cost of this service option element.

- **Display Unit Type**
  Specifies a text value that appears with the cost value.

- **Charge Type**
  Indicates whether cost value must appear as a Charge or a Credit on an Accounting invoice.

- **Budget**
  Indicates whether the service option element appears in the Budget and Planning worksheet.
  If Service Accounting Component is not installed, this field serves as additional categorization for the service option element.

- **Billing Cycle**
  Indicates how the cost value is applied to an invoice if Service Accounting Component is installed.
  Select from the following list:

  - One-Time - The charge is applied one time.

  - Installments - Cost is applied on an installment plan.
    This setting displays the following fields:

    - Periodic Type: The type of interval to be used when applying the cost: Daily, Weekly, Monthly, or N/A.

    - Periodic Type Interval: The frequency of the interval in Periodic Type field for determining the billing interval of the cost.

    - Number of Installments: The number of times the cost must be applied before no longer applying the cost.

  - **Periodic**
    This setting displays the following fields:

    - Periodic Type: The type of interval to be used when applying the cost: Daily, Weekly, Monthly, or N/A.

    - Periodic Type Interval: The frequency of the interval in Periodic Type field for determining the billing interval of the cost.

- **Quantity Specification**
  Indicates how a quantity value must be applied. Select from the following list:

  - **Flat Rate**
    The cost is applied as a flat rate without alteration.
    This setting displays the following fields:

    - Default Quantity Value: The multiplier for the cost value.

- **Specify Quantity**
  The cost is multiplied by the value in the Quantity field.
  This setting displays the following fields:
  - Quantity: The multiplier for the cost value.
  - Show Quantity: Indicates whether the Quantity value must be shown in the catalog.
- **Lookup Admin Specified Quantity**
  The cost is applied according to an associated service option group.
  This setting displays the following fields:
  - Service Option Group: Displays the associated service option group from the list of tiered Service Option Groups in the list or None.
  - Service Option Element: List of service option elements in the tiered service option group which must be associated with this service option element.
  - Show Quantity: Indicates whether the Quantity value must be shown in the catalog.
- **Lookup User Specified Quantity**
  The cost is applied according to a service option element in a service.
  This setting displays the following fields:
  - Service: List of services or None.
  - Service Option Group: List of service option groups for the selected service in the list or None.
  - Service Option Element: List of service option elements in the selected service option group which must be associated with this service option element.
  - Show Quantity: Indicates whether the Quantity value must be shown in the catalog.
- **User Specified**
  The cost is multiplied by the value in the quantity field.
  This setting displays the following fields:
  - Default Quantity Value: The multiplier for the cost value. The user can set this value.
  - Show Quantity: Indicates whether the Quantity value must be shown in the catalog.
- **System Specified**
  The Catalog system applies the cost based on a usage quantity.
- **Form Specified**
  The Catalog system applies the cost based on a form field.
  If you select this option, complete the additional related fields that appear for the related form.
  The Charge Effective From Form Field provides the date field on the form that specifies when billing starts.

Fields for Adjustment Elements

Note that some fields apply only if Service Accounting Component is installed. Adjustments appear on Accounting invoices.

- **Adjustment Value**
  Displays the numeric value of the adjustment to the Accounting invoice.

- **Charge Type**
  Indicates whether cost value must appear as a Charge or a Credit on an Accounting invoice.

- **Adjustment Type**
  Indicates how the Adjustment Value is applied to an invoice if Service Accounting Component is installed. Select from the following list:

  - Applied Amount - The actual amount of the associated service option element is applied.

  - Multiplier - A multiplier of the associated service option element is applied.

- **Service**
  Specifies the service to which the adjustment applies.

- **Service Option Group**
  Specifies the service option group (of the selected service) to which the adjustment applies.

- **Service Option Element**
  Specifies the service option element (of the selected service option group) to which the adjustment applies.

Usage Based Costs Element Fields

Note that some fields apply only if Service Accounting Component is installed.

- **Pricing Structure**
  Specifies the method of charging for a selected application. Select from the following list:

  - **Subscription Based**
    The cost is based on a pre-defined fixed rate. This setting structure displays the following fields:

    - Cost Type: The cost type that must be used to apply the cost of this service option element. This field has the same effect as the Cost Type field on the rate element: Depending on the Cost Type selected, additional fields appear.

    - Display Unit Type: Text value that appears with the cost value

    - Charge Type: Indicates whether cost value must appear as a Charge or a Credit on an Accounting invoice.

  - **Tier Based**
    The cost is derived from an associated tiered service option group according to a lookup value. This setting displays the following fields:

- Service Option Group: The list of tiered service option groups, allowing the Administrator to select an associated service option group.
- Tier Type: The list of available tier types for the selected service option group.

The options that appear in tier type drop-down have the same meaning as the options for tiered service option groups (see page 3014).

- **Usage Based**
  The cost is based on the usage information from data mediation.

  Note: For Service Accounting Component to assign costs correctly, the fiscal period of the Budgeting and Planning Set that is used and the account Billing Cycle must be aligned. For example, if monthly fiscal periods are defined in the set, the billing cycles of associated accounts must also be set to monthly. The Period Start and Period End dates for the Accounting Profile must be aligned. The period start date and period end dates for the account period must have an end date one day later than the fiscal period end date.

  This setting displays the following fields:

  - Cost Type: The cost type that must be used to apply the cost of this service option element. This field has the same effect as the Cost Type field on the rate element: Depending on the Cost Type selected, additional fields appear.
  - Display Unit Type: Text value that appears with the cost value
  - Charge Type: Indicates whether cost value must appear as a Charge or a Credit on an Accounting invoice.

- Show Metric Result
  Shows the metric results on an Accounting invoice and provides a link to a report representing this data.
- Application
  The list of available applications appears in the list.
- Metric
  The list of metrics available for the selected Application is shown.

Fields for Numeric Elements

- **Numeric Specification**
  Specifies whether the subscriber or requester can change the numeric value of the service option element. Select from the following list:

  - Specify Value - The Administrator sets the value of the service option element. This setting displays the following field:
    Numeric Value: The numeric value of the service option element.

- User Specified - The Administrator sets the default value of the service option element which the subscribing or requesting user can change. This setting displays the following field:
  Default Value: The default numeric value of the service option element.

- **Show Numeric Value**
  Determines whether the value of the service option element is shown to the user.

- **Associate Service Option Group**
  Indicates that a service option group is associated with this service option element.
  Select this field to display a list of tiered service option groups. Associate a service option group and tier type.

Fields for Numeric Range Elements

- **Lower Bound**
  Specifies the numeric value of the lower bound for matches when this service option group is referenced.

- **Upper Bound**
  Specifies the numeric value of the upper bound for matches when this service option group is referenced.

- **Infinite Upper Bound**
  Specifies that the Catalog system uses this service option element for matches when the lookup value exceeds the value of the lower bound.

- **Specify Median**
  Exposes the following field:

  - **Median Value**
    Specifies that when determining the tier to be used, the value to compare is the lookup value from the usage data. The value of the multiplier for any rate elements for the tier is the absolute value of the difference between the lookup value and the median value.

Localize a Single Service

Service Managers can specify localization attributes to make a single service available in multiple languages. The service appears in the catalog with localized names, descriptions, and forms. This feature lets a multilingual organization maintain one service in a single catalog for *all* supported languages. Multiple versions of a service or multiple catalogs are *not* required.

For efficiency, localize your *custom* services *only.* CA Service Catalog automatically localizes the predefined services when you install a language pack for a localized language. For example, after you install the French language pack, the predefined services appear in the catalog in French if you set your browser language to French.

Follow these steps:

- Step 1 - Review the Best Practices and Limitations (see page 3032)
- Step 2 - Set the Localization Attributes for the Folder (see page 3033)
- Step 3 - Set the Localization Attributes for the Service (see page 3033)
- Step 4 - Set the Localization Attributes for the Service Option Group (see page 3034)

Step 1 - Review the Best Practices and Limitations

The following best practices apply when you localize a single service:

- Before you localize services and the following related objects, verify that they are completed in the original language:
  - Service option groups
  - Service options
  - Service option elements
  - Forms (if applicable)
  - Folders
- If you update these objects in the original language after you localize them, update the localization attributes accordingly. Otherwise, your catalog could contain localized services and related objects that do not completely match the original-language versions.
- You can copy or inherit a service that includes localization attributes. But, the copied or inherited service retains the localization attributes of the original service.

To make a service available in the catalog, define the service as you define a service without localization attributes.

The following limitations apply when you localize a single service:

- Once all the fields are localized the localized values are seen in end user view only, in Request page. In Service Designer page the definition remains in original language itself.
- Only the fields that you localize appear in the local language in the catalog.
- You can set *one* currency unit (for example, dollars) that applies to *all* local languages.
- You can localize attributes *only* for the languages in which CA Service Catalog is localized for this release.

Note: You can optionally replace the default icon at *USM_HOME* \view\webapps\usm\images\localization_16.png with another icon.

Step 2 - Set the Localization Attributes for the Folder

After you set the Folder attributes, they appear in the local language when users view the folder in the catalog.

Follow these steps:

1. Click Catalog, Service Offerings. Expand the folders and open the folder that you want to localize.
2. Click the Localization icon  for the Name field and specify the text.
3. Save your changes and close the Localization Values dialog.
4. Click the Localization icon for the Description field and specify the text
5. Save your changes to the folder.

You have set the localization attributes for the folder.

Step 3 - Set the Localization Attributes for the Service

After you set the Service attributes, they appear in the local language when users view the service in the catalog.

Follow these steps:

1. Click Catalog, Service Offerings. Expand the folders and open the service that you want to localize.
2. Click the Localization icon  for the Name field and specify the text.
3. Save your changes and close the Localization Values dialog.
4. Click the Localization icon  for the Description field and specify the text.
5. Save your changes and close the Localization Values dialog.
6. (Optional) Click the Definition tab to see the Overview text. Click the Localization icon  , specify localized overview text in the Localization Values dialog, and save your changes.
7. Save your changes on the Overview dialog.

You have set the localization attributes for the service.

Step 4 - Set the Localization Attributes for the Service Option Group

To set the Service Option Group attributes, click the Localization icon for the Name field and Description fields of the Service Option Group you want to localize. Provide the information and save your changes.

Next, you set the localization elements for its service options and its service option elements, including forms.

Step 5 - Set the Localization Attributes for the Service Option

To set the Service Option attributes, click the Localization icon for the Name field and Description fields of the Service Option you want to localize. The Description field includes several options for rich text, including pictures, links, colors, formatting, and highlighting. You can optionally use these options for any language, including all languages on the Localization Values dialog.

You have set the localization attributes for the service options.

Step 6 - Set the Localization Attributes for the Form

You use the Form Designer to create and localize custom forms: You can localize the element names and selected attributes in forms, using the Localization Editor.

While editing the form in the Form Designer, you see localized names and values only when you are using the Localization Editor. However, when a localized form is used in a request, it displays all localized values. If no localized values exist, the form displays the default values for the selected attributes.

Localized system forms are applied *automatically* when you install the CA Service Catalog language pack for your language.

Follow these steps:

1. Select the form name in the Component Tree and click the Localize button.

2. Select a language from the Language drop-down list. Specify local values for the following attributes, for each element in the Localization Editor. Some attributes do not apply to all elements. When an attribute does not apply to an element, the attribute is omitted. *Only* the following attributes can be localized.

   - **Empty Text**
     Provides more description of a field to the user.
     The value that you specify for this attribute appears inside the field when the user opens the form. This text disappears when the user begins entering a value in the field. A sample value follows, for a password field: AAbb1234

   - **Hint**
     Specifies text to help users complete the field correctly. This text *always* appears below the field, regardless of the position of the mouse.
     For example, for a password field, you can specify the following hint: "Passwords must be six to eight characters and must include both letters and numbers."

- **Label**
  Specifies the name of the element. This text is used as the name of the field when the user displays the form in a request. For example, you can specify Name, Address, City, or State.

- **Pattern Message**
  Applies to text fields and text areas *only*, and only when the HTML attribute (see page 2928 named pattern is also used.
  Specifies the error message to appear when the user input violates the *pattern* attribute. In the value for the pattern attribute, you specify regular expressions to validate numeric and address data (see page 2980). Examples include credit card numbers, social security numbers, email addresses, IP addresses, and telephone numbers.

- **Tool Tip**
  Specifies the Tool Tip text, if applicable. Only certain elements use this attribute.

- **Value**
  Specifies the value of the element; this text is the default value for the field when the user displays the form in a request.
  For example, you can leave the value blank for an element whose name (label) is Name or Address, because each user must specify a custom value.

3. Click Save after you enter a localized value.

4. Continue specifying local values for attributes.

You have set the localization attributes for forms.

Step 7 - Test the Localized Services

To verify that the localized services appear as intended in the catalog**,** set your Web browser to the localized language and access the localized services in the catalog. Ensure that the localized elements and attributes appear correctly in folders and services, including its forms.

Localize Multiple Services

Service Managers can localize multiple service offerings (services), including forms, to be available in the catalog in multiple languages. You use IXUtil commands, a localization properties file, and a localization agency. This process lets a multilingual organization maintain one service in a single catalog for *all* supported languages. Multiple versions of a service or multiple catalogs are *not* required.

For efficiency, localize your *custom* services *only.* CA Service Catalog automatically localizes the predefined services when you install a language pack for a localized language. For example, consider the predefined services that appear in English when you install CA Service Catalog. After you install the French language pack, these predefined services appear in the French catalog if your browser language is set to French.

Follow these steps:

- Step 1 - Review the Best Practices and Considerations (see page 3036)
- Step 2 - Export the Services and Forms to an XML File (see page 3036)
- Step 3 - Send the Default Localization Properties File to the Localization Agency (see page 3038)

Step 1 - Review the Best Practices and Considerations

The following best practices apply when you localize multiple services:

- Before you localize services and the following related objects, verify that they are completed in the original language:
  - Service option groups
  - Service options
  - Service option elements
  - Forms (if applicable)
  - Folders
- After you export these objects to an XML file, (see page) make only critical updates to the objects. Otherwise, your catalog can contain localized services and related objects that do not completely match the original-language versions. When you merge the completed localization properties files (see page), any existing objects with the same IDs are overwritten. Thus, any changes that you make to these objects using the UI are also overwritten.

  Important! If you update these objects, apply the updates again after you merge the completed file.
- You can copy or inherit a service that includes localization attributes. But the copied or inherited service retains the localization attributes of the original service.

To make a service available in the catalog, define the service as you define for a service without localization attributes.

The following considerations apply when you localize multiple services:

- Fields appear with localized attributes in the catalog only. In all other components of the product, for example, in Catalog Component, fields appear in the original language.
- You can set *one* currency unit (for example, dollars) that applies to *all* local languages.
- You can localize attributes *only* for the languages in which CA Service Catalog is localized for this release.

Step 2 - Export the Services and Forms to an XML File

The export creates both the XML file and a default localization properties file. The default localization properties file includes the attributes of the exported objects, for the default (original) language *only*.

Follow these steps:

1. Open a CA Service Catalog command prompt.

2. Navigate to the *USM_HOME*\scripts folder.

3. (If you have access to the Catalog system and you are working individually)

   Enter the following command to export services and related data to an XML file. The XML file includes all services that you specified and the objects that comprise the services. This command also extracts the default translatable strings from the XML file into a default localization properties file.
   To export services *with* forms, use the following command:

   ```
   ixutil export service  - f filename.xml -include_forms -include_translation
   object-specific parameters
   ```

   To export services *only*, use the following command:

   ```
   ixutil export service  - f filename.xml -include_translation object-specific
   parameters
   ```

   ***filename*.xml**

   Specifies an intuitive name of your choice for the exported objects. Enclose the *filename*.xml in quotation marks if it contains one or more spaces.

   -include_translation

   Creates a default localization properties file. This file contains default localization parameters. You send this file to the localization agency, which supplies the language-specific attributes and completes the file. The file name is *xml-filename*_default.properties. For example, if you specify PersonnelServices.xml as the XML file name, then this file name is PersonnelServices_default.properties.

   object-specific parameters

   Specifies the parameters for a specific object. For example, a business unit or folder, as shown in the examples that follow this procedure.

4. (If you do not have access to the Catalog system or if you are working in a team)

   a. The first person or team exports the services to one or more XML files. Use the following command:

      ```
      ixutil export service  - f filename.xml -include_forms object-spec
      ```

   b. The second person or team receives the XML file or files and then extracts the default translatable strings from each XML file into a default localization properties file. Use the following command:

      ```
      ixutil export service  - f filename.xml -extract_translation
      ```

Examples

These sample commands show how to export services, with or without forms, using a single command. All single-command operations must specify the -include_translation option to create the localization properties file. If you are using two teams and two commands, use the following examples to help construct your first export command.

```
ixutil export service  - f AllServicesAndForms.xml -include_forms -include_translation
```

This command creates the AllServicesAndForms.xml file and the AllServicesAndForms_default.properties file.

The following command exports all services in the business unit that is named SaoPaulo25, and does not include forms:

```
ixutil export service  - f SaoPaulo25.xml  - domain "SaoPaulo25" -include_translation
```

This command creates the SaoPaulo25.xml file and the SaoPaulo25_default.properties file.

The following command exports the services and forms in the folder Folder 1 in the business unit named CA:

```
ixutil export service  - f CA-Folder1.xml  - folder "Folder 1"  - domain "CA" -
include_forms -include_translation
```

This command creates the CA-Folder1.xml file and the CA-Folder1_default.properties file.

Step 3 - Send the Default Localization Properties File to the Localization Agency

The agency completes the default localization properties file by adding localization attributes for the languages that you require.

Follow these steps:

1. Send the default localization properties file to the localization agency.
2. Instruct the agency to provide one new properties file for each required language. An example for the file naming convention is *filename*_pt_BR.properties for Brazilian Portuguese. Or *filename*_fr_FR.properties for French.

Important! Instruct the agency to save each file with the UTF-8 encoding. This encoding is required for the file to function properly.

You have sent the default localization properties file to a localization agency.

Step 4 - Merge the Completed Localization Properties Files

When the localization agency returns the completed localization properties file for each language, you merge these files into the catalog. After the merge, the services are available to catalog users in the localized languages.

Follow these steps:

1. Review each completed localization properties file that the localization agency returned to you. Verify that the localization attributes appear for services and forms (if applicable) in the required languages.

2. Copy the completed localization properties files to the same folder as the XML file that you exported (see page) originally.

   Important! This XML file and the properties files *must* reside in the same folder. Otherwise, the merge does not occur.

3. Open a CA Service Catalog command prompt and navigate to the *USM_HOME*\scripts folder.

4. (If you have access to the Catalog system and you are working individually)

   Enter the following command to import the completed localization properties files into an XML file. This command also imports the updated XML file into the Catalog system. Merge the completed localization properties files into the Catalog system, using the IXUtil import command.
   To import services *with* forms, use the following command:

   ```
   ixutil import service  - f filename.xml -include_translation -include_f
   ```

   To import services only, use the following command:

   ```
   ixutil import service  - f filename.xml -include_translation object-spe
   ```

   ***filename*.xml**

   Specifies the name of the XML file that you exported originally. Enclose the *filename*.xml in quotation marks if it contains one or more spaces. Specify the complete path name. Enclose the complete path name in quotation marks if it contains one or more spaces.

   -include_translation

   Merges the localization attributes from the completed localization properties files into the exported XML file. Also inserts the objects from this XML file into the Catalog system.

   object-specific parameters

   Specifies the parameters for a specific object. For example, a business unit or form.

5. (If you do not have access to the Catalog system or you are working in a team)

   a. The first person or team imports the completed localization properties files into one or more XML files. Use the following command:

      ```
      ixutil import service  - f filename.xml -merge_translation
      ```

   b. The second person or team imports each updated XML file into the Catalog system after receiving it from the first person or team. This command merges the completed localization attributes from the localization properties files into the corresponding

objects in the XML file. Next, the command inserts these objects into the Catalog system. The updated objects from the XML file overwrite any existing objects with the same ID in the system. Use the following command:

```
ixutil import  - f filename.xml -include_forms object-specific par
```

Examples

These examples show how to import services, with or without forms, using a single command. If you are using two teams and two commands, use these examples to help construct your first import command.

The following command imports all services and forms from the AllServicesAndForms.xml file into the catalog:

```
ixutil import service  - f AllServicesAndForms.xml -include_translation -include_forms
```

The following command imports all services (without forms) from the SaoPaulo25.xml file into the business unit that is named Sao_Paulo25:

```
ixutil import service  - f LocalizationSaoPaulo25.xml -include_translation  - domain
"Sao_Paulo25"
```

Step 5 - Test the Localized Services

Verify that the localized services appear as intended in the catalog.

Follow these steps:

1. Set your Web browser to the localized language and access the localized services in the catalog.
2. Verify that the localized elements and attributes appear correctly in folders and services, including its forms.
3. If necessary, correct any errors. Also, if necessary, synchronize changes between the original language and the localization attributes.

You have tested the localized services to verify that they appear as intended in the catalog.

Manage Events-Rules-Actions

As a CA Service Catalog administrator, you can use events, rules, and actions for automating the requests, users, and accounts process in the system as following:

- Events (see page 3041)
- Rules (see page 3041)
- Actions (see page 3042)

Events

Events are installed automatically when you install or upgrade CA Service Catalog.

- *Events* represent changes that occur within CA Service Catalog. Several *standard* events typically occur in various components. For example, the User Create event occurs when an administrator adds new user, by using either the user interface or the createUser web service method. You can also add *custom* events.
- Events can have *rules* that are associated with them. Rules can have a set of filter conditions that define when the rule applies. When the filter conditions are satisfied and the rule is enabled, the rule *actions* are launched.
- A rule can have one of more *actions that are associated* with it. When an event occurs and a rule filter is satisfied, the associated rule actions are executed, if the rule is enabled.

Perform one of the following actions when a *custom* event occurs:

- Use one of the postEvent web service methods for the event type
- Use a URL to post the event

To manage rules, select Administration, Events-Rules-Actions. The page displays the event types and provides access to the rules and actions that are associated with each event type. You can perform the following actions:

- Use Event Parameters
- Add a Custom Event Type
- Manage Rules
- Manage Actions
- Post an Event

Rules

All rules are initially disabled. A rule must be enabled to be used. In addition, for some of the rules, there are two mutually exclusive actions, one for use with CA Service Desk Manager and one for use without CA Service Desk Manager. By default, the actions which interface with CA Service Desk Manager are disabled.

The rule conditions that are shipped with CA Service Catalog may not completely match your business processes. They are generic and must be examined for applicability to your environment. In addition, some rules overlap in functionality. When activating rules, be careful to understand the full implications of your changes.

A rule can have one of more actions associated. When an event occurs and a rule filter is satisfied, the associated rule actions are executed. A rule action causes some task to be executed. A rule action can perform one of several action types such as run a command line command, send an email, start a CA Process Automation process, or run a Java plug-in.

The When Status is Submitted and Approval Process is Driven by Workflow rule handles the approval process. The rest of the rules handle the fulfillment process.

Actions

Actions are invoked when a condition in a rule is satisfied. Actions include running a command line command, starting a Java process, sending an email, and starting a CA Process Automation process. For more information about actions, see the descriptions of the rules.

Add a Custom Event Type

Administrators can create *custom* events by adding a new event type. You typically do so to address a need in your organization that the predefined event types do not meet.

Follow these steps:

1. Select Administration, Events-Rules-Actions.
2. Click Add.
3. Complete the fields on the page, and click OK.
   The following fields require explanation:

- **Event Source**
  Specifies that the event source is *physical.* A physical event is based on an update to a database table.
- **Audit Trail Level**
  Specifies the level of detail to log in an event log table.
- **Transaction Name**
  Specifies the name of the database table.
- **Transaction Type**
  Specifies the transaction type: Added, Modified, or Deleted.
  This type represents the general behavior of the custom event. The Transaction Type together with the Event Type Name and Event Source make a unique combination.

  Note: The event type name is not required to be unique. However, we recommend that you specify a unique name.

Event Parameters

Events represent changes that occur in components. Each standard event occurs when it is caused by an action. For example, the User Create event occurs when a new user is added using the Add User user interface or the createUser web service method. You can optionally add custom events.

Each event type may have parameters associated with it. When an event occurs, the parameter values reflect the context of the event. For example, when the User Create event occurs, the associated parameter named $user_id$ contains the User ID value for the new user just created. Event parameter values can be used in rule filters and rule actions.

Administrators can use event parameters as conditions to determine whether rules or actions are triggered. Each event type has parameters that reflect the context of the event. **Example:** The $user_id$ parameter of the User Create event contains the User ID value for the new user.

Most parameters for event types are intuitive. However, the parameters in the following sections require explanation:

Request Create Event and Change Event

These event types occur when the request header information is modified.

Note: You must have CA Service Catalog installed to use this event type.

Event Parameter	Meaning	Example
$completion_date$	Date the request is completed.	
$created_date$	Date the request is created.	
$desired_date$	Date required	
$domain$	Business unit name for the requested for user or account.	ABC Corp Sales
$modified_date$	Date the request was last modified.	
$name$	Request name	My new laptop
$priority$	Numeric value for request priority	3
$req_by_account_id$	Internal ID for Requested By user	10018

Event Parameter	Meaning	Example
$req_by_user_id$	User ID for Requested By user	ABCUser
$req_for_account_id$	Internal ID for an account that is associated with Requested For user or account.	10054
$req_for_user_id$	User ID for Requested For user	ABCUser - for a request for a user NIL - for a request for an account
$request_id$	Internal ID for request	10023
$status$	Numeric value of status of the request, for example: 400=Pending Approval800=Approved	400
all	Name=value pairs of all available event parameters including additional data not available as event parameters. Also includes variables containing old data before the save causing the event to occur.	comments='My laptop for travel' comments_eventdatatype='String' comments_old='NIL'

Request Item Form Element Create Event and Change Event

These event types occur when a field in a form that is associated with a request item is changed.

Note: Install Catalog Service Accounting component to use this event type.

Event Parameter	Meaning	Example
$form_elem_name$	Label for the field as it appears on the displayed form.	Employee Title
$form_elem_value$	Value for field on the form **Note**: This value is the HTML “value” field which is different from the choice list “label” field displayed.	Vice President (for an input type field) 1 (for a select list type field)
$subscription_detail_id$	Unique internal ID for this request item	10012
all	Name=value pairs of all available event parameters including additional data not available as event parameters. Also includes variables containing old data before the save causing the event to occur.	

Event Parameter	Meaning	Example
		form_elem_label='Employee Title' form_elem_label_eventdatatype='String' form_elem_label_old='NIL' form_elem_name='emp_title' form_elem_name_eventdatatype='String' etc

Request Pending Action Change

The following parameters apply to the Request Pending Action Change event type and any new event types that you create based on it.

Parameter	Value
rpa_action_type	0=Default1=System2 =CA Workflow3=CA Process Automation4=Policy
rpa_id	The request_pending_action_id entry in the usm_request_pending_action table in the MDB
rpa_object_type	1=Service Offering (service)2 =Request Item
$rpa_reassigned_id$	The reassigned value of the request_pending_action_id entry in the usm_request_pending_action table in the MDB
rpa_status	0=deleted1=active2=completed by assigned user3=completed by other user4=transferred5=delegated6=terminated
$rpa_users_or_groups$	The user_id or group_id entry in the usm_request_pending_action table (mdb)

Request/Subscription Item Create Event and Change Event

These event types occur when a request or subscription item is modified. The modification is generally a change to the status of the item.

Note: Requests or subscriptions are for service options. Service options are comprised of service option elements. When the status of a service option that is part of a request or subscription changes, this event occurs for each service option element in the service option.

Event Parameter	Meaning	Example
$account_label$	The account name for the Requested For user	ABC Corp:ABCUser (for a request for a user) Sales (for a request for an account)
$account_no$	Internal ID for the account in $account_label$	10002

$approval_level$	Numeric value for the approval level for service	10
$approval_process$	Numeric value for the approval process, as follows: 0=No approval1=System approval process2=Workflow driven approval process	2
$category$	Numeric value for requested item category, for example: 0=Software1=Hardware	0
$category_class$	Numeric value for requested item class within category, for example: For category 0 (Software), class 10 may be “Office”.	10
$category_subclass$	Numeric valued for requested item subclass within class within category, for example: For category 0 (Software), class 10 (Office), subclass 10 may be “Microsoft”.	10
$charge$	Numeric value indicating whether associated amounts are a charge or credit for use by Service Accounting Component where: 0=credit 1=charge	1
$charge_date$	Date the item is first charged for by Service Accounting Component.	
$code$	Code for the service option element	My Element Code
$domain$	Business Unit Name for the Requested For user or account	ABC Corp Sales
$enum_1$ through $enum_5$	Vary depending on service option element type.	
$external_id$	Service option element External ID	My Element External ID
$group_id$	Numeric value indicating the occurrence of the service in a request (in case a request includes more than one copy of a service)	1 NIL (for a subscription)
$form_data_sd$ - for the Request/Subscription Item Change Event only	If this service option includes a form, then this parameter lists the details of the form in JSON structure. To apply rules to subscription items whose type is form, append the following condition to the event filter: “AND form_data_sd <> 'NIL'”	See Sample Data for $form_data_sd$ (after this table)
$form_data_sd_row$ for the Request/Subscription Item Change Event only	If multiple forms exist in a service option, this parameter lists the details of all these forms in JSON structure.	See Sample Data for $form_data_sd_row$ (after this table)
id	Unique internal ID for this request item	10012

Event Parameter	Meaning	Example
$installments$	Numeric value indicating the number of installments for associated amounts for use by Service Accounting Component	0
$instance_name$	Optional value that is assigned when subscribing an account to a service.	My instance
$item_id$	Internal ID for requested service option element	9981
$last_charge_date$	Date the item was last charged for by Service Accounting Component.	
$numeric_1$ and $numeric_2$	Vary depending on service option element type.	
$offering_id$	Internal ID for requested service	10002
$offering_name$	Name of the service offering (service)	Standard Laptop Bundle
$rate_item_col$	Numeric value (zero-based) indicating the associated service option element's column position in the service option row	0
$rate_item_name$	Service option element Display Text	Standard Laptop
$rate_item_row$	Numeric value (one-based) indicating the associated service option element's row position in the service option group	1
$rate_item_text_1$	Additional text that is associated with the service option element. For example, for a Text type service option element, this is Text Value and for a Rate type service option element, this is Display Unit Type.	/month
$rate_item_type$	Numeric value for the associated service option element where: 0=Text1=Header2=Numeric Range 3=Rate4=Application5=Agreement6=Numeric7=Boolean 8=Adjustment9=Date10=Date Range11=Day12=Allocation13=Form	3
$rate_plan_id$	Internal ID for associated service option group	10035
$rate_plan_name$	Associated service option group name	Standard Laptop Accessories
$req_by_user_id$	User ID for Requested By user	ABCUser NIL (for a subscription)
$req_for_user_id$	User ID for Requested For user	

Event Parameter	Meaning	Example
		ABCUser(for a request for a user) NIL (for a request for an account) NIL (for a subscription)
$request_id$	Internal ID for request	10023 (for a request) NIL (for a subscription)
$request_name$	Request Name	My new laptop NIL (for a subscription)
$request_priority$	Numeric value for request Priority	3 NIL (for a subscription)
sd_row	Numeric value (one-based) for the service option containing this service option element relative to all the service options selected with the service.	1
$status$	Numeric value of status of the requested item, for example: 400=Pending Approval800=Approved	400
$subscribed_date$	Date the item was included in a request or subscription.	
$subscription_type$	Numeric value indicating the type of item where: 0=Other1=Application2=Agreement3=Adjustment4=Form	0
$text_1$ - $text_7$	Vary depending on service option element type.	
$tiered_item_id$	Internal ID of the tiered service option group of the associated service option element where: -1=Not associated with a tiered service option group	-1
$tiered_last_date$	Date the item was last charged for by Service Accounting Component. Applicable only if the related service option element is part of a tiered service option group.	
$track_as_asset$	Numeric value indicating whether this request item must be tracked as an asset where: 0=No1=Yes	1
$unsubscribed_date$	Date the item is cancelled or unsubscribed.	NIL
all	Name=value pairs of all available event parameters including additional data not available as event parameters. Also includes variables containing old data before the save causing the event to occur.	account_label='Sales 'account_label_eventdatatype='String' etc

Sample Data for $form_data_sd$

The following sample data lists the details of one form:

```
{"name" : "dept",
"value" : "001|Human Resources",
"type" : "9"},
{"name" : "empid",
"value" : "spadmin",
"type" : "5"},
{"name" : "empName",
"value" : "Administrator, Service Delivery",
"type" : "5"},
{"name" : "reason",
"value" : "0",
"type" : "12"}
```

Sample Data for $form_data_sd_row$

The following sample data lists the details of two forms (10246 and 10245) in the same service option. Form 10245 includes the form type subscription ids.

```
{
"10246" : [
{"name" : "dept",
"value" : "001|Human Resources",
"type" : "9"},
{"name" : "empid",
"value" : "spadmin",
"type" : "5"},
{"name" : "empName",
"value" : "Administrator, Service Delivery",
 "type" : "5"},
{"name" : "reason",
"value" : "0",
"type" : "12"}],
"10245" : [
{"name" : "accesstype",
"value" : "0",
"type" : "12"},
{"name" : "buildingcode",
"value" : "1|Building1",
"type" : "9"},
{"name" : "date",
"value" : "",
"type" : "14"},
{"name" : "date_fdms$$",
"value" : "",
"type" : null},
{"name" : "device_code",
"value" : "device access code value",
"type" : "5"},
{"name" : "empid",
```

```
"value" : "spadmin",
"type" : "5"},
{"name" : "empname",
"value" : "Administrator, Service Delivery",
"type" : "5"},
{"name" : "purpose",
"value" : "purpose value",
"type" : "8"}]
}
```

Notes Create and Notes Change

The Notes Create and Notes Change event types are described as follows:

Notes Create

This event type occurs when a note is created for a CA Service Catalog request. Rules associated with this event type are as follows:

- **When a note is added to a CA Service Catalog request**: When note is added to a CA Service Catalog request, email notifications are sent.
- **When notes are added to a CA Service Catalog request**: When a note is added to a CA Service Catalog request, it is also synchronized with the corresponding CA Service Desk Manager ticket.
- **When a CA Service Desk Manager note is synchronized to a CA Service Catalog request**: When CA Service Desk Manager (CA SDM) note is synchronized to CA Service Catalog request, email notifications are sent.

Notes Change

This event type occur when a Note is changed or modified for a request. The following rules are associated with this event type:

- **When note with attachment(s) is edited in a CA Service Catalog request**: When a note with attachment(s) is edited in CA Service Catalog request, E-Mail notifications are sent.
- **When note without attachment(s) is edited in a CA Service Catalog request**: When a note without attachment(s) is edited in CA Service Catalog request, E-Mail notifications are sent.

The following event parameters associated with these event types require explanation:

Event Parameter	Meaning	Example
$source_id$	The request ID of the corresponding Note.	10510
$note_text$	Description of the note.	
$ignore_notification$	Value will be true in the following cases: ▪ on submission of request that has note(s). ▪ When a note event is triggered for a comment with notes and attachments posted in Widgets.	

Attachment Create and Attachment Change

The Attachment Create and Attachment Change event types are described with associated rules:

Attachment Create

This event type occurs when an attachment is created for a request. Rules associated with this event type are as follows:

- **When attachment is added to CA Service Catalog request**: When an attachment is added to a CA Service Catalog request, it is added as a link to the corresponding CA Service Desk Manager ticket.
- **When attachment is added to a CA Service Catalog request:** When an attachment is added to a CA Service Catalog request, email notification is sent.
- **When note and attachment(s) are added to a CA Service Catalog request**: When note (s) and attachment(s) are added to a CA Service Catalog request from Widgets, email notifications are sent.
- **When a CA Service Desk Manager attachment is synchronized to a CA Service Catalog request**: When a CA Service Desk Manager attachment is synchronized to CA Service Catalog request, email notifications are sent.

Attachment Change

This event type occurs when an attachment is changed for a CA Service Catalog request. Following rule is associated with this event type:

- **When attachment associated with a CA Service Catalog request is edited**: When an attachment associated with a CA Service Catalog request is edited, email notifications are sent.

The following event parameters associated with these event types require explanation:

Event Parameter	Meaning	Example
$object_id$	Request ID of the corresponding attachment.	10510
$ignore_notification$	Value will be true in the following cases: ▪ on submission of request that has attachment(s). ▪ for the first *n-1* attachments when a comment with *n* attachments is posted in Widgets.	For example, if a comment in Widgets has 1 note and 5 attachments, so for the first four attachments (n-1=4), the value will be true.
$attachment_url$	Specifies the URL(s) of the uploaded attachment(s).	

Manage Actions

Administrators can configure actions in in several ways, to trigger the response you want for specific rules.

Example: You can create and configure a rule to trigger an automatic email notification when a fulfiller fulfills a request.

Follow these steps:

1. Select Administration, Events-Rules-Actions.
2. Click the event that contains the rule and action of interest.
3. Click the name of the rule and modify the actions associated with the rule.
4. (Optional) Retry failed action if required.

You create *global* policies and global actions for general use with any service. In contrast, you create *attached* actions and attached policies for use with a specific service option only. You can create an attached action or policy *only* from the Policies & Actions tab of that service option.

Note: You can perform significant edits on custom actions *only*. The predefined actions permit only limited editing. Similarly, you can delete custom actions *only*. You *cannot* delete predefined (built-in) actions.

If the predefined actions and existing custom actions do not meet your needs, you can add a new action to a rule. You can *add* new actions (create custom actions) in both custom rules and predefined (built-in) rules. When required, you can edit a custom action to meet a need in your organization more closely. For example, you can edit a custom action to refine the request email that the action sends.

Note: After you create, save, and close a custom action, you can edit its parameters. But you *cannot* change the Type field. To specify a different type for the action, copy and rename it. If you do so, update the related rule to trigger the renamed action.

Parameters

You can specify the several parameters for a *custom* action when you add or edit it. The following parameters are not self-explanatory:

- **Type**
  Specifies the type of action that must be used. To disable a rule action, select DISABLED. Based on the type you select, more fields are exposed. The add icon can be used to add an event parameter to the field used for each action type.

- **Command line**
  Specifies a command that must be run.

- **HTTP Post**
  Specifies the URL that must be posted.

- **Java**
  Specifies the Java Class and parameters that must be passed.

- **Email**
  Notifies users (typically administrators) about system activities that are not related to requests. Examples include the addition of new users or a new business unit, or a data mediation load.

- **Request Email**
  Notifies stakeholders about a request and optionally includes request details.
  The following parameters require explanation:
  Include Request Details - Specifies whether to add the details of the request to the text of the message body in the request email.
  Specify Yes to add these details or No to omit them.
  Type - Applies *only* when you use the $pending_action_users_or_groups$ variable.
  Specifies the Type: Request, Service, or Service Option.
  This parameter retrieves the list of pending action users or groups applicable to the selected Type. This parameter also assigns the retrieved list to the $pending_action_users_or_groups$ variable.
  Request ID - Specifies the ID (not the name) of the request, which must be a numeric value or variable.
  Request Item ID - Applies only when the selected Type is Service or Service Option.
  Specifies the ID of the subscription detail object, which must be a non-numeric value or variable. This value is used to retrieve the list of pending action users or groups applicable to the selected Type. The selected type can be Service or Service Option.
  From Email - Specifies the email address from which to send request emails.
  From Name - Specifies the name of the email address from which to send request emails.
  If you do not specify a value for From Email or From Name, the Catalog system assigns the following value: the value that is specified in the Catalog, Request Management configuration options of the business unit of the request.
  To - Specifies one or more primary recipients for the email.
  You can use specific email addresses, user IDs, and requested for user-related variables.
  To send an email to specific users or groups automatically, specify the matching variables, as follows:

  - For the requested for user, specify $req_for_user_id$
  - For the requested by user, specify $req_by_user_id$
  - For the pending action user, specify $pending_action_users_or_groups$

  To specify more than one value, separate the entries with a semi-colon (;).
  You can select these variables and other variables from the list that appears when you click the list icon next to the field.
  CC and BCC - Specifies more recipients for the email. Use the same syntax as the To field.
  A commonly used variable in the Subject and Message Body is $server_url$. You can optionally use it to direct the recipient to the request detail page.

- **CA Process Automation**
  Specifies the start request form (SRF) (for CA Process Automation) to invoke.
  Use the Find Start Request Form icon (for CA Process Automation).
  Specify the parameter values for the SRF, if applicable.

- **CA Automation Suites Reservation Manager**
  Specifies a parameter that must be passed to Reservation Manager.

- **Execution Mode**
  Specifies whether the action runs asynchronously or synchronously.
  Administrators *cannot* set the order in which actions run.

- **Timeout**
  Specifies the number of seconds the action must run before a user can cancel it.
  A value of 0 means no timeout applies.

Parameters That Accept Multiple Values

For some events, some parameters can have multiple values. For such parameters, use a delimiter to separate multiple values. For each parameter that can have multiple values, you can specify the separator to use when that event occurs. If the Multiple Values check box is selected, the rule action is executed for each value for the parameter indicated in the Parameter field.

Note: The only standard event with multiple values parameters is the Catalog Subscription Change event. This event provides multiple values for the $new_offerings$, $new_subscriptions$, $old_offerings$ and $old_subscriptions$ parameters. You can use multiple value parameters with custom event. However, the event posting logic must provide the multiple parameter values.

Retry Failed Actions

When a rule action fails to launch its associated CA Process Automation process, a system alert is created. Possible causes for the failure include the related service either not running, or being too busy to accept more work, or connectivity between CA Service Catalog and CA Process Automation is not established. Service Delivery administrators can retry failed actions of these types.

Follow these steps:

1. Select Home, Messages, Alerts from the Messages menu.
   The Alert Messages lists all the alert types appears.

2. Click **List All Failed Actions**.

3. Use **Filter Alerts** to display the list of alerts that include the failed actions you want to retry.

4. Click **Change Business Unit**, if the failed action is in another business unit,

5. Select the alerts in the that you want to retry, and click **Retry Failed Actions**.
   For example, if you have retried an alert of type ITPAM_QUEUE_FAILURE, then it appears as a separate alert message for that request on the Alerts page.
   You have retried the failed actions.

Manage Rules

Administrators can configure rules in several ways, to trigger the actions you want under the conditions you want. For example, you can create and configure a rule to trigger an action when a user, service, business unit, or account is created or updated.

You can perform the following actions to manage rules:

- Add a Rule (see page 3055)
- Add an Event Filter (see page 3055)

Add a Rule

Administrators can add a new rule for several reasons. **Example:** Create a rule to trigger an action, such as an email notification, when an approver approves or rejects a request pending action.

Follow these steps:

1. Select Administration, Events-Rules-Actions.
2. Click the event to which you want to add the rule and click Add.
3. Complete the fields, following these guidelines:
   - Specify a unique rule name.
   - Click the Add Filter icon and create or edit an event filter.
4. Click OK.
   The rule is saved. The Event Type Details page appears, and it includes the new rule.

Add an Event Filter

Specify the conditions for invoking the rule and triggering its actions by adding an event filter. Otherwise, the rule and actions are invoked whenever the event occurs.

The properties available to a rule condition depend on the event type of the rule. You can specify both *old* and *new* (or *before* and *after*) values for each event property in the condition.

Follow these steps:

1. Select Administration, Tools, Events-Rules-Actions.
2. Click the event that contains the rule for which you want to add/edit a filter.
3. Click the Add icon next to the Event Filter field.

Note: You can add or update event filters in custom rules *only*, not predefined (built-in) rules. The predefined rules permit limited editing. You can copy a predefined rule and can save it with a new name as a custom rule.

4. Specify the values for the property, operator, and constant of your new condition in the Condition Builder section.

5. Click the Add Condition arrow and add your new condition to the Current Conditions section. The Condition appears in the Current Conditions field. The condition is translated into a conditional SQL-style expression that the rule engine can process. You can add as many conditions as required.

6. Click OK.
   The Event Filter appears in the Rule Information section of the Edit Rule page for the selected rule.

7. Click OK.
   The system saves the rule, including the event filter.

You have added the event filter.

Post an Event

Administrators can post an event as an automated way to mimic an action by a user. **Example:** A catalog user submitting a request or a catalog administrator updating the details of a user or business unit. In both cases (posted event or user action), when the event occurs, its rules are evaluated. If the conditions for a rule are met, the rule actions are executed.

Posting an event is useful for performing such tasks using automation and with specific values and actions. **Example:** You can post events to specify custom values for the integration between CA Service Catalog and another CA product. This topic explains how to post a CA Service Catalog event through HTTP URL. You can also use this URL in rule actions whose type is HTTP Post.

Important! If you post an event, test it thoroughly before moving it to a production environment. Verify that the event does *not* run cyclically if the action is triggered.

Follow these steps:

1. Gather the data from the event and construct the HTTP URL.

2. Specify the HTTP URL. This topic uses a URL example to illustrate how to post an event.

> **Note:** You can also post events using web services. Both techniques produce the same results.

3. Verify that the event is posted.

Gather the Data from the Event to Construct the HTTP URL

Gather the following values from the event definition for the URL.

This example uses the Data Mediation Aggregation event on the Tools, Events-Rules-Actions page. Click the event name. You see the following details of the event. Use these details to help specify the HTTP URL, as illustrated in the following text:

- Event Type: Data Mediation Aggregation
- Event Type Name: Data Mediation Aggregation
- Event Source: Logical
- Audit Trail Level: System Default
- Transaction Name: DATA_MEDIATION_AGGREGATION
- Transaction Type: Modified
- Event Type Parameters: end_date, $start_date$, $status$, $status_date$
- Description: When Data Mediation Aggregation Status is changed

Specify the HTTP URL

To specify the HTTP URL to post an event to the system, use the following syntax:

> **Note:** In the following line and in the example that follows, the line breaks are for readability *only*. In the product UI, enter this code as a single continuous line.

```
http://hostname:port/usm/wpf?Node=icguinode.postevent
&username=userid&pass=password&domain=businessunit
&Args=eventsource&Args=nsppath&Args=transactionname&Args=eventtypename
&Args=transactiontype&Args=eventdescription&Args=associatedobjectid
&Args=false&Args=param1|oldvalue1!param#|oldvalue#!
&Args=param1|newvalue1!param#|newvalue#!
```

An example URL follows:

```
http://hostname:port/usm/wpf?Node=icguinode.postevent
&username=spadmin&pass=spadmin&domain=ca.com&Args=LOGICAL
```

```
&Args=DATA_MEDIATION_AGGREGATION:MODIFIED
&Args=DATA_MEDIATION_AGGREGATION&Args=MODIFIED&
Args=LOGICAL&Args=Modified&Args=$id$&Args=false
&Args=end_date|abc!start_date|abc!status|123!status_date|abc!
&Args=end_date|abd!start_date|abd!status|124!status_date|abd!
```

Note: When you post an event using a URL from Java or some other tools, encode the URL by replacing unsupported characters with codes. **Example:** Replace the ampersand (&) with %26 or replace a single blank space with %20.

Note: The Catalog system uses both old and new values when it evaluates rule filters for event rules.

The following parameters require explanation:

- ***userid* and *password***
  Specifies login credentials for authentication.

- ***businessunit***
  Specifies the business unit for the role of the user ID.

- ***eventsource***
  Specifies the Event Source from the event details: LOGICAL, PHYSICAL, CommonDB.
  In this example, the value is LOGICAL.

- ***nsppath***
  Specifies the namespace path, a placeholder value only. The Catalog system does not use the actual value but requires a placeholder value.
  Use the following format:
  <Transaction Name>-<Transaction Type>
  <Transaction Type> - MODIFIED, ADDED, or DELETED.
  <Transaction Name> - As displayed in event details
  In this example, the value is DATA_MEDIATION_AGGREGATION:MODIFIED.

- ***transactionname***
  Specifies the transaction name for the event.
  As shown in the event details, in this example, the value is DATA_MEDIATION_AGGREGATION.

- ***eventtypename***
  Specifies the name of the event type: MODIFIED, ADDED, or DELETED.
  In this example, the value is MODIFIED.

- ***transactiontype***
  Specifies the transaction type for the event.
  This value is the same as the value of the eventsource parameter.
  In this example, the value is LOGICAL.

- ***eventdescription***
  (Optional for web service) Specifies a description for the event.
  Specify the Transaction Type as displayed in event details.
  In this example, the value is Modified.

- ***associatedobjectid***
  Specifies the ID of an object to associate with this event.
  You can optionally specify one of the event parameters for this value. This value is used to associate the alert that was logged in Change Events.
  This example uses a dummy value: id.

- **ispartial**
  Specifies whether this event is partial; This value is always false.

- ***param#*|*oldvalue#***
  Specifies the parameter name and the *old* value. Delimit the name and value with a vertical bar. Separate each name and value pair with an exclamation point.
  In this example, the value is as follows:

```
end_date|abc!start_date|abc!status|123!status_date|abc!
```

  Note: This example uses dummy values for event attributes. Do *not* specify a value for the all attribute, because it reads *all* values.

- ***param#*|*newvalue#***
  Specifies the parameter name and *new* value. Delimit the name and value with a vertical bar. Separate each name and value pair with an exclamation point.
  In this example, the value is as follows:

```
end_date|abd!start_date|abd!status|124!status_date|abd!
```

  The note for the previous parameter also applies to this parameter.

Verify that the Event is Posted

To verify that an event is posted, follow these steps:

1. Disable all the rules for the event that you are posting.
2. Enable only one rule with no filter and one command-line action, as follows:

   ```
   cmd /c echo Posted Event: $all$ >> C:\PostEventCheck.txt
   ```

3. Verify that the PostEventCheck.txt file is created on the C:\ drive of the application server for CA Service Catalog.

Note: You can also post an event using one of the postEvent Administration web service methods.

Manage Dashboards

Administrators and other users use the Dashboard Builder to manage dashboards and their content elements (dash items). Administrators can create shared dashboards and manage the dashboard library. Other users can create personal dashboards and can access the shared dashboards to which they have access in the following ways:

- Add a Dashboard (see page 3060)
- Configure Content Elements (see page 3061)
- Administer Dashboards (see page 3063)

Add a Dashboard

You add personal or shared dashboards to provide access to information and to frequently used features of CA Service Catalog.

Follow these steps:

1. Click Home, Dashboards.

2. Click the << icon at the top right part of the page, and click Add Dashboard.

3. Name the dashboard, configure the options, and click Add.
   The following fields require explanation. Click the Help (question mark) icon for further assistance.

   - **Shared Dashboard**
     Creates a shared dashboard.
     Administrators use shared dashboards to publish information to users. If this option does not appear or if you do not select it, then this dashboard is available to you *only*.
     You can create a personal dashboard and can share it later.
     When you select Shared Dashboard, several other fields appear. These fields are mutually exclusive. Select one of the following options:

     - Accessible by Sub Business Units - Shares this dashboard with users in your business unit and its child business units.

     - Accessible by Role - Shares this dashboard with users who have the roles you specify. Only those roles can access the dashboard. If you do not specify your own role, you cannot access the dashboard after you create it.

   - **Default Dashboard**
     Sets the dashboard as the default dashboard.

   - **Full Screen**
     Configures the dashboard to open in full-screen mode when users select it.

   - **Open in New Window**
     Configures the dashboard to open in a new window when users select it.

- **Disable Session Timeout**
  Disables the session timeout feature. Users are not logged out if they are inactive longer than the session timeout value.

- **Auto Arrange**
  Arranges the dashboard items automatically.

- **Make Item Snappable**
  Creates an invisible grid on the Dashboard, which lets you position and resize the Dashboard items.
  You set the Grid Height and Grid Width properties of each cell in the grid. Each Dashboard item "snaps" to this grid when it is positioned or resized.
  This option applies only if Auto Arrange is *not* selected.

- **Lock Down Items**
  Fixes the location of the dash items so that other users cannot move them.

The new dashboard appears in the dashboard menu and is selected. The rest of the window is blank, because a new dashboard has no dash items.

4. Add dash items as follows:

   a. Verify that the new dashboard is selected. Click the << icon at the top right part of the page, and click Show Library.

   b. Navigate the Library tree and locate the elements that you want to use on the dashboard.

   c. Drag the content elements to the place where you want them on the dashboard. The elements become the dash items.

   d. Adjust the size of the dash items as needed.

5. Set the properties of the dash items by clicking the Edit icon on the dash item heading.

6. Click Save Layout.

Configure Content Elements

You configure content elements in dashboards to customize them to meet the needs of your organization.

Follow these steps:

1. Click Administration, Dashboard Builder.

2. Expand the folders and subfolders and select a content element.
   The details of the element appear in the Content Preview and Content Properties panes.

3. Configure the fields on the Content Properties pane, and click Save.
   The following fields require explanation:

- **ACL Settings**
  Specifies the access control list (ACL) settings.
  Use these settings to specify the level of access for each role to the content element.

- **Content Type**
  Specifies the type of content element, as explained in the next section.

Type of Content Element

- **Folder**
  Configures the content element as a folder.

- **External Web Content**
  Configures the content element as a web page URL.

- **External XML Source**
  Configures the content element as an external web reference in XML format. If access to the XML content requires authentication, the web publishing framework automates the authentication login to gain access.
  The web publishing framework can use Web Services to transform the information to meet the needs of the user. You can view the XML directly. Alternatively, you can supply a custom XSL instead.
  If you use XSL, you can embed it as part of the published data definition or can obtain it through a URL.

- **Embedded HTML**
  Configures the content element to include the HTML to display.
  You supply the information in HTML format. The information is stored with the metadata in the Dashboard Library. Embedding HTML enables you to integrate with application data accessible through web controls and Java applets, such as Microsoft Outlook.

- **Embedded XML**
  Configures the content element to include the XML to display.
  You supply the information in XML format. The information is stored with the metadata in the Dashboard Library. Embedding XML enables you to view it directly. Alternatively, you can optionally supply a custom XSL instead of XML.

- **GUINode**
  Configures the content element to reference a CA Service Catalog page.
  Specify the page as a Graphical User Interface (GUI) node.

- **GUINode XML**
  Configures the content element to reference internal CA Service Catalog data that you obtain through a GUI Node.
  This setting enables you to define custom views of information without modifying back-end methods and customizing XSL style sheets.
  Alternatively, you can optionally supply a custom XSL instead of XML.
  Access to the published data requires access to the GUI Node.

- **Managed Document**
  Configures the content element as a document maintained in CA Service Catalog.
  Specify the path in the Filename field. This document must be in the same location on all Catalog Component servers if you are using multiple Catalog Component servers.

Administer Dashboards

You administer dashboards to meet the needs of your organization.

Follow these steps:

1. Click Administration, Dashboard Builder.
   The Dashboard Library folders appear and display the dashboards that you have permission to access.

2. Expand the library tree and display the category for which you want to administer dashboards.

3. Install ActiveX components, if you are prompted to do so.

4. Select an option from the Action drop-down list and click Go. The options vary, according to the category that you select in the library tree.

5. Repeat these steps as needed for more dashboards.

Manage Outage Calendars

You can create and Maintain Outages, outage groups, outage calendars, create business hours, and associate outage calendars and business hours to a service in the following ways:

- Create and Maintain Outages (see page 3063)
- Create and Maintain Outage Groups (see page 3064)
- Create and Maintain Outage Calendars (see page 3064)
- Create Business Hours (see page 3065)
- Associate Outage Calendars and Business Hours to a Service (see page 3066)
- (Optional) Specify Default Outage Calendar and Business Hours (see page 3066)

Before you perform these tasks, verify that you have completed the tasks to manage request SLAs.

Create and Maintain Outages

You create a scheduled outage to specify a single occurrence when a service is not available. Reasons for such outages include holidays, maintenance periods, disaster recovery activities, one-time events such as major hardware or software changes. Both outages and outage groups are independent entities that can be reused in multiple outage calendars. During the outage periods that the outage calendars define, the monitoring of time for a request SLA is stopped.

Follow these steps:

1. Click Catalog, Service Hours.

Check the business unit identification message under the main menu. Verify that you want to create this outage for the current business unit.

- Click Add to create a new outage.
- Complete all required fields and add or edit an SLA.
- Click Save.

This outage can be used in an outage group or outage calendar.

Create and Maintain Outage Groups

Outage groups are logical sets of related outage events, such as holidays or annual maintenance days. These outage groups typically recur annually. As an administrator, you combine individual outages into outage groups. Outages and outage groups are the major ingredients of an outage calendar. Both outages and outage groups are independent entities that can be reused in several different outage calendars.

Follow these steps:

1. Click Catalog, Service Hours.
2. Check the business unit identification message under the main menu. Verify that you want to create this outage for the current business unit.
3. Click Add to create a new outage group.
4. Complete all required fields and add or edit an SLA. For existing outage groups, any outages that are already included in the group appear in the Associated Outages box.
5. Click Save.
6. Click Associate Outages to add an outage to the current outage group.

This outage group is ready to be used in an outage calendar.

Create and Maintain Outage Calendars

As an administrator, you use outages and outage groups to create *outage calendars*. For each business unit, you can optionally apply *one* outage calendar to a service. You cannot apply outages or outage groups to a service directly; they must be associated to a calendar. The criteria that you use for determining the outages, outage groups, and calendars for each service in a business unit are based on different groupings. Examples of such groupings are geographical areas, departments, time zones, and other customer-related considerations. Both outages and outage groups are independent entities that can be reused in several different outage calendars.

Follow these steps:

1. Click Catalog, Service Hours.

Check the business unit identification message under the main menu. Verify that you want to create this outage for the current business unit.

- Click Add to create a new outage calendar.
- Complete all required fields and add or edit an SLA. For an existing outage calendar, outages and outage groups that are already in the calendar appear in the Associated Outages box. For outage groups, the Group Name column is completed; for outages, the Group Name column is empty.
- Click Save.
- Click Associate Outages to add one or more outages to the current outage calendar.
- Click Associate Outage Groups to add one or more outage groups to the current outage calendar.

After selecting the outages and outage groups for your outage calendar, you can associate the calendar to a service.

Create Business Hours

Business hours specify the regularly scheduled days and times of service. The service provider sets the business hours. But for best customer relations, business hours are geared towards the typical business schedule of all requestors.

As an administrator, you can optionally apply *one* outage calendar and *one* business hours specification to a service. The criteria that you use for determining the business hours for each service in a business unit can be based on different grouping.

During the time periods that the business hours define, time is monitored for the request SLA attached to a service. During the outages that the outage calendar of the service specifies, the time in not monitored.

Follow these steps:

1. Click Catalog, Service Hours.
2. In that Menu, click Business Hours.
3. Check the business unit identification message under the main menu. Verify that you want to create this outage for the current business unit.
4. Click Add to create a new Business Hours specification.
5. Complete all required fields and add or edit the Business Hours.
6. Click Save.

After you select and save your business hours specification, you can associate it to a service.

Associate Outage Calendars and Business Hours to a Service

The outage calendar and business hours that are associated to a service work together to specify the time periods during which the service is expected to be available. During these periods, the time is monitored for the Request SLAs attached to the service.

You are not required to associate an outage calendar and business hours object to a service at the same time. However, we recommend that you do so. When you associate an outage calendar and business hours object to a service at the same time, it ensures the expected up time and down time govern the Request SLAs attached to the service. **Example:** Suppose that you attach a Request SLA to a service without specifying either an outage calendar or business hours. The clients then expect that the service is to be available 24 hours per day and 365 days per year.

Follow these steps:

1. Click Catalog, Service Offerings.
2. Expand the tree and access the service you want.
3. Follow these steps to associate an outage calendar to a service.
    a. Click the Not Specified link for the business hours.
    b. Click Search in the Associate Business Hours dialog. The currently associated object (if applicable) is selected.
    c. Select the objects that you want and click Associate.
    The list of available objects disappears, and the object that you selected appears in the Associated Business Hours field.
4. Follow these steps to associate business hours to a service.
    a. Click the Not Specified link for the business hours.
    b. Click Search in the Associate Business Hours dialog. The currently associated object (if applicable) is selected.
    c. Select the objects that you want and click Associate.
    The list of available objects disappears, and the object that you selected appears in the Associated Business Hours field.

(Optional) Specify Default Outage Calendar and Business Hours

Business unit administrators can optionally specify a default outage calendar and default business hours for all services in their business units. Doing so helps verify consistency in the days and hours that services are available throughout the business unit.

If a service is associated to a different outage calendar, you can assign the default outage calendar by clicking the Use Default button of the calendar. If a service is associated to a non-default business hours, you can assign the default business hours by clicking the Use Default button of the business hours.

If the business unit administrator assigns no default outage calendar and if the administrator for a service does not associate a custom outage calendar to the service, then time is tracked for SLAs associated to the service *every day of the year*. Similarly, if the business unit administrator assigns no default business hours and if the administrator for a service does not associate custom business hours to the service, then time is tracked for SLAs associated to the service *every hour of the day*.

Therefore, as a best practice, business unit administrators and administrators of individual services work together. Together, they verify that the default outage calendar and default business hours for the business unit are reasonable and achievable. Otherwise, avoidable SLA warnings and violations are issued for such services.

Follow these steps:

1. Review the outage calendars and business hours that you have created already. Identify the ones that you want to use as defaults. Verify that your selections meet your requirements for all services in the business unit. If no suitable options exist yet, create suitable outage calendars and create suitable business hours.

2. Click Catalog, Service Offerings.

3. Check the business unit identification message under the main menu. Verify that you want to create this outage for the current business unit.

4. Click the root folder, which is also the name of the business unit that you selected in the previous step.

5. Click Not Specified in the Default Business Hours field and select the business hours.

6. Click Not Specified in the Default Outage Calendar field and select the outage calendar.

7. (Optional) Specify the default outage calendar and default business hours for each child business unit.

Note: You set the default outage calendar and default business hours for each business unit *individually*. Child business units do *not* inherit these default settings from their parent business unit.

Review SLA reports for the affected services to verify that the default settings meet your requirements for the business unit.

Manage News, Change Events, and Alerts

Administrators can manage news, change events, and alerts from the Home, Messages tab.

News is any announcement for the user community. Administrators can perform the following tasks to manage news messages:

- Add a news message for other users or roles in the same business unit.

- Delete news messages from themselves and from other users.

Change Events are automatically generated when either the system or users (especially administrators) perform significant actions. For example, if you add a user, your action appears as a change event message on the Change Events page. Administrators can view and delete change events.

Alerts represent failed change events. Typically, CA Service Catalog components issue alert messages when a system action fails or a user action fails. For example, failed actions and alerts can result from an administrator specifying an incorrect email address for a user. In such cases, actions that use the email address can fail. An attempt by a request manager to perform email-based approval of a request from that user can fail, resulting in the "REQEMAILACTION_FAILED" alert. Administrators can view and delete system alerts and also retry failed actions.

Manage the Scheduler

Administrators can use the Scheduler to schedule tasks that you want to run one or multiple times. Scheduling is especially useful for recurring tasks, so that you do not have to repeat them manually. To manage scheduled tasks, Click Administration, Tools, Scheduler. You can:

- View the list of scheduled tasks.
- Add or edit a scheduled task.
- Delete a scheduled task.
- View Scheduler-related system alerts.

Note: For optimum scheduling capabilities, use CA Process Automation to schedule tasks. For more information, see the CA Process Automation documentation.

Follow these steps:

1. Click Administration, Tools, Scheduler.
2. Click the Add button and create a scheduled task.
3. Complete the fields and click OK.
   The following options for the *Category* field require explanation:

- **Valid Until**
  Specifies the date when the scheduled task stops running. If this field left blank, the scheduled task continues to run indefinitely.
- **Action Type**
  Depending on the Action Type, other fields appear to help further define the action.

- **Execute Command Line**
  Specifies a command that runs on the server.

- **Execute Scheduler Plugin**
  Specifies an option for system use *only.*
  If you have scheduled data mediation tasks, you can view this option.

- **Missed Actions**
  Specifies the action to perform when a scheduled task cannot run, as follows:

  - *Ignore* skips all missed scheduled tasks.

  - *System Alert* posts a system alert when a scheduled task is missed.

  - *Execute All* runs all missed scheduled tasks as soon as possible.

Manage Content Packs

A content pack is a collection of CA Service Catalog objects, such as services, forms, policies, events, report data objects, and CA Process Automation processes. This article contains the following topics:

Who Creates, Exports, or Imports Content Packs

Both customers and CA Technologies can create content packs, as follows:

- CA Technologies typically creates content packs that include new objects or updated versions of existing objects, including sample objects and fixes.

- Customers typically create content packs that include objects that are customized to meet specific organizational requirements.

- Customers can optionally copy content packs from CA Technologies. They can then customize the content packs before they apply them across their implementations.

- You can export and import multiple content packs for a single business unit. Similarly, you can export and import multiple content packs for all business units. If a conflict occurs between the existing content pack and the one you are activating, the new content pack automatically overrides the old one.

- As a producer or designer, create and export content packs to package customized versions of the CA Service Catalog objects.

- As a consumer or adopter, import content packs and use the customized objects without having to perform the same customization processes.

Typically, the customizations in a content pack are focused to configure CA Service Catalog system for the optimal use of a specific feature, service, or environment. Content packs enable you to repeat the customizations efficiently and accurately from one system to another, multiple times.

Service Management Content Pack

Demo Content

The Demo Content (Demo) content pack contains several model services for common requests throughout an enterprise. Some services require CA Process Automation processes and integration with underlying systems to function as intended.

An example service is the **Smartphone Selector service.** This service lets catalog users select a smartphone and accessories by guiding them through several nested levels of choices. This service uses JavaScript programs in forms for this purpose. To copy and customize this service, you must have advanced knowledge of the Form Designer and a working knowledge of JavaScript.

For the complete list of services in the Demo content pack, import it and view the Import Report. Then view the services in the CA Service Catalog Demo Content folder in the catalog. You can import the Demo content pack file from this location: USM_HOME\Filestore\contentpacks.

Overview of Content Configuration Form

This article contains the following topics:

You can create a content configuration form (see page 3071) to specify any custom configuration information and then use your content pack. These forms are typically not required but can be helpful, especially under the following circumstances:

- The imported objects require configuration before you can use them.
- The administrator who imports the content pack did not export it.
- You require custom values for variables in API plug-ins or CA Process Automation processes. Instead of hard-coding specific values, you can retrieve values from fields on content configuration forms (see page 3072). **Example:** The values can change and cause the API plug-ins or CA Process Automation processes to fail, leading to system downtime. **Example:** A server URL that can change during a migration from a low-security to high-security environment.

Content configuration forms can be helpful when your imported content requires a custom configuration for:

- CA Process Automation processes and plug-ins that require configuration data.
- A plug-in that needs access to an external data source (not the MDB), such as web service or database.
  An example is an Active Directory query that supplies CA EEM. The configuration form can list a *server name=field-name* field. The Active Directory query references this field in the form, rather than a hard-coded server name.
- Organization-specific requirements, such as user names and passwords that change both at regular intervals and intermittently as-needed.

Content configuration forms are specific to the business unit for which you create them. Parent business units have access to the forms of their child business units.

Administrators of each business unit can define their own configuration forms in the same way as they define request forms. Catalog, Configuration, Content Configuration page includes the Change Business Unit button. This button opens a dialog that lets you select another business unit that you are authorized to access. If you change business units, the list of configuration forms on the left pane of the page updates to display the forms of the current business unit.

Create the Content Configuration Form

To create a content configuration form, follow this process:

Note: For more information about creating forms using the Form Designer, see the section Manage Forms (see page 2914).

1. Decide the purpose of the configuration form. Examples include specifying custom *parameter*=*value* expressions for API plug-ins or CA Process Automation processes.

   Note: These custom expressions are *not* the same as the parameters on the Administration Configuration page, the Accounting Configuration page, or the CA Service Catalog Configuration page. Moreover, these expressions are *not* the same as any other parameters on the CA Service Catalog GUI. Custom parameters can *complement* the GUI parameters, but they are not required to do so.

2. Determine the fields that are required on the form. Create the fields that require user input and determine configuration data that the Catalog system saves and uses.
   Examples include the following fields, which supply database parameters:

   - Server name or URL
   - User name
   - Password
   - Port number

   Note: This form applies to your business unit *only*. Queries to the fields on the form from API plug-ins or CA Process Automation processes must specify the business unit.

3. Create the form in the Form Designer. Follow these guidelines:

- For the Form attributes (see page 2927), specify a value of configuration for the Form Type attribute.
- Create *unique* configuration forms, especially if you use multiple configuration packs. A unique configuration form has unique value for the _id attribute in the Form attributes. Verify that no other configuration form in your business unit has the same value for that attribute.

4. Open the form on the Catalog, Configuration, Content Configuration page and specify the values that you want in each field. Follow these guidelines:
   - Specify default values that can help run the content pack successfully without the user changing any data. Doing so is helpful if the user creating or exporting the content pack is not familiar with it.
   - Optionally specify _.bu and _.user JSON objects as values. You *cannot* specify any other JSON objects as values.
5. Save the form.

Note: If you import configuration forms using content packs, the values for the form fields are available only when you save them on this page. This page is the Catalog, Configuration, Content Configuration page that you opened previously.

Retrieve Values from Fields on Content Configuration Forms

You can have custom values for variables in API plug-ins or CA Process Automation processes.

Important! The values on a content configuration form can have a maximum length of 4,000 characters for single-byte languages. **Example:** English.

The values can have a maximum length of 2,000 characters for double-byte languages. **Example:** Chinese or Japanese. For example, a select box with many options can exceed this limit and cause errors.

Follow these steps:

1. (API plug-in) Locate the com.ca.usm.plugins.apis.PluginContext object. In that object, use one of the following methods to retrieve values from fields on a content configuration form:
   - **Object getCatalogConfigValue(String configGroup, String tenantId, String configName);**
     Queries *one* field on the form. This method returns the value of the configuration parameter.
     Specify the values for the following parameters:
     configName specifies the value of the _id attribute of the field on the form.

configGroup specifies the literal value "ca_cc_" followed by the value of the _id attribute of the form. An example is ca_cc_form1.
tenantId specifies the business unit ID, for example, ca.com.

- **Map<String, Object> getCatalogConfigValues(String configGroup, String tenantId);**
  Queries *all* fields on the form. This method returns the map of key value pairs. The keys are the values of the _id attributes of the form fields.
  For configGroup and tenantId, the same values apply as for the previous method, Object getCatalogConfigValue.

2. (CA Process Automation) Link the process to one of the following methods in the CA Service Catalog web services. You link the process and the method so that you can retrieve values from fields on a content configuration form:

   - **public String getConfigurationValue(String sessionId, String configGroup, String tenantId, String configName)**

   - **public Map<String, Object> getConfigurationValues(String sessionId, String configGroup, String tenantId)**
     The parameter explanations are the same as for the methods in the previous step, except session ID.
     session ID uniquely identifies the session. This parameter is required and the client uses the value for the remaining web service calls.

     Note: For more information about web services and examples, see the Plug-in Documentation. To access the Plug-in Documentation, log in to CA Service Catalog and click Administration, Tools, Links, Plug-in Documentation.

You have retrieved values from the form fields.

Implement the Content Packs

Implementing the content packs enables you to do *both* of the following tasks:

- As a producer or designer of content packs, package a library of objects including your updates and customizations in a single location.

- As a consumer or adopter of content packs, import the customized objects programmatically in a single operation, as many times as necessary.

You do not have to repeat individual operations for each object type. Content packs provide an efficient method of packaging and applying such updates and customizations, especially when you move from one implementation to another. For example:

- Test-to-production migrations and other same-release migrations

- Replacement of a decommissioned computer

- Restoration of CA Service Catalog customizations after upgrades

To manage the content packs, perform the following tasks:

Step 1 - Complete the Prerequisites

- If you are using CA Process Automation as your process automation tool, verify that you have:
  - Installed and configured CA Process Automation.
  - Integrated CA Service Catalog with CA Process Automation.
- If you use content packs to import CA Process Automation objects and if *both* CA Process Automation and CA Service Catalog are using secure socket layer (SSL), verify that you have completed all applicable tasks for configuring CA Service Catalog to use SSL. As part of that process, you configure CA Process Automation to communicate with CA Service Catalog using SSL.

Step 2 - Create and Export the Content Pack

You create content packs to record (export) customizations so that you can reuse them in another implementation. Using content packs provides greater efficiency and accuracy than repeating multiple customization processes manually.

Follow these steps:

1. Decide and record the objects that you want to include in the content pack.
   You can include any or all of the following categories:
   - API plug-ins
   - CA Process Automation processes
   - Events, including rules, and actions
   - Form Designer forms
   - Policies
   - Report data objects
   - Services, including service hours and request SLAs

   For each category that you select, decide and record which objects to include, as follows:
   - All objects in your implementation; that is, all objects in all business units (domains).

- All objects from one or more specific business units only.
- Only the objects that you specify by object names, for example, in a comma-separated list.
- Only the objects that you specify by object-specific criteria.
  For example, for services, you can specify the last modified date.

Events, rules, actions, and report data objects (including API plug-ins) are *not* specific to any business units. That is, they always apply to *all* business units. The exception is *attached* actions. The attached actions apply *only* to the individual service options that you specify explicitly. Attached actions are service option elements of the service option for which they were created.

2. Select **Start**, **Programs**, **CA**, **CA Service Catalog**, **Service Catalog Command Prompt** on the source computer.
3. Run the following command at this command prompt:

   ```
   ant create-contentpack
   ```

   The Catalog system creates the folder structure for the content pack.
   The Catalog system also prompts you to specify the following information:

   - Simple identification data for the content pack, such as a name, author, and description.
   - The message with which to prompt the user during an import.

   We recommend that you name the *folder* to include the name, version, and locale (language) of the content pack.
   The ant command creates the content pack folder named *USM_HOME* \FileStore\contentpacks*folder-name*. This folder includes the contentpack.properties file. This file stores the identification data for the content pack. This folder also contains several subfolders, including Forms, Policies, Reports, and Services.
4. Answer the prompt about whether to export the objects into this content pack now or later, as follows:

   - If you specify Yes, skip to the next step.
   - If you specify No, run the following command on the source computer:

     ```
     ant export-to-contentpack
     ```
5. Answer the prompts about which objects must be exported, and their attributes.
   The ant command performs the following functions:

   - An XML file for each object is created, using the attributes that you specified.
   - In most cases, copies the XML file to the appropriate subfolder.

   For example, if you exported services, the ant command performs the following functions:

   - A services.xml file is created using the attributes that you specified.

- Copies the services.xml file to the Services subfolder of the content pack folder

The ant command copies some (but not all) categories of objects to their subfolders. Therefore, you copy the remaining categories of objects to their folders manually, as explained in the next step.

6. When prompted, copy the objects that you want to include (if any) to the following subfolders of the content pack folder:

   - **Processes**
     Stores CA Process Automation processes.
   - **Images\Offerings**
     Stores images for the services that you have included the Services subfolder.
   - **Images\RatePlans**
     Stores images for the service option groups that you have included in the Services subfolder.
   - **Prescripts**
     Stores custom scripts to run *before* you import the content pack. Examples include scripts, required to unzip files that are needed for the import or scripts to display the critical information.
   - **Postscripts**
     Stores custom scripts to run *after* you import the content pack. Examples include scripts that load data into the Catalog system or that prompt the user for configuration specifications.
   - **Plug-ins**
     Stores custom API plug-ins.

You have created and exported the content pack on the source computer. You are now ready to import it on the target computer.

Step 3 - Import Content Packs

You import content packs so that you can reuse customizations that you (or another administrator) previously exported from another implementation.

Note: As a best practice, use scheduled down time. Verify that no users are active on CA Service Catalog before you import, enable, or disable content packs.

You can import the content packs using one of the following methods:

- Import Content Packs using the Ant Scripts (see page 3077)
- Import Content Packs from the GUI (see page 3078)

Import Content Packs Using the Ant Scripts

This section describes importing the content packs using the ant scripts.

Follow these steps:

1. Copy the content pack folder (*USM_HOME**FileStore**contentpacks**folder-name* folder) from the source computer to a location on the target computer. Record the location for reference.
2. Select **Start**, **Programs**, **CA**, **CA Service Catalog**, Service Catalog Command Prompt on the target computer.
3. Run the following command at this command prompt:

   ```
   ant import-contentpack
   ```

4. Enter the complete path name of the folder that stores the content pack to import.
5. Perform the following steps:
   a. Confirm that you want to continue the import.
   b. Enter the business unit ID for the content pack. You can specify any business unit, including the root business unit.
   c. Answer the object-specific prompts. When applicable, consider carefully whether to import objects as disabled.
   For example, you import a new rule action that affects the emails that the Catalogs system sends. Before you enable the new rule action, you likely want to update the configuration of your mail server.

   Note: If you import objects as disabled, manually enable them before you can use them.

6. Restart the Windows service named CA Service Catalog if the content pack includes events, rules, or actions. Restart this service on all Catalog Component computers in your environment.

   Important! If you do not restart the CA Service Catalog service as directed, unpredictable results can occur.

You have imported the content pack using the ant scripts. All imported objects are either read-only or permit only limited editing.

Import Content Packs from the GUI

This section describes how you can import the content packs from the GUI.

Follow these steps:

1. Click **Catalog**, **Configuration** in CA Service Catalog UI.
2. Click **Content Packs** in the left menu.
3. Click **Import** tab.
4. Specify the folder where the content pack is stored. Select the content pack zip file and click Open.
5. Clear the **Continue import with default values** check box if you want to import the Content Pack without the default values.
6. Click **Start Import**.
   If the Content Pack includes any CA Process Automation Objects in it, the following three options appear:
   - Set imported version of CA Process Automation objects as the current version:
     - If the option is selected, the imported version of CA Process Automation objects and the current version is same.
     - If the option is not selected, the imported version of CA Process Automation objects and current version is different.
   - Make imported custom operators or sensors available:
     - If the option is selected the operators or sensors that are imported are in Available status in CA Process Automation.
     - If the option is not selected, the operators or sensors are imported as it is present in the content pack.
   - Enter the name of CA Process Automation configuration and import the process definitions to specific CA Process Automation instance.
7. If the content pack includes events, rules, or actions, the Import rules, actions in a disabled state option appears. If the option is selected, the events, rules, or actions in the content pack are imported in disabled state irrespective of the content pack status.
8. Restart the Windows service that is named CA Service Catalog on *all* Catalog Component computers in your environment.

Important! If you do not restart the CA Service Catalog Windows service as directed, unpredictable results can occur.

For example, you import a new rule action that affects the emails that the Catalog system sends. Before you enable the new rule action, update the configuration of your mail server.

Note: Enable the objects manually if you import the objects as disabled.

9. If the content pack includes policies, the Import policies in a disabled state option appear. If the option is selected, the policies in the content pack are imported in disabled state irrespective of the content pack status.

10. Click Continue Import.
The content pack import is successful.

Note: The import of the content packs is blocked with the availability of any .bat or .cmd files in the content packs. Ant scripts are used import the content packs containing .bat or .cmd files.

You have imported the content pack in CA Service Catalog UI. All imported objects are either read-only or permit only limited editing.

When the import of the content pack is complete, the images of the services are copied to the *USM_HOME**Filestore**Images* folder. The Plug-ins are copied to the *USM_HOME**Filestore**Plugins* folder.

Step 4 - Verify the Content Packs

After you import the content packs in CA Service Catalog, you can verify if the content packs were imported successfully in CA Service Catalog.

Follow these steps:

1. Click **Catalog**, **Configuration**, **Content Configuration**.

2. Select the content pack that you imported.

3. Verify the following criteria:

   - The Content Pack Details section lists the details that you specified when you created the content pack, for example, the name, version, and status.

   - The Content section lists the object that you specified, according to the criteria that you specified.

4. Verify that the user interface menus include the imported objects, for example:

- Select **CA Service Catalog**, **Service Offerings**, **Offerings**, **Services**. Verify that the list of services includes any services that you imported.

- Select **Administration**, **Events**. Verify that the list of events includes any services that you imported.

Step 5 - Enable or Disable the Content Packs

You can enable and disable either an entire content pack or individual objects (if applicable) in the content pack. You enable objects in a content pack so that the Catalog system can use the objects. Enabling the imported objects and setting permissions on them work together to let users view and use the imported objects. After you enable objects in a content pack you can disable them, for example, if a problem occurs.

Note: As a best practice, use scheduled down time, verify that no users are active on CA Service Catalog to import, enable, or disable content packs.

Follow these steps:

1. Log in to the business unit that contains the content pack that you want to enable or disable.
2. Click **Catalog**, **Configuration**, **Content Packs**.
3. Click the content pack that you want and enable.
4. Enable or disable objects in the list, as follows:

   - Activate *all objects* in the content pack by clicking the Enable button for the entire content pack. This button appears on the Content Pack Details bar.

     Important! Use this option with caution. The content pack contains rules, action, or policies that perform redundant or conflicting tasks, causing unpredictable results. Therefore, if you are not certain regarding the purpose or goal of the content pack, then enable each object individually.

   - Conversely, deactivate *all objects* in the content pack by clicking the Disable button for the entire content pack.

   - Enable or disable individual objects within a category by clicking the Enable or Disable button for the object.
     You can enable or disable objects in any or all of the following categories:

     - **Services**
       Enabling a service activates its Date Available setting: The service uses its Date Available setting to determine whether and when it is available to users.

- **Service Option Groups**
  Enabling a service option group activates its Date Available setting: The service option group uses its Date Available setting to determine whether and when it is available to users.
  Enabling a service or service option group sets its status to System Object--Available (6). Similarly, disabling a service or service option group sets its status to System Object--Unavailable (7).

- **Policies**
  You enable a policy to set its status to Active, and disable a policy to set its status to Inactive.
  You can make only limited updates to imported polices that you have enabled. To make more updates to such policies, copy and modify them.

- **Rules**
  You enable or disable rules individually, without affecting the status of any other rules in the same event.
  Enabling or disabling a rule does not automatically enable or disable the actions in the rule. The actions remain in the original status.

- **Actions**
  You enable or disable actions individually, without affecting the status of any other actions in the same rule. Similarly, enabling or disabling an action does not affect the status of the rule that contains the action.

Enabling and disabling does not apply to the following objects: Events, forms, reports, images, and CA Process Automation processes. You specified during the import process whether to make CA Process Automation processes active or inactive.

5. Click **Done**.

6. (Optional) Verify that the object is enabled (active) or disabled (inactive) by viewing its status. For example, select Services, *folder-name*, and open a service that you enabled. Verify that its status is System Object--Available. Also verify that its Date Available meets your requirements.

You have enabled or disabled objects in the content pack. All objects that you enabled are available in the Catalog system.

Note: If you copy and customize an object from a content pack, the customized object is *not* affected by enabling or disabling the content pack.

Step 6 - Modify the Imported Objects

The actions that you can perform on the objects that are imported from a content pack vary by object. When applicable, you perform certain actions on certain imported objects so that users can view and use the objects. The following table shows which actions apply to which objects.

Object	Enable or Disable	Set Permissions	Limited Editing
Services	Y	Y	Y
Service Option Groups	Y	Y	Y
Policies	Y	Y	Y
Events	N	Y	N
Rules	Y	Y	N
Actions	Y	Y	N
Forms	N	Y	N
Report Data Objects	N	Y	N
Images	N	N	N

The actions are as follows:

- **Enable or disable**
  You enable objects so that users and the Catalog system can use them. For example, suppose that your content pack includes policies. You enable these policies so that the Catalog system can use them and manages requests. Similarly, your content pack includes services and you enable these services for the users to view and request the services. For any reason, such as a problem occurring, you can disable any objects that you have enabled.

- **Set permissions**
  To set permissions for each Catalog role on an imported object, use the portion of the UI that stores and maintains the object. For example, to set permissions for services, select Catalog, Service Offerings, Services, Permission, and edit the service details.
  Edit limited attributes
  Typically, imported objects are read-only. You can perform only limited editing on certain imported objects, as follows:

  - For services and service options, you can change the date available and date unavailable.
  - For policies, you can add or remove approvers, change the priority, and set the status as active or inactive.

  Otherwise, to customize an imported object, copy, and modify it. For example, to customize an imported report data object, copy and modify it.

Step 7 - Customize the Imported Objects

To customize an imported object, copy and modify it. For example, to add a field to an imported form, copy the form, rename it, and add the field.

You can customize a service, service option group, or a form. The common customizations are as follows:

- Adding, deleting, and modifying the service option groups or the image in the service.
- Setting the dates that the service is available or unavailable.

Note: For more information about performing these tasks, see the Manage Services (see page 2987), Manage Service Option Groups (see page 3011), Manage Service Options and Service Option Elements, (see page 3017) or Manage Forms (see page 2914) sections.

Important! If you copy and customize an object that you imported in a content pack, copy and customize all *parent* objects that include the original object. This requirement exists because forms, services, and service option groups allow only limited editing.

Follow this process to copy a form, customize the copy, and include the form in a service option group and service that are based on the original service option group and service in the content pack:

1. Copy Form A and modify the copy, creating Form B.
   Service Option Group A (SOG A) contains Form A. You cannot modify SOG A to replace Form A with Form B, because SOG A allows only limited editing. So, you perform the next steps.
2. Copy SOG A to create SOG B.
3. Update SOG B by deleting Form A and adding Form B.
   Service A contains SOG A. You cannot modify Service A to replace SOG A with SOG B, because Service A allows only limited editing. Therefore, you perform the next steps.
4. Copy Service A to create Service B.
5. Update Service B by deleting SOG A and adding SOG B.
6. Copy Folder A to create Folder B.
7. Update Folder B by deleting Service A and adding Service B.

The following table lists the parent objects that you must copy and customize if you copy and customize a child object.

Child	Parent
Form	Service Option Group
Service Option Group	Service
Service	Folder
Folder	Parent Folder

Use CA Service Catalog Content Packs

This content pack contains a folder named Service Management with a subfolder named Asset Services for the business unit in which you import the content pack.

The Asset Services folder (available in Catalog, Service Offerings, IT Support Services, Service Management) stores the services for *Request a Hardware Asset* and *Request a Hardware Asset (for mobile users)*. The other services are available in Catalog, Service Offerings, IT Support Services, Service Management folder.

Services

The content pack provides the following service offerings:

- **My Resources**
  Lets business users view all the devices, software, and applications that are assigned to them. For example, the resources can be computers, mobile phones, or software that is installed on the devices. Business users can access this service and the items that it includes through a mobile device, laptop, desktop, or a server.
  The My Resources service does not require any approval process. This service offering is of type informational service.

- **Problem with My Resource**
  Lets business users report an issue with the resources that are assigned to them and are listed under My Resources. The Problem with My Resource service is used only with the My Resources service. When business users use this service, the application displays the information corresponding to the selected resource.
  The Problem with My Resource service does not require any approval process.

- **Reset Application Password**
  Lets business users reset the password of any application that they have subscribed to. Typically, an application is a software program that is not installed on your computer. For example, a web-based defect tracking tool is an application. You may not have installed the tool on your computer, but you access it using a web browser.
  The Reset Application Password service is a self-service feature. It helps business users reset their passwords without having to raise Service Desk tickets. The service and the items that it includes can be accessed through a mobile device, laptop, desktop, or a server.
  The Reset Application service does not require any approval process. This service offering is only an informational service.

- **Reset User Password**
  Lets business users reset their domain passwords. The service is an example of automating the procedure to reset a user password in Active Directory.
  This service offering does not require any approval process.

- **Report an Issue**
  Lets business users report an issue (incident) in CA Service Desk Manager. For example, a CA Service Catalog user can use this service to report a broken laptop in CA Service Desk Manager and arrange for a repair or replacement.
  Business users can access this service and the items that it includes through a mobile device, laptop, desktop, or a server.
  The Report an Issue service has no approval process, because the service is only for reporting an issue. When the request reaches Pending Fulfillment status, the incident is created in CA Service Desk Manager. After this incident is created, the request reaches Request Opened status. The incident IDs are attached to the request, and notes and attachments are synchronized between CA Service Catalog and CA Service Desk Manager.

- **Request a Hardware Asset**
  Lets catalog users select and request a hardware asset.

- **Request a Hardware Asset (for mobile users)**
  Lets catalog users request a hardware asset from a mobile device.

The following table provides the details of the Option Groups available for the services:

Service	Option Group	Option	Items in the Option Group
My Resources	My Resources	My Resources	My Resources form
Reset Application Password	Reset Application Password	Reset Application Password	Reset Application Password form
Reset User Password	Reset User Password	Reset User Password	Reset User Password form
Report an Issue	Report an Issue	Report an Issue	Report an Issue form
Request a Hardware Asset	Request a Hardware Asset	Request a Hardware Asset	Request a Hardware Asset
Request a Hardware Asset (for mobile users)	Request a Hardware Asset (for mobile users)	Request a Hardware Asset (for mobile users)	Request a Hardware Asset (for mobile users)

Note: All the Service Option Groups are available in Catalog, Service Offerings, Option Groups.

Forms

The content pack provides the following forms:

- **My Resources Configuration**
  Lets administrators configure the options that display the resources assigned to a user.

- **SAM Configuration**
  Lets administrators configure the CA Software Asset Manager server details. This enables retrieving the software and displaying it in My Resource for business users.

- **Reset Password Configuration**
  Lets administrators map applications with their knowledge documents. This helps end-users know the procedure to reset their passwords for applications.

- **Reset User Password**
  Lets catalog users configure the fields that are displayed for end-users to reset their domain passwords.

- **Reset Application Password**
  Lets administrators configure the fields that are displayed for end-users. These fields help end-users reset the password for the applications they have access to.

- **Report an Issue service**
  This service includes a service option group named Report an Issue, which includes a form named Issue Details. This form lets catalog users provide details for an issue to the service desk and request help. Users enter a description and assign the issue to a CA Service Desk Manager category. This form is the only form that catalog users see.

- **SDM Incident Configuration**
  Lets administrators define settings or attributes that CA Service Catalog creates in CA Service Desk Manager. This form is also used to define settings or attributes that CA Service Desk Manager creates in CA Service Catalog.

- **Issue Details**
  Lets catalog users use this form to provide details of an issue to the service desk and request help. Users enter a description and assign the issue to a CA Service Desk Manager category.

- **Request a Hardware Asset**
  Lets catalog users select and request a hardware asset.

- **Request a Hardware Asset (for mobile users)**
  Lets catalog users request a hardware asset from a mobile device.

The *Request a Hardware Asset* and *Request a Hardware Asset (for mobile users)* are available in Catalog, Forms, CA Catalog Content, Service Management Forms, Asset Service. All the other forms are available in Catalog, Forms, Forms folder, CA Catalog Content, Service Management Forms

Plug-ins and Default Locations

The plug-ins that are available in the content pack also include the source code. You can copy the code and can customize it to suit your requirements. To customize the code, copy the Java files into any folder of your choice and modify as required. Ensure that the plugin_class attribute in the plugin.properties file includes the modified folder path.

To view the plug-ins, go to Administration, Tools, Plug-ins. The following plug-ins are available in the content pack:

Imported Object	Plug-in
My Resources	USM_HOME\filestore\plugins\ ca.catalog.content.resource-plugin
Reset Application Password	USM_HOME\filestore\plugins\ ca.catalog.fetchallservicedeskapplicationareas.plugin USM_HOME\filestore\plugins\ ca.catalog.fetchkbapplications.select-plugin USM_HOME\filestore\plugins\ ca.catalog.fetchkbdocument.select-plugin

Imported Object	Plug-in
	USM_HOME\filestore\plugins\ ca.catalog.fetchservicedeskapplicationareas.plugin
Reset User Password	USM_HOME\filestore\plugins\ ca.catalog.updateactivedirectoryuserpassword.select-plugin
Common	USM_HOME\filestore\plugins\ ca.catalog.samples.configurationreader-plugin
Plug-in for fetching incident areas from CA Service Desk Manager	ca.catalog.servicedesk-select-plugin

Events, Rules, and Life Cycle

The following table lists the action that apply to the Request/Subscription Item Change event:

Event	Status	Action
Request/Item Subscription Change	Not Applicable	When a Note or an Attachment is added to CA Service Catalog, this event triggers CA Process Automation process to synchronize with CA Service Desk Manager.

The following table lists the action that applies to the different rules:

Rule	Status	Action
When Category is Service Management Content	Canceled	Cancel Incident
When Category is Service Management Content	Completed	Close Incident
When Category is Service Management Content	Pending Fulfillment	Create Incident

Typically, you do not need to customize these rules and actions.

Verify the General Prerequisites

To verify that you can use the content packs as intended, complete the prerequisites. For more information about the prerequisites for individual offerings and services, see the corresponding section.

Software Prerequisites:

This content pack requires integrations with other applications. Ensure that you install the following components:

- CA Service Desk Manager 12.9 or higher
- CA Asset Portfolio Management 12.9 or higher
- CA Software Asset Manager 12.9 or higher
- Microsoft Active Directory 2008 R2

General Prerequisites:

The following prerequisites apply to all content packs:

- Restart the CA Service Catalog Service.
- Have a working knowledge of content packs, including how to import and verify the import, and how to enable and disable the objects in the content pack. For more information about importing a content pack, watch this video.
- Understand that you can edit only limited attributes of the objects that you import from the content pack. To make further changes, copy the objects and customize the copies. You must have a working knowledge of how to copy and modify any object that you want to modify, and all its parent objects. For more information about how to customize the content, watch this video.
- Follow these steps to update the Problem with My Resource offering ID, Reset User Password offering Id, and Report an Issue offering Id in the Content Configuration page.

  Note: Ensure that you update these IDs before using the My Resources and Reset Password service offerings.

  1. Log into CA Service Catalog as an administrator.
  2. Go to **Catalog**, **Service Offerings**, **IT Support Services**, **Service Management**.
  3. Select the ID from the required service offering.
  4. Use this ID value to update the existing value in the Content Configuration page (**Catalog**, **Configuration**, **Content Configuration**).
  5. Click **Save** after you update the configuration details.
     The offering ID has been updated.

Use My Resources Service

The *My Resources* offering lets business users view all the devices, software, and applications that are assigned to them. For example, the resources can be computers, mobile phones, or software that is installed on the devices.

Prerequisites:

Before going through this topic, ensure that you verify the general prerequisites (see page 3087).

The following prerequisites apply for using the *My Resources* offering:

- CA Service Catalog is integrated with CA Service Desk Manager and CA Asset Portfolio Management.
- CA Software Asset Manager configuration and My Resources configuration details are updated under **Catalog**, **Configuration**, **Content Configuration**.

The following video demonstrates how to use the My Resources offering:

Use Reset Password Service

The Reset Password offering consists of two parts:

- Reset Application Password
- Reset User Password

Prerequisites:
Before going through this topic, ensure that you verify the general prerequisites (see page 3087).
The following prerequisites apply for using the Reset Password offering:

- The Active Directory server is installed and configured.
- The alternate email address is added to Active Directory.
- Ensure that the Active Directory Certificate Services are installed.
- The reset password offering ID is mentioned in the Reset Password Configuration form.

Add the alternate email address to Active Directory

To add an alternate email address to Active Directory, you must first add the custom attribute Alternate Email to the Active Directory User class. To add a custom attribute, you modify the Active Directory schema. Adding custom attribute requires that the modifying user be a member of the Schema Administrators and Enterprise Administrators groups.

Follow these steps to add a custom attribute to the user object:

1. Register the schema snap-in.
2. Create a custom attribute.
3. Add the custom attribute to the user class.
4. Restart the Active Directory Domain Services.

Follow these steps to register the schema snap-in:

1. Press Windows + R on your keyboard.
2. Type RegSvr32 SchmMgmt.dll and click OK.
   When the schema snap-in is registered, a confirmation message appears.

Follow these steps to create a custom attribute:

1. Press Windows + R on your keyboard.
2. Type mmc.exe and click OK.

3. Click File, Add/Remove snap-in, or simply press Ctrl + M.

4. Select the snap-in Active Directory Schema, click Add >, and then click OK.

5. Expand the Active Directory Schema root node, right-click the node Attributes, click Create Attribute.

6. If the Schema Object Creation warning message appears, click Continue.

7. Create the custom attribute Alternateemail. Complete the following fields:

   - Common Name: Enter Alternate Email
   - LDAP Display Name: Enter alternateemail
   - Unique X500 Object ID: Enter the object ID that is applicable for your domain.
   - Syntax: Select Unicode String

8. Click OK.
   The new custom attribute Alternateemail is created and displayed in child node of Attributes.

Follow these steps to add the custom attribute to the user class:

1. Navigate to the node Active Directory Schema, Classes, and select the class User.

2. Right-click the User class and click Properties. Go to the Attributes tab and click Add.

3. Select the schema object alternateemail and click OK.
   This adds alternateemail as an optional attribute for the User class.

4. Click Apply.
   You have successfully added the alternate email attribute to the User class.

Restart the Active Directory Domain Services

After you have created the custom attribute and added it to the User class, you must restart the Active Directory domain service to apply the schema change.

Follow these steps:

1. Press Windows + R on your keyboard.

2. Type services.msc and click OK.

3. Right-click Active Directory Domain Services and click Restart, and then click Yes.
   All the related services are restarted.

Follow these steps to create the Active Directory Certificate and use it:

1. Create an Active Directory Certificate File on the computer where Active Directory is hosted.

2. Register the certificate in CA Service Catalog.

Follow these steps to create the Active Directory Certificate:

1. Log in to a computer where Active Directory is installed.
2. Open a Command Prompt window using the Run as Administrator option.
3. Type MMC and press Enter.
   The Microsoft Management Console opens.
4. Click File, Add/Remove Snap-in.
5. Select Certificate in the Available snap-ins section, click Add to move it to the Selected snap-ins section, and then click OK.
6. Select Computer account and click Next.
7. Select Local computer: (the computer this console is running on), and click Finish.
   The Add or Remove Snap ins page opens. The Certifications (Local Computer) is added to Selected snap-ins.
8. Click OK.
   The Add or Remove Snap-ins wizard closes.
9. Expand Certificates (Local Computer) in the Console and then expand Personal.
10. Right-click Certificates, select All Tasks, and then select Request New Certificate.
    The Certificate Enrollment wizard opens.
11. Read the instructions and click Next.
    The Select Certificate Enrollment Policy page opens.
12. Verify that Active Directory Enrollment Policy is selected, and click Next.
    The Request Certificates page opens.
13. Select Domain Controller, Domain Controller Authentication, and click Enroll.
    The Certificate Installation Results page opens.
14. Verify that the status is Succeeded for both policies, and click Finish.
15. Verify that there are three certificates under Certificates, in the Console.
16. Right-click the certificate with the Intended Purpose of <All>.
17. Select All Tasks and Export.
    The Certificate Export Wizard opens.
18. Click Next.
    Select the option No, do not export the private key, and click Next.
19. Select DER encoded binary X.509 (.CER), and click Next.
20. Browse and create a folder called Certificate (\Certificate).

21. Name the certificate file to identify it (for example, ITSM-AD.cer) and click Next.
    The Completing the Certificate Export page opens.

22. Verify the Certification Export information and click Finish. Click OK.

23. Close the Microsoft Management Console.

24. Click Yes and Save to save the Console.
    A Certification File (for example, ITSM-AD.cer) is created in the Certification folder on the Domain Controller.

25. Copy the Certification File (ITSM-AD.cer) to the computer where CA Service Catalog is installed.

Follow these steps to register the certificate in CA Service Catalog:

1. Log in to a computer where CA Service Catalog is installed.

2. Go to [USM_Home]\view\conf and open the viewService.conf file.

3. Find the Djavax.net.ssl.trustStore parameter under Java Additional Parameters, and get the value of the parameter. Identify the keystore.
   For example, if the key store value is "C:/Program Files (x86)/Java/jdk1.7.0_40/jre/lib/security /cacerts", navigate to the directory C:\Program Files (x86)\Java\jdk1.7.0_40\jre\bin.

4. Run the following command where ITSM-AD.cer is the name of the file from your Active Directory server:
   keytool -import -keystore ..\lib\security\cacerts -alias ADCertificateRegistration -file C:\ITSM-AD.cer

5. Enter the keytool password, which is available in the 'Djavax.net.ssl.trustPass' parameter value in the viewService.conf file.
   The message Trust this certificate? [no]: appears.

6. Enter yes and confirm the key import.

Change the Reset Password Offering ID

If you want to modify the Reset User Password form and include other details, change the Reset Password Offering ID.
Follow these steps:

1. Log in into CA Service Catalog as Service Delivery Administrator or Catalog Administrator.

2. Specify the new Reset Password Offering ID in the Reset Password Configuration form. Click Save.

Note: The new offering ID is generated when you copy the default Reset Password offering and create a custom form.

3. Log in into EEM using the CA Service Catalog instance.
4. Click Manage Access Policies and click the offering.
5. Click ACL_Guest_Offering.
6. Remove all resources except "_preventWildcardMatch__ACL_Guest_Offering".
7. Add the resource "offering__<new reset password offering id>".

> **Note:** This offering ID is generated when you copy the default Reset Password offering and create a custom form.

8. (Optional) To find the offering ID, log in to CA Service Catalog and click the new Reset Password Service offering. The Id is displayed in the Details tab.
   For example suppose that the offering is under ca.com (Id = 10001), IT Support Services (Id = 10013), Service Management (Id = 10048). When you click a service offering or a folder, the offering ID is displayed in the Details tab. Per the example, add the following resources to the ACL_Guest_Offering policy:
   - offering__10001
   - offering__10013
   - offering__10048
9. Click Save. Click Configure, Session, Synchronize Cache.
10. Restart CA service Catalog.

The following video demonstrates how to use the Reset Password offering:

Use Report an Issue Service

The *Report an Issue* service creates an incident in a predefined (default) implementation of CA Service Desk Manager. If you have customized CA Service Desk Manager to match your business needs, copy and customize the service to match your implementation.

Before going through this topic, ensure that you verify the general prerequisites (see page 3087).

Follow these steps:

1. Understand how the Catalog system creates and populates a CA Service Desk Manager incident.
2. Include custom attributes in the CA Service Desk Manager incident.
3. Customize status codes, attribute prefixes, and other details for the CA Service Desk Manager incident.

4. Review the guidelines and limitations for the Report an Issue service and your custom versions of it.

5. Follow the guidelines for using and customizing rules and actions.

The following video demonstrates how to use the Report an Issue service:

Retry Failed Attempts to Create CA Service Desk Manager Incidents

At times, a catalog user submits a request for the Report an Issue service. But the attempt to create the incident in CA Service Desk Manager fails. In such cases, the Catalog system reports the failed attempts as alert messages (alerts). The system issues one alert per incident. For example, if a service contains two service options that create an incident, the system issues two alerts. A common reason for failed attempts is a temporary network problem that makes CA Service Catalog inaccessible to CA Service Desk Manager. After the problem is resolved, retry the failed attempts.

Follow these steps:

1. Log in to CA Service Catalog as Service Delivery Administrator.

2. Click **Home**, **Messages**, **Alerts**.

3. Click **List All Failed Actions**, and proceed as follows:

    a. If necessary, click Change Business Unit to display the list of alerts that include the failed actions you want to retry.

    b. Retry all Incident Creation Failures of the following type: INCIDENT_CREATION_FAILED.

4. Select five or fewer rows and click **Retry Failed Actions**.
   If the retry fails, the Catalog system marks the alert as Retried, and issues a new failure alert that you can retry again later.
   If the retry succeeds also, the Catalog system marks the alert as Retried. You can view the request and its corresponding ticket in CA Service Desk Manager.

Synchronize Attachments and Notes between CA Service Catalog and CA Service Desk Manager

You can synchronize notes and attachments between CA Service Catalog and CA Service Desk Manager.

Follow these steps:

1. Log in to CA Service Catalog as Service Delivery Administrator.

2. Click **Administration**, **Event-Rules-Actions**.

    a. Open the **Document Create** event type.

    b. Select the **When attachment is added to Service Catalog request** rule and click **Enable** .

    c. Enable the Launch PAM SRF to sync Attachments action.

This action synchronizes the attachments between service options and tickets after the ticket is created. That is, if a business user adds an attachment to a service option after submitting the request, this action passes the attachment to the related ticket.

3. Follow these steps to synchronize notes:

    a. Open the **Notes Create** event type.

    b. Select the **When note is added to Service Catalog request** rule and click Enable.

    c. Enable the Launch PAM SRF to sync notes action.

    This action synchronizes notes between service options and tickets after the ticket is created. That is, if business user adds a note to a service option after submitting the request, this action passes the note to the related ticket.

Use Asset Services

To use the *Asset Services* offering, follow these processes.

Before going through this topic, ensure that you verify the general prerequisites (see page 3087).

Request a Hardware Asset Service

Follow this process to create a custom service for requesting a hardware asset from CA Asset Portfolio Management. In this process, you copy the Request a Hardware Asset service and customize the copied objects.

1. Select **Administration**, **Events-Rules-Actions**, and perform these actions:

    a. Open the event named **Request/Subscription Item Change**.

    b. Enable and open the rule named **When Category is Hardware and Status is Pending Fulfillment**.

    c. Enable the action named **Auto assign the selected asset to the user**.
    After all approvals are supplied and the request reaches Pending Fulfillment status, this action automatically assigns the CA Asset Portfolio Management asset to the Requested For user. If this action is not enabled, an administrator must fulfill the request manually, using gold brick icon.

    Note: You perform this step only once per business unit. Unlike the remaining steps, you do not perform this step each time that you create a service.

2. Create a folder and copy the Request a Hardware Asset service from the content pack to the new folder.

Note: Copy all objects in the service.

3. Rename the folder, service, service option group, service option, and form to intuitive names. An example is Request a Hardware Asset--custom-V1.

4. Meet the following requirements:

   - Assign models to a service option.
   - Verify that this service option is included in a service option group in the service.
   - Understand that the Request a Hardware Asset form uses a hidden field named Selected Assets' Id to store the UUID of the IT Asset Manager asset that the user selects.

     Important! Do not modify or replace this field. If you decide to modify or replace this field for any reason, the new or modified field must use the same value for the _id attribute as the original field: ca_itam_attr_asset_id. Otherwise, the selected asset is not assigned properly.

   - When the request for the selected asset is approved, the Assign Asset action from the content pack (or your custom version of that action) assigns that UUID to the Requested For user specified in the request.

5. Verify the following requirements for using the report data object (data object) from the content pack:

   - The catalog user and the assets must have the same location.
   - The assets must not have been assigned to any user.
   - The assets must be active in status.

6. (Optional) If the CA Service Catalog database runs on SQL Server, you can optionally create and use a custom query that removes one or more of the restrictions in the predefined data object for requesting a hardware asset.
   This topic illustrates the process to remove the restriction that users and assets have the same location. You can use this topic as a model to make similar customization to your queries. Follow this process:

   a. **Create a data object with your custom query:**

      i. Click **Administration**, **Report Builder**, **Data Objects**.

      ii. Expand **Catalog**.

      iii. Open the data object named **Fetch Hardware Assets to Assign - Table Provider** .

      iv. Copy the fields of this report data object to a Notepad file. The fields include Database, Table, Fields, and Query.

v. Create a data object. Specify an intuitive name, for example, Fetch Hardware Assets--Custom-version1.

vi. Copy and paste the text from the Notepad file to each field of the new data object.

vii. Update the query in the new data object to remove the location requirement. The updated query appears as follows:

```
SELECT cc.resource_name AS ca_itam_attr_asset_name,cc.host_name AS
ca_itam_attr_host_name,cs.name AS ca_itam_attr_resource_family,
cv.name AS ca_itam_attr_resource_class,lc.name AS
ca_itam_attr_lifecycle_status,sc.name AS ca_itam_attr_cost_center,
bb.location_name AS ca_itam_attr_location_name,cc.resource_name,
CONVERT(CHAR(100),own_resource_uuid,1) AS
ca_itam_attr_asset_id_temp
FROM ca_owned_resource cc
JOIN ca_model_def cl ON cc.model_uuid = cl.model_uuid
JOIN usm_link_rateitem_model lrm ON cl.model_uuid=lrm.model_uuid
JOIN usm_rate_definition r ON lrm.rate_item_id=r.item_id
JOIN usm_offering_ratedef_inclusion ori ON r.item_id=ori.child_id
JOIN usm_offering o ON ori.parent_id=o.offering_id
JOIN ca_resource_family cs ON cc.resource_family = cs.id
JOIN ca_resource_class cv ON cc.resource_class = cv.id
LEFT OUTER JOIN ca_asset_lifecycle_status lc ON cc.
lifecycle_status = lc.id
LEFT OUTER JOIN ca_resource_cost_center sc ON cc.cost_center = sc.
id
LEFT OUTER JOIN ca_location bb ON cc.location_uuid = bb.
location_uuid
WHERE cc.resource_contact_uuid IS NULL AND cc.inactive='0' AND cl.
name=(SELECT cl.name WHERE cl.inactive='0' AND cl.family_id='%
family_id%' AND o.offering_id='%offeringid%')
```

viii. Copy the ID of this new report data object to a Notepad file. You use this information in the next procedure

b. **Copy and customize the form to accommodate the new object**

i. Select **Catalog**, **Forms**.

ii. Expand **Forms**, **CA Catalog Content**, **Service Management Forms**, **Asset Services**, **Request a Hardware Asset** and review the value of the Report/Plug-in Variables attribute in the original form

iii. Select the **Select An Asset** field and review the value of the Report/Plug-in Variables attribute.
The original value of the attribute follows:
$({'offeringid':_.service.id,'family_id':'600','location':_.user.location.uuid})

iv. Copy the form. Specify an intuitive name, for example, Request a Hardware Asset--Custom-version1.

v. Update the following attributes of the Select An Asset field:

vi. Report/Plug-in Id: Replace the existing value with the ID of the new report data object that you created in the previous procedure.

vii. Report/Plug-in Variables: Remove the location requirement.
The updated value appears as follows:
$({'offeringid':_.service.id,'family_id':'600'})

7. (Oracle Users Only) Replace the SQL Server query in the content.
The predefined queries in the data objects in the content pack are for SQL Server only. Therefore, if the CA Service Catalog database runs on Oracle, create a custom query for Oracle that performs the same functions as the predefined query.

   - Create an Oracle query for requesting hardware assets (see page 3098).
   - Create an Oracle query for requesting hardware assets (for mobile users) (see page 3099).

8. You can use the predefined or custom approval process of your choice.

Create an Oracle Query for Requesting Hardware Assets

Create an Oracle query for requesting hardware assets, for use in a service that users submit from a laptop or desktop computer (not a mobile device).

Follow this process:

- Step 1 - Create a data object with your custom query (see page 3098)
- Step 2 - Copy and customize the form (see page 3099)

Step 1 - Create a data object with your custom query

1. Select **Administration**, **Report Builder**, **Data Objects**.

2. Create a data object. Specify an intuitive name, for example, Fetch Hardware Assets–RequestedFromLaptop.

3. Configure the new data object to perform the same functions for Oracle as the original data object for SQL Server.
Use this query as a model to create your query. This query includes the location requirement. Remove it if you do not want it.

```
Database: mdb
Fields: ca_itam_attr_asset_name,ca_itam_attr_host_name,
ca_itam_attr_resource_family,ca_itam_attr_resource_class,
ca_itam_attr_lifecycle_status, ca_itam_attr_location_name,
ca_itam_attr_cost_center,resource_name,item_id,ca_itam_attr_model_name,
ca_itam_attr_location_uuid,ca_itam_attr_asset_id_temp
Query: SELECT cc.resource_name AS ca_itam_attr_asset_name,cc.host_name AS
ca_itam_attr_host_name,cs.name AS ca_itam_attr_resource_family, cv.name AS
ca_itam_attr_resource_class,lc.name AS ca_itam_attr_lifecycle_status,sc.name AS
ca_itam_attr_cost_center,bb.location_name AS ca_itam_attr_location_name,cc.
resource_name, CAST(own_resource_uuid AS CHAR(100)) AS
ca_itam_attr_asset_id_temp FROM ca_owned_resource cc
JOIN ca_model_def cl ON cc.model_uuid = cl.model_uuid
JOIN usm_link_rateitem_model lrm ON cl.model_uuid=lrm.model_uuid
JOIN usm_rate_definition r ON  lrm.rate_item_id=r.item_id
JOIN usm_offering_ratedef_inclusion ori ON r.item_id=ori.child_id
JOIN usm_offering o ON ori.parent_id=o.offering_id
JOIN ca_resource_family cs ON cc.resource_family = cs.id
JOIN ca_resource_class cv ON cc.resource_class = cv.id
LEFT OUTER JOIN ca_asset_lifecycle_status lc ON cc.lifecycle_status = lc.
id
LEFT OUTER JOIN ca_resource_cost_center sc ON cc.cost_center = sc.
```

```
id
LEFT OUTER JOIN ca_location bb ON cc.location_uuid = bb.
location_uuid
WHERE cc.resource_contact_uuid IS NULL AND cc.inactive='0' AND CAST(cc.
location_uuid AS CHAR(100))='0x' + '%location%' AND cl.name=(SELECT cl.name
FROM ca_model_def cl WHERE cl.inactive='0' AND cl.family_id='%family_id%' AND o.
offering_id='%offeringid%')
```

4. Copy the ID of this new report data object to a Notepad file. You use this information in the next procedure.

Step 2 - Copy and customize the form

1. Review the value of the Report/Plug-in Variables attribute in the original form in the content pack, as follows:

   a. Select **Catalog**, **Forms**.

   b. Expand **Forms**.Select **CA Catalog Content**, **Service Management Forms**, **Asset Services**, **Request a Hardware Asset**.

   c. Click the **Select An Asset** field and review the value of the Report/Plug-in Variables attribute.
   The original value of the attribute follows:
   $({'offeringid':_.service.id,'family_id':'600','location':_.user.location.uuid})

2. Copy the form. Specify an intuitive name, for example, Request a Hardware Asset--From a Laptop.

3. Update the Report/Plug-in Id attribute of the Select An Asset field: Replace the existing value with the ID of the new report data object that you created in the previous procedure.

Create an Oracle Query for Requesting Hardware Assets (for Mobile Users)

Create an Oracle query for requesting hardware assets, for use in a service that users submit from a mobile device.

Follow this process:

- Step 1 - Create a data object with your custom query (see page 3099)
- Step 2 - Copy and customize the form (see page 3100)

Step 1 - Create a data object with your custom query

1. Select **Administration**, **Report Builder**, **Data Objects**.

2. Create a data object. Specify an intuitive name, for example, Fetch Hardware Assets–RequestedFromMobile.

3. Configure the new data object to perform the same functions for Oracle as the original data object for SQL Server.
   Use this query as a model to create your query. Test your query thoroughly before making the service that includes it available to catalog users. This query includes the location requirement. Remove it if you do not want it.

```
Database: mdb
Fields: ca_itam_attr_asset_id,ca_itam_attr_asset_name,ca_itam_attr_host_name,
ca_itam_attr_resource_family,ca_itam_attr_resource_class,
ca_itam_attr_lifecycle_status,ca_itam_attr_location_name,
ca_itam_attr_cost_center,resource_name,item_id,ca_itam_attr_model_name,
ca_itam_attr_location_uuid
Query: SELECT CAST(own_resource_uuid AS CHAR(100)) AS ca_itam_attr_asset_id,cc.
resource_name + ', ' + cl.name AS ca_itam_attr_asset_name,cc.host_name AS
ca_itam_attr_host_name,cs.name (http://cs.name) AS ca_itam_attr_resource_family,
cv.name AS ca_itam_attr_resource_class,lc.name AS ca_itam_attr_lifecycle_status,
sc.name AS ca_itam_attr_cost_center,bb.location_name AS
ca_itam_attr_location_name,cc.resource_name
FROM ca_owned_resource cc
JOIN ca_model_def cl ON cc.model_uuid = cl.model_uuid
JOIN usm_link_rateitem_model lrm ON cl.model_uuid=lrm.model_uuid
JOIN usm_rate_definition r ON  lrm.rate_item_id=r.item_id
JOIN usm_offering_ratedef_inclusion ori ON r.item_id=ori.child_id
JOIN usm_offering o ON ori.parent_id=o.offering_id
JOIN ca_resource_family cs ON cc.resource_family = cs.id
JOIN ca_resource_class cv ON cc.resource_class = cv.id
LEFT OUTER JOIN ca_asset_lifecycle_status lc ON cc.lifecycle_status = lc.
id
LEFT OUTER JOIN ca_resource_cost_center sc ON cc.cost_center = sc.
id
LEFT OUTER JOIN ca_location bb ON cc.location_uuid = bb.
location_uuid
WHERE cc.resource_contact_uuid IS NULL AND cc.inactive='0' AND CAST(cc.
location_uuid AS CHAR(100))='0x' + '%location%' AND cl.name=(SELECT cl.name
FROM ca_model_def cl WHERE cl.inactive='0' AND cl.family_id='%family_id%' AND o.
offering_id='%offeringid%')
```

4. Copy the ID of this new report data object to a Notepad file. You use this information in the next procedure.

Step 2 - Copy and customize the form

1. Review the value of the Report/Plug-in Variables attribute in the original form in the content pack, as follows:

    a. Select **Catalog**, **Forms**.

    b. Expand **Forms**. Select **CA Catalog Content**, **Service Management Forms**, **Asset Services** , **Request a Hardware Asset (for Mobile Users)**.

    c. Click the **Select An Asset** field and review the value of the Report/Plug-in Variables attribute.
    The original value of the attribute follows:
    $({'offeringid':_.service.id,'family_id':'600','location':_.user.location.uuid})

2. Copy the form. Specify an intuitive name, for example, Request a Hardware Asset--From Mobile Devices.

3. Update the Report/Plug-in Id attribute of the Select An Asset field: Replace the existing value with the ID of the new report data object that you created in the previous procedure.

Best Practices for Service Catalog Management

IT organizations have focused on technology without clear accountability for adding business value, while their customers have focused on costs. Increased competition in the marketplace and increased dependence on high technology demand that IT organizations:

- Build a stronger understanding of the customers they serve.
- Work in a close partnership with them to deliver true value.

These business alignment initiatives require:

- A clear definition of the services that the IT organization provides.
- An understanding of the components and resources that constitute the services.
- An identification of the costs of the associated services.

With centralization of IT services and movement toward a utility model, implementing a service catalog becomes an increasingly important necessity. Using a service catalog leads to better IT service alignment with business goals and improved internal customer satisfaction. It also leads to standardized processes to achieve greater operational efficiency.

The ITIL™ (IT Infrastructure Library) framework stipulates that IT organizations start their process enhancement initiatives by developing a service catalog to:

- List all the services being provided
- Summarize the details of the services, customers, service designers, and service administrators.

Many IT groups produce a service catalog as part of their ITIL Service Level Management deployment. Others view the opportunity to leverage the service catalog as the focal point for communication between IT and the business.

Benefits

CA Service Catalog enables you to load catalog content and to enable related business process automation through CA Process Automation. The goal of this initiative is not to create a complete and comprehensive list of services. Instead, the goal is to help you get started in building your own catalog.

As the foundation for aligning IT with the business, service catalog represents a crucial element of success in ITIL initiatives. By using a service catalog, IT organizations can:

- Create clear service definitions.
- Define service levels and costs.
- Deliver usage and performance data in business terms.
- Track user subscriptions and service requests.

- Provide a fast, consistent, and more effective access to IT services.
- Publish or review service reports.

Developing a service catalog can provide the following improvements to drive down costs while still achieving high levels of service:

- Improved efficiencies in handling incoming requests.
- Eliminate service redundancies.
- Increased IT staff productivity.
- Better allocation of resources.
- Reduced calls to the help desk.

Guidelines for Collecting Data

The following guidelines are for using staff interviews to collect data regarding the services and service levels currently existing in your organization. These guidelines are developed based on ITIL Methodology and CobiT™ Principles. These guidelines consist of the following activities for collecting and analyzing data, in sequential order:

- Review of the purpose of the staff interviews. (see page 3102)
- Use of the suggested questions (see page 3103) and any related questions of your own to conduct the staff interviews. (see page 3103)
- Analysis of service-related documents. (see page 3103)
- Review and benchmark activities (see page 3104) for existing services.
- Collation the results of staff interviews. (see page 3104)
- Organization of the newly determined information into service specifications that include detailed descriptions of each service.

Purpose of the Staff Interviews

The purpose of the interviewing the staff is to obtain and understand organization-wide policies and procedures relating to provider-to-user relationships. Examples follow:

- IT policies and procedures:
  - Service level agreements
  - Operational reporting content, timing, and distribution
  - Performance tracking methods
  - Corrective action activities

- IT documentation:
  - Service level performance reports
  - Service budget and costing procedures
  - Charge-back algorithms and methodology for calculating charges
  - Service improvement programs
  - Recourse resulting from nonperformance
  - Service level agreements with internal and external users and providers of services

Questions for Staff Interviews

The staff interviews can include the following questions:

- Who delivers which services where, to which organization or organizational groups, and at what cost?
- Who requests which services from which IT group and at what volume?
- What level of service is in place within the organization?
- Who are the stakeholders?
- How can we use the template catalog?

Staff Interviews

The staff whom you Interview include the following personnel:

- Chief Information Officer
- IT senior management
- IT Contract Administrator
- Service Level Administrator
- IT Operations management
- User management

Documents to Analyze

You review and analyze the following documents:

- Service level agreement process
- Definitions of responsibilities of users and providers

- Management reports on the achievement of the specified service performance criteria and all problems encountered

The purpose of analyzing the documents is to verify whether:

- Users understand service level agreement processes and procedures.
- The level of user satisfaction with the service level process and service level agreements is sufficient.
- Service fulfillment data is available to track performance.
- A performance improvement program exists.
- The accuracy of actual charges matches agreement content.
- A comparison of historical performance and prior service improvement commitments is tracked.
- Managers appropriately use reports on service performance.

Review and Benchmark Activities

The review and benchmark activities are as follows:

- Benchmarking of service level agreements against similar organizations or appropriate international standards and recognized industry best practices.
- Review of service level agreements to determine qualitative and quantitative provisions confirming obligations are defined and being met.
- Review of selected service level agreements to confirm compliance and resolution procedures for problems, specifically nonperformance.

Results of Staff Interviews

The results of the staff interviews help the organization identify the:

- Adequacy of the provisions describing, coordinating, and communicating the relationship between the providers and the users of information services.
- Incorrect calculations for selected categories of information.
- Ongoing review and corrective action by management of service level reporting.
- Adequacy of proposed service improvements in comparison with cost-benefit analysis.
- Adequacy of the ability of providers to meet commitments for improvements.

Best Practices Foundation

This article contains the following topics:

- Service Catalog Logical Structure (see page 3106)
- Customer-Focused Documentation (see page 3107)

Request and Fulfillment Automation with CA Process Automation

A key characteristic of the predefined foundation content is the automation of approvals and notifications for actions that complete the service fulfillment process. This automation makes the services "actionable." Service designers accomplish this goal through the workflow capabilities included with CA Process Automation.

All services in the predefined foundation content invoke the workflow-driven approval process. This process sends an email to the manager of the requestor, indicating the requiring approval for the request. The email includes a link to the approval page in CA Service Catalog to streamline the approval process. You can use a different approval process for individual services. To do so, select a different approval mechanism for those services through the Service Builder.

After a service request has been approved, the requested items in the service option group then follow a fulfillment workflow. The category that is specified for the requested component determines the workflow. The predefined service option groups contain components that belong to one of these categories: Hardware, Software, or Service.

The event rules for each category control the notifications that are generated as the components of the request move through the stages of fulfillment. The foundation content, as delivered, follows the predefined rules for each category. You can customize these rules to address your specific requirements.

The predefined foundation content provides a category-class-subclass structure (see page 3105) for your use.

Category-Class-Subclass Structure

The predefined foundation content provides a category-class-subclass structure. You can use the class and subclass designations within each category to customize the workflow process. The default structure contains the following top-level categories:

- None
- Hardware
- Reservation Manager
- Service
- Service Offering Management
- Software
- Other

Multiple classes exist within each category, and in most cases multiple subclasses within each class.

To view and optionally update the complete detailed structure of category classes and subclasses, edit the category.xml file.

Note: You can add categories to meet your specific requirements. However, you cannot change the internal numeric values of the default categories. This field is used for logic in other portions of the product.

Service Catalog Logical Structure

You can use a table or spreadsheet to design the full logical structure of the catalog before its actual implementation. This approach facilitates communication between stakeholders and end users regarding the service catalog structure and content required.

We recommend that you agree on the general service catalog content and structure first and the details next. As the catalog and its use mature within an organization, some restructuring and fine-tuning are likely to occur.

IT Support Services						
Folder	**Service**	**Service Option**	**Category**	**Class**	**Subclass**	**Description**
Data Security						
	Virus Protection / Remediation Plan SLA					
		Bronze	Service	IT	SLA	Bronze SLA for Virus Protection /Remediation
		Silver	Service	IT	SLA	Silver SLA for Virus Protection /Remediation
		Gold	Service	IT	SLA	Gold SLA for Virus Protection /Remediation
	VPN Access					
		Request VPN Access	Service	IT	Security	Request VPN access for remote user
	Proxy Access					
		Subscribe to Proxy	Service	IT	Security	Request proxy access (security request)
	Pre-Production Security Scans					
		Security Scan	Service	IT	Security	Request Security Scan before production status
Data Management						
	Backup Data					
				IT	Data	

	Backup Production Server Data	Service	Backup Services for Production Server Data.
	Backup Local PC / Laptop Data	Service	IT Data Backup Services for Local PC / Laptop Data.
Restore Data			Services to restore production or local data.
	Restore Production Server Data	Service	IT Data Restore data on a production server from backup files.
	Restore Local PC / Laptop Data	Service	IT Data Restore data on a local PC from backup files.

We recommend limiting the number of levels that users navigate to reach specific services in your catalog. As an example, consider an IT Support Services category such as Hardware and Software Procurement. For ease of use, divide it into two separate categories. Examples include Hardware Procurement and Software Procurement. This approach is more efficient than using subfolders, for example, under Hardware and Software Procurement.

You can customize the structure of the provided content to meet the needs of your organization. For example, you can divide a single-Server service into the following services: Blade Server, Standard Server, and Mainframe Server. In this case, create a folder that is named Server to contain the other thee services. Each service contains descriptions and service option group items to assist users in their selection.

Customer-Focused Documentation

Prepare customer-focused documentation for the service catalog and make it available to all potential users. Sample contents follow:

- Forward from the IT Director
- Table of Contents
- IT Service Provider profile
- Version number, date created, date amended
- Changes from last published Catalog
- Service times and accessibility of the IT Service Provider
- Overview of Services and Products
- Customer-focused Service and Product descriptions
- Specifications of Services
- Deliverables
- Service Times

- Maintenance Times
- Support Times
- Delivery Times
- Quality Target (availability, reliability, usability, priority)
- Requirements
- Request and Change procedures
- Contingency policy
- Pricing and Charging
- Index and definitions

Service Accounting

Service Accounting lets you manage your invoicing and financial reports, accounts, subscriptions, exchange rates, budgets and plans, and so on. You can search and view all invoices for an account for a certain period. It offers you a consolidated view of all invoices for a selected group. Financial reports provide insight and visibility about account details, adjustment details, invoice details, and payment details. An Administrator can manage invoices for an account using the available options. Accounting configuration enables you to prorate the online as well as batch processes. You can generate an invoice for charges as per the usage rate. Administrators can schedule the on-demand invoice to produce instant current invoice for an account.

This section contains the following articles:

Manage Invoicing and Financial Reporting

This article contains the following topics:

Invoice History

The Invoice history feature enables you to search for and view all invoices for a certain period for any account. Ensure that you have access to the accounts for which you want to view the invoices. Invoice History Records offer a consolidated view of all invoices for a given group. Information that is displayed includes the Invoice group and the status (successful or unsuccessful). Invoices can be viewed in HTML, CSV, or XML format, and provides the facility to email these invoices.

Invoicing and Financial Reporting

Once services are tied to accounts through a subscription, you can schedule these accounts for batch invoicing. You can process any rates, adjustments (general or SLA violation), and payments posted for the current billing period. An invoice group with global settings can be established to bill an associated list of accounts together in one instance at a scheduled future date. This list can be assembled at the time the group is created or determined dynamically during invoice execution. At the scheduled time, the invoice engine kicks off. The group is then placed into a queue for the accounting service to pick up for processing. Once selected, the engine queries the accounts that are associated with the invoice group. The engine then proceeds to generate an invoice for each of accounts.

The invoice states and justifies charges to users and business owners. These charges can be rolled up by a Business Unit organization. The stakeholders, at each level, can be given access to their IT cost information. Once processed, organizations can provide each Business Unit Web access to real time and historical chargeback invoice information. Business Units can also see detailed IT usage reports. IT owners can view actual spending versus budget and can determine the actual cost by business function. Providing such visibility into IT costs enables providing an organization with the necessary data for setting budgets and business planning.

Financial Reports

Several reports are available to help provide insight and visibility into IT. These reports include:

- Accounting Details - shows the accounting profile details for all accounts given the filter specification.

- Adjustment Details - displays details pertaining to any defined adjustments.
- Invoice Details - shows information that is related to invoicing such as dates, balance, and number of violations.
- Payment Details - provides a listing of payments posted against account balances.

Invoice Criteria for Accounts

For the invoice engine to process the account, the account must be:

- Included in the Account List associated to an active invoice group.
- Have the Billing Date field (in the Accounting profile) specified earlier than the date of the bill run.
- Have the status field (in the Accounting profile) specified.
- Have the Automatic Invoicing field (in the Accounting profile) set to Yes.
- Subscribed to a service under a valid state if the configuration is set for *Allow No Activity Invoices*.

Invoice Criteria for Subscriptions

A subscription must meet the following criteria before showing on an invoice:

- Chargeable items such as one time, daily, weekly, monthly, and installment appear when those periods for those charges are recognized.
- An element in the service option groups of a service is not specified to be Excluded From Invoice.
- Usage and transaction based charges appear when there have been metrics that are collected to represent use or transactions.
- Agreement and contract charges as defined through CA Business Service Insight appear on an invoice. The subscription is being charged as a one time, periodic or installment charge.

Invoice Groups

Administrators can create invoice groups. An Invoice Group provides the capability for grouping and scheduling accounts for future invoicing. When the invoicing process initiates, each group enters a queue to provide the accounting service the facility to retrieve and process the list of accounts in the group. This account list can be assembled and maintained manually or dynamically depending on the group type. The invoice groups generate invoices on a schedule or on demand and facilitate financial reporting.

Add a Static Invoice Group

Static Invoice Groups contain an account list that is comprised of accounts that have been manually assigned to it. Accounts assigned to a static invoice group cannot be assigned to any other group. Any accounts that are assigned to an invoice group remain unless explicitly removed or deleted from the system. You can further expand the account list for active groups by directly selecting and adding accounts to it.

Follow these steps:

1. Click Accounting, Invoices, Groups.

2. Click the Add button.

3. Complete the Invoice Group information:

   Note: Do not select Dynamic for this procedure because groups are static by default.

4. Complete the Accounting Profile information

   - Billing Cycle
     Determines the cycle when an account is invoiced.

   - Billing Cycle Interval
     Indicates the number of billing cycles that must elapse before an account is invoiced. This parameter is used with Billing Cycle.
     For example, to specify a quarterly billed account, select a monthly billing cycle, and specify 3 as the billing cycle interval.

   - Period Start Date
     Indicates when the accounting profile billing period begins. Choices include:

     - The date when department was created.

     - The date when the account was opened.

     - The current date that the accounting profile is created.

   - Period End Date
     Indicates when the accounting profile billing period ends.

   - Days Due Default
     Calculates the number of days past the date of the invoice that payment is due.

   Review the information on the Group Confirmation window. Click Next to confirm the information.

5. Click Add Accounts and use the shuttle box to move any accounts you wish to include in the account list. Verify that all selected accounts appear in the Accounts to Save column, and click OK.

6. Click Next and apply the appropriate Scheduler settings giving the billing date and the time zone.

7. Set the status to Active and click Finish.
   The Invoice Groups window appears, reflecting your newly created group.

Add a Dynamic Invoice Group

With Dynamic Invoice Groups, account lists are generated dynamically given a specified criteria that is stored as a Data Object. As new accounts are added and fall within that criteria, they are included in the account lists in that group. In essence, Invoice Groups can now be set to maintain and manage their own account lists.

Follow these steps:

1. Click Accounting, Invoices, Groups.
2. Click the Add button.
3. Complete the Invoice Group information and select Dynamic.
4. Review the Accounting Profile information and change the fields as necessary.
5. Review the information on the Group Confirmation window.
6. The Account List window appears empty since there are no associated criteria to assemble this list. Click Define Criteria and use the Account Criteria Builder to create a query to generate a list.
7. Click the Create Criteria button.
   - Save Last Executed Search
     Saves the last search that the Account Criteria search account mechanism executes.
   - Advanced Custom Search
     Enables the user to specify directly the where clause in SQL.
8. Once a criteria type is selected, two more fields are present:
   - Name
     Specifies the name to be associated to this query. (This value is stored as a Report Data Object.)
   - Comments
     Provides a field for more information.
9. Click Save when complete.
10. Click Next.
11. Apply the appropriate Scheduler settings giving the billing date and the time zone.
12. Set the status to Active.
13. Click Finish.
    The Dynamic Invoice Group has been created and is reflected in the Invoice Groups window. Click View Accounting Tasks to view the scheduled task.

Specify the Output Location

The default locations where invoices are saved to the hard drive are as follows:

- Accounts that receive invoices through email have a copy of their invoices that are stored in %ACC_HOME%\outbox\email.
- Accounts that receive invoices through regular postal mail have a copy of their invoices that are stored in %ACC_HOME%\outbox\postal.
- Accounts that receive invoices through fax have a copy of their invoices that are stored in %ACC_HOME%\outbox\fax.
- Accounts that the administrator wants to print internally have a copy of account invoices that are stored in %ACC_HOME%\outbox\printer.

Note: Specify \\ as a folder separator on Windows.

Instead of emailing a business unit an invoice directly, you can also to print or fax it. You can store the files in a directory on your hard drive. To do so, set the **Invoice Method** in the accounting profiles of all your customer accounts to *Postal* by default.

Manage Invoices

An administrator has several options to manage invoices that have already been generated for an account.

Follow these steps:

1. Click Accounting, Account Management.
2. Search for and select an account.
3. Click the Invoices tab.
4. Manage invoices, as follows:
   - View the invoice history
   - Edit an invoice (see page)
   - Perform an invoice on-demand (see page 3114)
   - View an invoice online (see page 3114)
   - Rollback an invoice (see page)

An invoice can be edited and line items can be added, modified, or removed. These line items include text, charges, adjustments, and payments.

Proration

Prorating is the process of dividing the cost of a subscription over the billing cycle period of an account. For example, Suppose that a monthly charge is $3000.00, and an account is on a Monthly billing cycle. An invoice is generated one day into the billing cycle with 30 days that are left in that month. The charge on the invoice is $100.00 and a description that specifies that the charge is for one day.

The accounting configuration enables you to specify that both online and batch process invoices are prorated:

- Only online invoices are prorated.
- Only invoices that are generated during the batch process are prorated.
- Or neither are prorated.

By default, both online invoices and batch invoices are configured to prorate charges.

Generate Invoice

An invoice can be generated to show the charges that are computed against the usage. If User Usage-Based billing was employed, the charges come from all users who are associated to the invoiced account.

Invoice On-Demand

On-demand invoicing enables an administrator to bypass the scheduled invoicing and instantaneously produce the current standing invoice for an account.

Performing an invoice on-demand produces the same results as if it had been processed as a scheduled bill run. A new invoice is generated for the current billing period and the accounting profile is updated.

Invoice Online

Online invoicing enables you to view your charges in real time with a web browser. An online invoice displays charges that an account has incurred since its last billing period, up to and including the current date. All the charges are computed in real time. Because these values can change, the invoice does not get persisted until the end of the billing cycle when the invoicing process runs.

Similar to on-demand invoicing, online invoices do not have to go through the same account query and verification: an invoice is requested to be viewed for that account regardless of the account status, billing cycle, or automatic invoicing. The criteria still apply for choosing or selecting which subscriptions show up on the invoice as charges, as with the invoice process.

You can enable or disable prorating charges when viewing your invoice online. Set the **Pro Rate Online** to Yes in the **Invoice Engine Configuration** of Accounting Configuration.

View Invoice Status

As the Invoice Engine processes the invoices, it logs alerts to the CA Service Catalog database. These alerts can be viewed by clicking Messages from the main menu.

Your Alert messages are listed in a table displaying the following parameters:

- Date/Time
- Type
- Source
- Computer
- Message

If a failure occurs during any one of the phases, the Invoice Engine logs a critical severity alert. The Invoice Engine then displays a message.

Rollback Invoice and Rollback Invoices Utility

Rollback invoicing enables you to invoice accounts from a previously billed period. This sequential rollback of invoices can reprocess an invoice to reflect any changes that are made to charges. To roll back to a previous invoice period, select the invoices to roll back from the Invoice History window of the account. Click Rollback. The period date, bill date, and account balance for the accounting profile is updated up to the period, invoices were rolled back. These Invoices and their associated transactions are permanently deleted from the system once the rollback is complete. Invoice On-demand can be used to regenerate any or all the invoices whenever necessary.

Note: The rollback works *only* for invoices that a successful invoice bill creates.

The syntax for using the rollback.bat (Windows) command follows.

rollback -g *groupname* -b *businessunitid*

- **-g *groupname***
  Specifies the name of the invoice group that defines the accounts whose most recent invoices you want to roll back. This parameter is required.

- **-b *businessunitid***

  Specifies the business unit ID of the accounts--in the named invoice group--whose most recent invoices are being rolled back. For Windows, the rollback.bat file is located in the USM_HOME\accounting\scripts folder.

Examples

The following command rolls back the most recent invoices for all accounts in the InternationalAccounts invoice group, in *all* business units:

```
rollback -g InternationalAccounts
```

The following command rolls back the most recent invoices for only the accounts in the InternationalAccounts invoice group that belong to the ForwardInc business unit:

```
rollback -g InternationalAccounts -b ForwardInc
```

Batch Printing

Service Accounting Component offers a Batch Printing option. You can create print jobs and print invoices individually or as a whole. A print job is a collection of invoices that have been grouped according to the specified credentials. After it has been created, the collection remains unchanged and its invoices can be printed as a whole or individually.

Follow these steps:

1. Click Accounting, Invoices, Batch Printing.
2. Click Add Print Job.
3. Enter the Name and Description.
4. Select the appropriate Invoice Group.
   An Invoice group is a set of accounts that you can run together in one instance. With the Batch Printing feature, invoice groups serve as an invoice filter. Only those invoices that are associated with the accounts in the selected invoice groups are included in this print job.
5. Select Services. Select all Services (the default) or further refine your number of invoices by filtering by Service name.
6. Select Billing Cycles.
   By including specific types of billing cycles, the number of invoices in the collection is once again decreased. This billing cycle is for the account, not at the Invoice Group.
7. Click Add.
   Once a print job has been added, the Batch Printing user interface can be used to manage them. Clicking a print job changes its details on the right. You can delete the selected print job or can reuse it.

Note: You can return the invoices in reverse order or filter the invoices by selecting a specific Item Status.

By default, 50 invoices are returned for each page. To adjust this number, specify the desired amount and click Refresh. Clicking an invoice launches it into a new window serving as a print preview tool. This tool can also check all invoices by item status. By clicking the Reverse Order check box, the checked invoices on the current page is printed in ascending order.

After each print item is completed, the status for each item is updated. The print job status appears at the top.

Manage Accounts

This article contains the following topics:

Administrators manage the accounts for a business unit. An *account* represents a corporate unit, a regional office, an individual user, or a logical group of them. CA Service Catalog applies charges to accounts.

If a user requests a service from the catalog, the product automatically creates an account for the user. The product also subscribes the account to the requested service.

Note: In Accounting Component, two digits appear after the decimal point for all supported currency units, including the Japanese yen. If your organization uses the yen, decide how to process the two digits after the decimal point because Yen is processed in whole numbers only. For example, you can decide to ignore the two digits after the decimal point or round them up or down to the nearest whole number.

Add or Edit Accounts

You can add an account so that you can bill it for services that it has requested or subscribed to. Typically, administrators edit accounts periodically as part of standard business unit operations.

Follow these steps:

1. Select Administration, Business Units from the main menu.
2. Expand the business unit tree and find the business unit that you want.
3. Click:
   - Add Account.
   - Account name of interest and edit it.
4. Complete or update the fields.

When you add an account, the Add a New Account page appears. You complete the fields on this page to configure the new account to meet the needs of your organization.

- **Opened Date**
  Specifies the date when the account becomes part of your organizational structure, in local time.

- **Status**
  Specifies whether the account is open or it is closed.

- **Primary Contact Information**
  Specifies the user ID of the primary contact for the account.

- **Location Information**
  Specifies information about the location of the account.

  Note: All CA products using the same MDB share location data. Therefore, be careful when you edit location information.

- **Account Settings**
  Specifies the list of users who are associated with this account. Usage-based billing references these users.

  Note: When a user creates a request for the first time, the Catalog system creates a request-related account for the user.

Close and Delete Accounts

Closing an account is typically a required task as you create and maintain accounts in your business unit over time. If the status of an account is Closed, you cannot:

- Enter a subscription for the account.
- Generate the invoices.
- Edit the Accounting Profile.

If you close an account, the associated accounting profile handles any residual accounting functions before the status is Closed. The status field moves from “Close Requested” to “Closed” once the outstanding charges and credits are processed for that period.

Follow these steps:

1. Review the effects of closing or deleting an account and verify that you want to proceed.
2. Run the final invoicing (see page 3109) for the account, if necessary.
3. Select Administration, Business Units, and expand the tree to display the business unit that contains the account that you want.
4. Click the account name.

5. Edit the account profile and change the status to Closed.

6. Delete the account. You can optionally close an account without deleting it.

Effects of Deleting or Closing an Account

Deleting or closing an account affects the subscriptions and requests for the account, as follows:

- **Subscriptions**
  The status of subscriptions for the account change to the default cancellation status (Pending Cancellation or Cancel).

- **Requests**
  The status of requested service options for the account change that is based on their original status as follows:

Original Status	New Status
Not Submitted	None. Request is deleted.
Submitted. An approval status, a fulfillment status, Pending Resource Assignment, or Resource Assigned	Cancelled
Completed	Default cancellation status (Pending Cancellation or Cancel) if Service Accounting Component is installed. Cancelled if Service Accounting Component is not installed.
Pending Cancellation or Cancelled	Same as Original Status.

Aggregation of Accounts

A business unit can designate an account to aggregate the charges and account balances for all other accounts within its scope. To do so, configure the accounting profiles for a set of accounts appropriately. Set the Aggregate option in the Accounting Profile to Aggregating Account to select the accounts for this consolidation. The aggregating account includes all accounts in the business unit hierarchy. Even sibling accounts whose Aggregate option is set to Yes are included in the aggregating account.

When the aggregating account is used to maintain the account balances of all accounts included in its aggregation, the aggregated accounts are typically zero balancing accounts. Set the Account Type option to Zero Balance in its Accounting Profile.

Post a Payment to an Account

Payments can be posted for an account to settle any outstanding balances.

Follow these steps:

1. Click Accounting, Account Management.

2. Click the Make Payment icon for the account for which you are posting the payment.

3. The Payments List and Payment Details page appears. From this window, you can perform the following actions:
   - Add payments to the Payments List by completing the payment details and clicking the Add to List button.
   - Modify Payments in the Payments List by selecting the payment, making your modifications and clicking the Update Payment button.
   - Delete Payments in the Payments List by selecting the payment and clicking the Delete Payment button.
4. The Business Unit, Account Name, and Account Balance are populated in the Payment Details window.
5. Complete the mandatory Payment Details and any optional fields.
6. Click Submit Payment.
   The payment is processed.

Manage Subscriptions

This article contains the following topics:

A *subscription* is a Service Accounting Component to identify the assignment of a service by an administrator to an account. Once the service is activated for the account and the subscription is active, the charges are calculated for each invoice period. If a subscription is cancelled, the service is deactivated as soon as all outstanding charges are processed. In addition, subscriptions can be suspended for any amount of time, during which no charges are incurred.

Subscription Types

Subscriptions are possible *only* when Service Accounting Component is installed.

Accounts can have *physical* subscriptions, *data mediation logical* subscriptions, or both types of subscriptions.

- A physical subscription includes one or more service options in a service. A physical subscription results from one of the following conditions:
  - When a service that a user explicitly requests is completed or a request that is only submitted but not completed. When a service is completed, it results in *request-based* subscription.

- The business unit administrator assigns subscriptions to accounts, which are based on certain criteria, such as business needs. Such subscriptions are *account-based* subscriptions.

- A data mediation logical subscription is virtual; it includes no physical subscription records. Rather, it is a logical mapping and an aggregation mapping. This type results from an administrator using the Data Mediation component to aggregate usage data. In the Invoice component, the usage cost for this subscription is shown when data is aggregated. Considering data mediation logical subscriptions is important when you implement usage-based billing.

A single account can have one or more subscriptions of either type or both types. If an account has both a physical subscription and a data mediation subscription, the physical subscription *always* overrides the data mediation subscription.

On the Existing Subscriptions window, each applicable subscription type appears in the Currently Subscribed column. However, data mediation logical subscriptions appear *only* if no physical subscription exists.

Subscription types are cancelled when:

- A physical subscription (S) is canceled when you cancel the subscription for an account.
- A request subscription (R) is canceled when you cancel the request for an account.
- A Data Mediation logical subscription (D) is not shown when an administrator unloads or aggregates usage data again.

Administrators manage subscriptions by selecting Accounting, Account Management, clicking an account name, and clicking the Subscriptions tab. The subscription process is primarily an administrator task. But end users are given read access to active subscriptions for their accounts.

The Administration, Configuration, Subscription Configuration menu option enables Administrators to change the way future subscriptions of an account are handled.

Create a Physical Subscription

You can create a physical subscription.

Follow these steps:

1. Select Accounting, Account Management.
2. Click the account name for which you want to add a subscription.
3. Click the Subscriptions tab.
4. Select the service to which you want to subscribe.
5. Click the Subscribe link.
6. Click Yes.
   The physical subscription is added.

Enable Notes in Physical Subscriptions

To add notes to a physical subscription, you first enable the related notes feature.

Follow these steps:

1. Click Accounting, Configuration.
2. Click Subscription Configuration.
3. Click the Edit icon.
4. Check "Enable Subscription Notes."
5. Click Update Configuration.

The feature has been enabled and you can add notes to a physical subscription.

Add Notes to a Physical Subscription

After you have enabled notes in physical subscriptions, you can add notes to physical subscriptions.

Follow these steps:

1. Click Accounting, Account Management.
2. Click the account name for which you want to add notes.
3. Click the Subscriptions tab.
4. Click the Existing Subscriptions button.
5. Locate and expand the subscription for which you want to add notes.
6. Click the Notes link for the item of interest.
7. Click Save Notes.

The notes are added to the selected physical subscription for the selected account.

Suspend a Physical Subscription

You can *suspend* a physical subscription (see page 3120) only for rate items that have a periodic billing cycle. You can cancel a physical subscription (see page 3123) for all other rate items.

Follow these steps:

1. Click Accounting, Account Management.
2. Click the account name for which you want to suspend the subscription.
3. Click the Subscriptions tab.

4. Click the Existing Subscriptions button.
5. Locate and expand the subscription that you want to suspend.
6. Click Suspensions.
7. Enter the start and end dates for the suspension or select "Indefinite Suspension."
8. Click Add New.
9. Click Close.

The physical subscription is suspended for the selected account for the period indicated.

Cancel a Physical Subscription

You can *cancel* a physical subscription (see page 3120) for all rate items except ones that have a periodic billing cycle. For such rate items, you can suspend a physical subscription (see page 3122).

Follow these steps:

1. Click Accounting, Account Management.
2. Click the account name for which you want to cancel a subscription.
3. Click the Subscriptions tab.
4. Click Existing Subscriptions.
5. Remove the subscription for the service.
6. Click Save.
   A message appears asking you to confirm the subscription changes.
7. Confirm or cancel the changes.
8. Verify that the physical subscriptions were successfully updated.

You can set subscription options that apply to services, service option groups, and service option elements. By default, these settings apply to all accounts. In addition, however, you can specify custom settings for one or more selected accounts.

Follow these steps:

1. Click Accounting, Configuration.
   The Accounting Configuration page appears. On the left, in the Menu under the main menu, Options is selected by default. On the right, links appear for each category (subset) of the accounting configuration options.
2. Review the name of the current business unit. To manage subscription options for a different business unit, change the business unit.

3. Click Subscription Management in the Menu on the left under the main menu.
   The Subscription Decision Tree appears on the right, replacing the links for the accounting configuration categories.

4. Decide whether to update subscription options for all accounts in the business unit or only one more selected account. In either case, decide whether to update subscription options for a specific service, service option group, or service option element.
   To help you decide, review the following order of precedence:

   - A setting for a service option element overrides the setting for the service option group to which it belongs.
   - A setting for a service option group overrides the setting for the service to which it belongs.
   - A setting for a specific account overrides the corresponding setting under "All Accounts."

5. Perform *one* of the following actions:

   - Click All Accounts to apply your updates to every account in the business unit.
     The Services and Service Option Groups nodes appear, under all accounts.
   - Click Apply to Individual Account to apply the updates to only one or more selected accounts in the business unit.
     The Select Accounts dialog appears. Select the account or accounts you want and click OK.
     The Services and Service Option Groups nodes appear, under the selected accounts.

6. Click the Service or Services node (whichever you want to update), under either All Accounts or a selected account.

7. Drill down the Services and Service Option Group node to reach the subscription management options (see page 3125) of interest. You can update the options for services, service option groups, and service option elements.

   Note: Optionally specify *no* value for Bill In Advance field or the Effective Dates And Bill Dates field when you create an account. In that case, the system applies default settings. So, the account does *not* appear in the Subscription Decision tree. For information about creating accounts, see the Manage Accounts (see page 3117) section.

8. Update these options as needed and save your changes.

You have managed subscriptions. These settings apply to any sub business units of the business unit that you are updating. If a business unit has sub business units, it has its own configuration settings.

Subscription Management Options

To manage subscriptions (see page 3120), you specify the subscription management options, using the Subscription Decision Tree. Specify separate settings that apply to all either *all* accounts in the business unit or to selected accounts *only*. In both cases, use the tree to set the following options for individual services, service option groups, or service option elements:

- **Effective Dates and Bill Dates**
  Specifies when billing begins after an account subscribes to a service option element. Select *one* of the following options:
  - **Bill Date begins on the Effective Date**
    Begins billing the account on the date the subscription is made.
  - **Specify a Bill Date separate from the Effective Date**
    Begins billing the account on a specific date, regardless of the subscription date.
  - **Specify a Bill Date relative to the Effective Date**
    Begins billing the account that is based on the *complex* option you specify, relative to the subscription date. An example is “the first day of the month of the subscription.”
  - **Specify a Bill Date offset from the Effective Date**
    Begins billing the account that is based on the "before and after" option you specify, relative to the subscription date. An example is “two months after the subscription date.”
- **Bill in Advance**
  Specifies whether a subscribing account is charged in advance of a service being rendered. Select *one* of the following options:
  - **Do not bill in advance**
    Bills the account when the service is rendered.
  - **Specify how far in advance the charge should be billed**
    Bills the account the specified number of periods in advance.

  The billing period is the billing period of the service option element being subscribe*d to*. For example, suppose that a service option element specifies a Unit Cost of $10 with a Billing Cycle of Periodic, a Periodic Type of Monthly, and a Periodic Type Interval of 1. If this setting is 3, then a subscribing account is billed $30 on the first invoice and each interval invoice, rather than $10 per month.

Manage Exchange Rates

Service Accounting Component supplies the Accounting, Configuration, Exchange Rates table. By default, this table displays exchange rates for the current time period. You can also view any previously defined exchange rates for earlier or future periods.

Using this table, you manage exchange rates for the currencies that are used in your implementation. The exchange rates are relative to the US dollar. The Catalog system uses these exchange rates to produce invoices for each account. The invoices are produced in the currency of the business unit to which the account belongs.

All exchange rates are relative to the US dollar. When you convert from one currency type to another, the system first converts the catalog amount to US dollars. Next, the system converts the amount to the currency type of the account.

By default, the exchange rates for all currency types are set to 1.0. This setting means that the exchange rate for each currency type relative to the US dollar is 1.0.

Updates to exchange rates apply to the *entire* system. You *cannot* specify different exchange rates for different business units.

You can update exchange rates in Service Accounting Component when the official exchange rates change. Updates to exchange rates apply to the *entire* system. You *cannot* specify different exchange rates for different business units.

Follow these steps:

1. Click Accounting, Configuration.

2. Click Exchange Rates in the Menu on the left under the main menu.
   The Exchange Rates table for the current date range appears on the right. The table lists the currency name, symbol, date, exchange rate, and so forth. By default, The table for the current time period (the previous month) appears.

3. View the exchange rates for the currency that is defined in your system.

4. (Optional) Edit exchange rates for the current time period to provide a regularly scheduled update.

5. (Optional) Delete an exchange rate for a date range.

   Important! Deleting *all* exchange rate entries for a currency name deletes that currency name from the Exchange Rates table completely! You *cannot* use the GUI to restore a deleted currency name. Therefore, use caution when deleting exchange rates from the table.

6. (Optional) Delete a currency name from the exchange rate table if your implementation does not need the currency.

   Note: Delete currency names with caution, because you *cannot* use the GUI to add a missing or deleted currency name.

7. (Optional) Add an exchange rate for a date range to provide a periodic update or to prepare for the start of the next billing period.

> **Note:** You *cannot* add a new exchange rate that overlaps the same date range as any existing exchange rate.

Manage Budgets and Plans

This article contains the following topics:

Implementing a successful budgeting process is a primary key to achieve organizational business objectives. Budgets help IT managers evaluate the performance of a business unit though comparison analysis of actual expenditures against budgeted amounts. These findings can aid in justifying IT costs or identifying why expectations have not been met. In addition, this information can be used to establish new goals and discovering the means to reach them through planning.

Through the Budget and Planning module, a financial manager can set up period budgets for business units and their services. At the end of each fiscal period, a variance report evaluates the differences between actual and budgeted costs. This information can be then used to help identify the root cause for areas of inefficiency.

Manage Fiscal Periods

Fiscal Periods can be user-defined for any time period to represent an accounting period. Service Accounting Component allows for the definition of monthly, quarterly, or yearly fiscal periods. Once defined, these periods are used in Budget and Planning worksheets when defining budgets or setting costs for services. These periods are also used for data mediation when selecting a period for aggregation.

By default, you create monthly fiscal periods for the current year, which is based on your installation date. You also use fiscal periods to view Data Mediation aggregations and to manage budgeting and planning.

You cannot create different fiscal periods for different business units. *Only one* set of fiscal periods applies to all business units.

Use Worksheets

Worksheets are used to capture budget and cost totals for services. A Service Worksheet can be used to set budgets, unit cost, or total cost for services across fiscal periods. Costs can also be pooled. Then, use the Service Worksheet to set service costs by tracing pooled activities to the services that consume them. A Pool Worksheet is used to establish these pooled costs. A cost pool is comprised of contributing cost elements whose sum makes up the total cost of the pooled activity. A percentage of this total can then be allocated among the services in the Service Worksheet.

Follow these steps:

1. Click Accounting, Budget and Planning, Worksheets.
2. Click Change Business Unit and select a different business unit, if necessary.
3. Complete the Worksheet Options:
4. Click View Worksheet.

The services that are presented in the worksheet contain any chargeable service option group elements whose Budget option is selected. For the elements that employ a Cost Type of either *Allocated Cost* or *Standard Cost*, the values that are entered in the worksheet determine the cost of the service element.

For the *Allocated Cost* setting, the value represents the total cost of the service element to be allocated back to Business Unit accounts. The associated Allocation Method specification determines the distribution of that cost. For example, suppose that the method is set to Distribute by Subscription. Then, the total cost of the chargeable element is divided by the number of subscriptions to it.

The *Standard Cost* option, is used to define a predetermined unit cost for the service option group element. This cost can be used to assign a rate to a service that can vary from period to period, or as the expected costs defined in a budget. For example, suppose that you have to pre-define a set of unit costs for a particular period and then change. Worksheets are tools that enable these service rates to change over time. Worksheets allow the definition of budgets for service during specified fiscal periods. The values that are defined in this instance are not used in the cost calculation of a service option group element. But these values are used instead in reporting variance between budgeted and actual amounts.

Create a Set

Sets enable you to define related financial and quantitative values. For example, you can use sets to represent various types of budgets, especially when you are initially creating these budgets. You can also link costs to services. Sets can be defined to represent a unit cost or total cost of a service. These types of sets are typically associated with a service during service definition when you employ a Cost Type of *Allocated Cost* or *Standard Cost.*

Follow these steps:

1. Click Accounting, Budget and Planning and click Sets.
2. Click the Add Set button.

3. Complete the following information:

   - **Name**
     Specifies the set name.

   - **Description**
     Indicates the optional text area for a description.

   - **Status**
     Specifies whether the associated worksheet values can be modified. Choices include Locked or Unlocked. Once a set is locked, values are read-only in the worksheets until the Status is changed to Unlocked.

   - **Source**
     Provides for further classification of the associated values. Choices include:

     - Allocated Cost - used when defining the total cost of a chargeable service. Once this type of set is bound to a service, an associated Allocation Method can be selected to employ a means of distributing the cost.

     - Standard Cost - used when defining the total unit cost of a chargeable service. Once this type of set is bound to a service, a predetermined service cost can be set for each period.

     - Actual Units - used to attribute unit quantities to services.

4. Click Add New Set.

Create a Cost Element

A Cost Element is a resource that is used to subdivide costs corresponding to the consumption of a particular service. The amount is paid for a resource that an activity consumes and is included in a cost pool.

Follow these steps:

1. Click Accounting, Budget and Planning, Cost Elements.

2. Click the Add Cost Element button.

3. Complete the fields for this cost element.

4. Click the Update button.

You have created a cost element.

Create a Cost Pool

A Cost Pool is the grouping of all cost elements that are associated with an activity carried out by an entity. The cost pool can be used to identify the cost of any main activities in providing a service.

Follow these steps:

1. Click Accounting, Budget and Planning and click Cost Pools.
2. Click the Add Cost Pool Button.
3. Complete the fields on the dialog:
   - **Name**
     Specifies the cost pool name.
   - **Type**
     Specifies how Cost Pool totals apply to service costs.
4. Click Add New Pool button.

Assign Cost Elements to Cost Pools

Once the main cost pools have been defined, a total cost of each cost pool can be calculated. First, the activities that are related to each cost pool are identified and assigned to the appropriate cost pool. To trace the expenses to each cost pool, identify the cost drivers for each cost element.

Follow these steps:

1. Go to Accounting, Budget and Planning, Cost Elements.
2. Select the Cost Elements to assign to a cost pool.
3. Click the Assign to Cost Pools button.
4. Assign the pools with cost elements by selecting the corresponding check-box.
5. Click the Save Assignments button.

Assign Activity Based Costing to Services

Activity Based Costing (ABC) is a process of assigning costs to services and is used as a tool for planning. The method aims initially to identify and categorize the main operating activities within an organization. Once defined, the costs attributable to these activities are assigned to cost pools. The cost pools are then allocated back to services based on how the service consumes the activity. The steps that follow outline the ABC process:

- Typically, an organization can be broken down into a set of succinct activities that accomplish business processes. The cost pools are created to assemble all cost elements that are related to each of these activities.
- Once the activities have been identified, the principle causes of the costs for each activity are identified. These expenses are categorized by establishing cost elements.
- Add the cost elements. Then, ensure that the cost elements are related to their corresponding cost pools through cost pool assignment.
- The Pool Worksheet applies values to the cost pools based on the expense attributed to each associated cost element. Go to Accounting, Budget and Planning, Worksheets and use the Pool Worksheet option. Then apply these values.

- The Service Worksheet is used as activities are traced to services. The associated pooled costs are allocated to services based on their level of consumption of activities. The Service Worksheet is used to capture these amounts, which can be fixed or a percentage of the pool total.

- Only services that contain chargeable service option group elements are eligible to appear on the Service Worksheet. Check the Budget properly in the service option group element definition dialog when defining a service. In addition to having the worksheet values applied in invoicing calculations, a cost type of *Allocated Cost* or *Standard Cost* must be selected for the service element.

- Invoices are generated for accounts that are subscribed to these services. These invoices show an expandable breakdown of services by cost pools and cost elements.

Manage General Adjustments

Adjustments are credits or debits applied to services, individual charges of a service option group or service option element, and SLA violations. These adjustments are a fixed dollar amount or a percentage. Applying an adjustment to a business unit applies to all accounts within the selected business unit.

The General Adjustment properties appear on the Adjustment Information window.

- **Adjustment For**
  Specifies the account number of the account being adjusted.

- **Adjustment Type**
  Specifies whether the adjustment is a fixed amount or a percentage. More fields appear depending on the option you select in **Adjustment Type**.

Administrators can apply general adjustments either globally to all accounts or individually to a specific account. Applying general adjustments globally are required when a general adjustment applies to all accounts. For example, global credit to all accounts to cover an accidental overcharge of a specific fee in an earlier bill.

Follow these steps:

1. Select Accounting, Adjustments.
2. Select General from the side menu.
3. Click the Add General Adjustment button.
4. Complete the fields.
5. Click OK.

If only one account requires general adjustments, use the following procedure to apply the adjustments to the account.

Follow these steps:

1. Select Accounting, Account Management.
   Click the Add Adjustments icon (+/-) associated with the account.

2. Complete the fields.

3. Click OK.

Manage QoS SLA Violation Adjustments

Request Service Level Agreements (SLAs) are a feature of CA Service Catalog. Quality of Service (QoS) SLAs are available only if CA Service Catalog is integrated with CA Business Service Insight. The terms request SLA and QoS SLA are used to distinguish between the two types of SLAs.

Administrators can apply violation adjustments for QoS SLAs either globally to all accounts or individually to a specific account.

Note: To use SLA violation adjustments, CA Service Catalog must be integrated with CA Business Service Insight. For more information, see the Integrate CA Service Catalog with CA Business Service Insight (see page 3441) section.

You specify the QoS SLA Violation Adjustment properties on the Add SLA Violation Adjustment window.

- **Adjustment For**
  Specifies the account number of the account being adjusted.

- **Adjustment Type**
  Specifies whether the adjustment is a fixed amount or a lookup. A lookup refers to a tiered service option group based on the total violations of an SLA package, agreement, or agreement value.

- **Lookup Service Option Group**
  Specifies the tiered service option group to use with the lookup adjustment types. The selected item is used to help calculate the adjustment amount.

- **Per Violation**
  Specifies the fixed amount to adjust for each violation.
  This option applies *only* when the Adjustment Type is Fixed Amount.

- **Aggregate Violations on Invoice**
  Specifies that each violation appears as one line item on the invoice.
  This option applies *only* when the Adjustment Type is Fixed Amount.

- **Tier Type**
  Specifies the type of lookup into the tiered service option group, as follows:

- **Lookup**
  Selects the first matching tier.

- **Variable Lookup**
  Selects all tiers up to and including the matching tier.

Applying QoS SLA violation adjustments globally is required when an SLA violation affects all accounts. For example, a system-wide outage resulting in no services to all accounts for a period that exceeds the downtime that an SLA allows.

Follow these steps:

1. Select Accounting, Adjustments.
2. Select SLA Violation.
3. Click the Add SLA Violation Adjustment button.
4. Complete the fields as required.
5. Click OK.

If only one account requires QoS SLA violation adjustments, use the following procedure to apply the adjustments to the account.

Follow these steps:

1. Select Accounting, Adjustments.
2. Select SLA Violation.
3. Click the Add SLA Violation Adjustment button.
4. Complete the fields on this window as required.
5. Click OK.

Manage Data Mediation

This article contains the following topics:

- Repository Agent (see page 3138)
- Data Import Frequency (see page 3139)

Data Mediation lets you import usage event data from various external sources. Data Mediation uses the process of ETL (Extraction, Transform, and Load). You can use this process to transform operational data into event data to support billing, and reporting. After the data has been imported, other CA Service Catalog components can use this data. Data Mediation is useful when batch operational data from a source other than CA Service Catalog is available. Also, the requirements allow for historical rather than real-time data.

Data Mediation supports the following types of data feeds:

- Delimiter Separated File
- Fixed-Length File
- Database Import includes Database Table Import and Advanced Database Import.

When the external usage data is imported through Data Mediation as File Type data feeds, it is transformed into a flat file. The file is uploaded to the \datamediation subdirectory of the filestore location. By default, the filestore location is the USM_HOME\FileStore\ directory of the Catalog Component computer that you are using. To view the location of the imported flat files, select Administration, Configuration, File Store Information. Use the filestore location to find and view the flat files in the datamediation subdirectory. The value can be a local directory, or it a directory on another Catalog Component computer.

Important! The folder name *FileStore* is case-sensitive. Therefore, use the correct case in path names and all other programmatic references.

Depending on the completeness of the usage data, the data is loaded into the database into a *reference table*, a *temporary data table, or* a Data Mediation *event table*. Define the mapping between external data feed fields to database field types before importing data. The field definitions also contain the Driver Validation Rules which are enforced upon data import and filter irrelevant data.

Data Summary

During Data Mediation design, determine where to summarize data. For example, if your business objective is to measure average CPU usage over a month for reporting. If the data source system has running information and can determine the average over the period, then use a single, summarized data point rather than a data series of five-second samplings over the same time period. This data point serves to use computer and human resources (CPU, bandwidth, maintenance) efficiently. The best practice is to summarize information early in the process.

Data Aggregation

Data Aggregation is the gathering and expressing of data in a summary form. Data from the reference tables or temporary data tables are normalized into a set of Data Mediation event tables.

Aggregation processes one event at a time. Normalization or initial aggregation is customized using a SQL query and is specified in the Data Mediation profile. Data that is stored in Data Mediation event tables represents complete usage event data. All data from Data Mediation event tables is aggregated. The results are loaded into the set of metric-based result tables. These metric requests are processed for the Service Accounting Component rating engine. Budgeting information and billing transactions are created based on the resulting data that is contained within the metric result tables.

Imported usage data by defined profiles is processed for Service Accounting Component through Data Aggregation. The usage data is imported using the Metric Data Profile. Before usage data is aggregated, the data must be normalized into a common format. The common format consists of fields that are known as Server Mandatory fields. Five Default Server Mandatory Fields are required in every record to qualify as complete event usage data.

Service Accounting Component creates billing transactions that are based on the event results. The data that is imported through Data Mediation is aggregated based on the fiscal period. The data can be aggregated for a defined fiscal period or for all fiscal periods. Aggregation produces results by server mandatory fields, for example, by account, service offering, metric, and fiscal period.

When an aggregation is run for a defined fiscal period, the transactions of the previous aggregation are deleted. Then, new transactions are created to reflect the data being imported. This result is due to the transactions being rolled back on re-aggregation. The new transactions are created as part of the aggregating again. Therefore, regenerate the invoices to capture these new transactions, and show the associated charges.

Note: You can use Invoice groups and then generate your invoices in batch mode. You can also bill for two different data sets that are imported at two different times. You can do an aggregation after the first one is imported and then aggregate again after the second data imported. Generate the invoices *after* you verify that all the data for that fiscal period is valid.

The Data Mediation component aggregates data as follows:

- Generates usm_mr_itemp_XXXXXX data from the external files and databases.
- Generates usm_mr_ievent_XXXXXX data from the usm_mr_itemp_XXXXXX data based on the SQL aggregation specified in the Data Mediation profile. The XXXXXX values are sequential numbers that the system generates.
- Generates usm_mr_iresult_YYYY data from the usm_mr_ievent_XXXXXX table that is based on the built-in aggregation logic. The YYYY is the internal metric ID for the event that is specified by the aggregation.
- Generates transactions for the accounts that are based on the usm_mr_iresult_YYYY data that is created.

You can run the aggregation process any number of times for a fiscal period to reflect the latest imported data.

Custom Fields

You can use custom fields to facilitate aggregation logic. For example, business rules can indicate that the processing of rows in a data set varies based on external value.

You can also use custom fields to maintain legacy information as part of a user interface customization. For example, a charge can have a value in an external system that is used to perform cross referencing.

Aggregation Status

The possible data aggregation status values are as follows:

- Load files only -- New data has been imported since the last aggregation. Aggregation is not currently occurring.
  Numeric code: 0
- Importing -- Data is being imported and initial aggregation logic in profiles is being executed. In this phase, any data in reference tables or temporary data tables is being placed into Data Mediation event tables.
  Numeric code: 1
- Aggregating -- Aggregation is being performed. DC Importer is performing aggregation. In this phase, the data in Data Mediation event tables is being stored into the metric results tables.
  Numeric code: 6
- Profile Error -- An error occurred while executing initial aggregation logic contained in profiles. Aggregation is stopped. Go to Profile Management to locate profiles that are in error. Profiles in error are denoted with Error in the Import Status column.
  Numeric code: 8
- Profiles Pending -- A profile has not been defined. Aggregation is stopped. Profiles containing usage event data must be defined.
  Numeric code: 7
- Waiting for CA Service Accounting -- The Service Accounting Component rating engine is creating billing transactions.
  Numeric code: 5
- Aggregation Error -- A severe error occurred during aggregation.
  Numeric code: 4
- Aggregation Complete -- Aggregation completed successfully.
  Numeric code: 3

Data Management

Data Management lets administrators manage data sets imported into the CA Service Catalog by using the following functions:

- **Unload Checked**
  Unloads (removes) the data from the data mediation tables. The associated charges are removed the next time aggregation occurs.

  Note: You do not need to roll back the invoices that used the data that this data set provides before unloading and aggregating again,

- **Re-import Checked**
  Reloads imported data sets and effectively resets the aggregation flag of the imported data set to "not aggregated." The associated charges are recalculated the next time aggregation occurs.

- **Archive Checked**
  Archives the selected data set. The status of the data set is changed to Archived.

  Note: Archived data sets cannot be unloaded or re-imported after archiving. Use archiving only if required.

Note: Aggregation results for a period appear on the Aggregation Status page, although data for that period has been unloaded and aggregated again.

Reference Data

Reference data is often required to facilitate the transformation process. An example is the need to translate account codes from a legacy system to match accounts in CA Service Catalog. In such a case, you can match accounts in the following ways:

- You can customize the user interface to add a field for the legacy account code in CA Service Catalog. This option is best to use when the mapping information is static and can be maintained through data entry.
- You can use a reference table. This option is required if the mapping data is dynamic and it is maintained outside of CA Service Catalog.

Data Import

After creating a data mediation profile and defining the data feed and structure of the external data, import the data. You can import database profiles as needed and can schedule them to occur later.

You can import data from a file or from an Ingres, SQL Server, or Oracle database table. Data is loaded into database tables when imported.

The database tables that the Data Mediation creates include the following types:

- **Reference tables**
  Contains reference data to be used as lookup tables (usm_mr_iref).

- **Temporary tables**
  Contains partial usage event data, meaning that all server mandatory fields are not present, implying that normalization is necessary (usm_mr_itemp).

- **Event tables**
  Contains complete usage event data (usm_mr_ievent).

- **Metric result tables**
  Contains aggregated event data (usm_mr_iresult).

Data Profiles

Every data profile has one data source. The data profile contains a definition of the data feed of the external data. The profile also contains the initial aggregation logic in the form of a SQL statement. This initial aggregation logic is specified during profile definition. A data source can consist of an ASCII file (fixed-length, or delimited) or a database query. For database queries, multiple physical database resources (tables, databases) can be combined into a single result set. The resulting set is considered a single data source.

One set of fields exist per profile. Consider the size of the returned dataset. Determine how to deal with portions of the total data so that you can perform loads, unloads, and aggregations in smaller sets.

Unique initial aggregation logic (normalizing and aggregating raw data) indicates a unique profile. However, given the same data source and fields you can copy an existing profile to create a profile. You do not have to redefine the source information. For example, consider the situation when given a single data source, aggregation logic varies based on some field value.

The types of profiles for Data Mediation are as follows:

- Metric Data -- Usage event data for the cost allocation process of Service Accounting Component. This type of profile loads data into temporary or event tables that are based on the completeness of the usage event data.

- Reference Lookup Data -- Data contains reference data for lookup purposes. Data is loaded into reference tables.

If necessary, usage event data can be normalized or aggregated, preparing it for the aggregation process and cost allocation process. To do so, use an SQL query or procedure that is defined in the profile.

Repository Agent

The CA Service Repository Agent automates the process of importing usage data. The usage data is stored in Delimiter Separated File or Fixed-Length File format. The CA Service Repository Agent is also known as Data Mediation Data Repository Agent. The repository agent is installed as a service named CA Service Repository Agent during the installation of Catalog Component.

The Repository Agent imports usage data files into the database in the following ways:

- The agent can be configured to read files from an FTP server. The files are automatically copied from the FTP server locally and processed based on associated Data Mediation profiles.
- An external system can locally copy the usage data files. The usage data files are then processed based on associated Data Mediation profiles.
- A Data Mediation profile can be generated externally as an XML file. The XML file can then automatically be loaded and used to process a corresponding data file where both the profile definition XML file and the data file are copied locally by an external system.

Note: The integration with CA NeuMICS uses this technique.

Data Import Frequency

Decide the frequency of data imports. To determine the frequency, consider your reporting requirements.

For example, consider the following situations:

- If an invoice, an SLA report, a metric report, or a custom report is run daily, then the Data Mediation feed frequency must also be daily.
- If the data is required for a monthly bill run, then a monthly feed can be appropriate.
- If millions of records are loaded monthly, import subsets daily to spread the processing. You can also minimize the end-of-month window. Another benefit of this approach is to avoid having to unload and reload larger data sets when changes are necessary. The size of the data set does not affect the commit size in the database tables. The best practice is to perform commits in small batches, rather than after the entire data set. This approach minimizes lock contention and log file growth.

Implement Data Mediation

This article contains the following topics:

Administrators use data mediation functions to import, aggregate, and summarize data from external sources. Administrators use the results to help calculate costs for usage-based billing and to generate reports.

Important! As a prerequisite, verify that your fiscal period has been defined to fit your business model.

Step 1 - Define Data Fields

Define the Extraneous fields from an external data feed to map the external data feed field to a database field type. You can also define field definitions when creating a profile. When creating a profile, you use field definitions to define the structure of the external data.

When usage data is imported, it is uploaded into the database. During data import, data validation checks are performed. The invalid records are not uploaded into the database. Before data is imported into the database, you can apply rules to filter out erroneous or irrelevant data. The field definitions hold the definition of these validation rules, specifying a validation rule on each column of data imported.

Follow these steps:

1. Select Accounting, Data Mediation.
2. Click Add to define a new field.
3. Specify the information in the Define a Field window. The following fields need explanation:
   - **Mandatory Types**
     - None - indicates that both the server and the client are not mandatory.
     - Server Mandatory - indicates that the field is required for data mediation aggregation to occur. The absence of these fields results in a profile error.

     Client Mandatory - includes the field in profile definitions.
   - Both - indicates that both the server and client are mandatory.
   - **Default:** Server Mandatory
4. **Check type**
   Specifies the check type, if applicable.
   - **Default:** No check
5. (Optional) Specify a driver validation rule:

- **Not Empty**
  Specifies that the field value must not be empty.

- **Range**
  Specifies that the field value falls within the specified range.

- **Lookup**
  Specifies that a field value exists in a database table field.

- **Lookup Replace**
  Specifies a replacement value, if the value in the field exists in the specified database table field.

These validation rules are enforced when usage data is imported. If the driver validation rules are violated upon import, a kickoff report is generated. The report is available through the Data Management user interface.

6. Click Submit.
   The data fields are defined.

Default Server Mandatory Fields

Normalize the usage data into a common format that data mediation can understand before it is aggregated. The aggregation results in an error if the following server mandatory fields are not included:

- **CA Service Account Number**
  Associates a data record to a Service Accounting Component account ID.

- **Event ID**
  Associates a data record to an event (Event ID).

- **Event Time**
  Associates a data record to a fiscal period (Time Stamp).

- **Metric Value**
  Associates a data record with a metric value.

- **Service Code**
  Associates a data record with a service offering (Service Offering ID).

Note: Formatting data to include all server mandatory fields before data import is unnecessary. Data Mediation features complex data mapping mechanisms, such as validation and normalization, which help the administrator include server mandatory fields.

Step 2 - Create a Profile

Profile management is a definition of the data feed of the external data. The profile also contains the initial aggregation logic in the form of an SQL statement.

If necessary, usage event data can be normalized or aggregated, preparing it for the Data Mediation's aggregation and cost allocation processes through a SQL query or procedure defined in the profile. This profile feature helps normalize the data to a common format understood by Data Mediation.

You can create a profile to define the data feed of the external data.

Follow these steps:

1. Click Accounting, Data Mediation, Profile Management.
2. Click Add New Profile.
3. Select the Data Type:
   - **Metric Data**
     Specifies the usage event data for the cost allocation process. This type of profile loads data into temporary or event tables based on the completeness of the usage event data.
   - **Reference Lookup Data**
     Data contains reference data for lookup purposes. Data is loaded into the reference tables for data mediation.
4. Select the Import Format.
5. Click the Define Fields button.
   A profile template window appears for field definitions.
6. Enter a unique name for the profile you are creating. Define the fields for the profile.
7. Click Save.
   The profile is created.

Note: You can optionally edit or delete profiles. But you cannot edit profiles after they have been aggregated. If the Import Status is “Processed,” you cannot edit the profile. You cannot delete data profiles after they have been aggregated.

Step 3 - Create an Application Metric

The Data Mediation component uses metric packages to measure usage of an application.

Follow these steps:

1. Add, edit, or delete event information, as follows:
   a. Select Accounting, Data Mediation, Application Metric, Event.
      The Event List window appears.
   b. Click Add to create an event or click Edit to modify an existing event.
      The Event Detail window appears.

c. Specify all details about the event and click Save.

2. Add, edit, or delete metric information, as follows:

   a. Select Accounting, Data Mediation, Application Metric, Metric.
   The Metric List window appears.

   b. Click Add to create a metric or click Edit to modify an existing metric.
   The Metric Detail window appears.

   c. Specify all details about the metric and click Save.

   d. Link or unlink related events, as described in the next step.

3. Link or unlink related events for a metric, as follows:

   a. Ensure that at least one event is associated with each metric.

   b. Click Associate Event.
   The Metric Name: *metric name* window appears, displaying all events that are not already associated with the metric.

   c. Select the events that you want to associate with the metric.

   d. Click Associate Event. The selected events are linked and therefore appear in the Associated Events list.

   e. Select the events that you want to disassociate and click Disassociate Event.

4. Add, edit, or delete application information, as follows:

   a. Select Accounting, Data Mediation, Application Metric, Application.
   The Application Detail window appears.

   b. Click Add to create an application or click Edit to modify an existing application.
   The Application Detail window appears.

   c. Specify all details about the application and click Save.

   d. Link or unlink related metrics, as described in the next step.

5. Link or unlink related metrics for an application, as follows:

   a. Ensure that at least one metric is associated with each application.

   b. Click Associate Metric.
   The Application Name: *application name* window appears, displaying all metrics that are not already associated with the application.

   c. Select the metrics that you want to associate with the application.

   d. Click Associate Metric. The selected metrics are linked and therefore appear in the Associated Metrics list.

e. Select the metrics that you want to disassociate and click Disassociate Metric. The selected metrics are unlinked and therefore no longer appear in the Associated Metrics list.

6. Click Done.

The application metric is created.

Step 4 - Import the Data

You can import data by using Data Mediation.

Follow these steps:

1. Click Accounting, Data Mediation, Data Management.
2. Click Import Data.
3. Select the appropriate Data Type of the profile.
4. Select the import format.
5. Select the appropriate import profile for the data to be imported.

> **Note:** You can specify a filter and description.

6. Click Import Now.
7. (Optional) Click Schedule Import to automate the process of importing usage data.
   The scheduling information is already populated. The administrator only schedules the task by entering an optional Comment and the required fields. Do not modify fields other than Comment and the required fields.

> **Note:** To edit a scheduled database import, go through the Scheduler user interface and click View Scheduled Tasks.

Configure the CA Service Repository Agent

You can configure the CA Service Repository Agent by modifying the settings in the configuration file USM_HOME\repagent\config\repagent.cfg. Use the CA Service Repository Agent to automate the import of usage data that is stored in Delimiter Separated File or Fixed-Length File format

The repagent.cfg file uses the following parameters:

- **usm.url**
  Specifies the Catalog Component URL.

- **init.pause.ms**
  Specifies the pause time (for initialization) in milliseconds when the repository agent starts up.

- **repeat.interval.ms**
  Specifies the polling interval in milliseconds. The Repository Agent polls the FTP server for any new files that are based on this value. This value also determines the polling interval for processing local files.

- **upload.list.file**
  Specifies the profile configuration file name.

- **history.file**
  Specifies the repository agent upload history log file name. The repository agent keeps a log of all files that are imported to the database.

- **ftp.host**
  Specifies the FTP host name.

- **ftp.user**
  Specifies the FTP user name.

- **ftp.password**
  Specifies the FTP password name

Automatic Profile Load with Data Load

If the profile to be used is not already in the database, the repository agent can automatically load the profile and can load the associated data. This approach requires a pair of files in the USM_HOME\repagent\data folder with the same file name except for the extension. The file with the extension of .xml contains the profile definition. The file with the extension of .txt contains the usage data. For example, suppose a profile definition that is named abc.xml exists. The repository agent loads that profile into the database and uses it to process an associated usage data file abc.txt.

The profile definition XML file must follow a certain format. If integrated with CA NeuMICS, CA NeuMICS automatically generates this profile definition. For loading other usage data from other systems, generate the profile XML file according to the supported format.

Profile XML File Format

To generate a profile from an external source, use the format in the sample profile XML file. This file resides in the USM_HOME\repagent\data\samples folder.

The profile XML file that the repository agent uses to create a Data Mediation profile contains two sections:

Profile section
Contains information about the data mediation profile. Only one profile section can exist for each XML file.

- profile_name - the profile name (mandatory).

- profile_type - the profile type where 0=reference, 1=metric (default is 0).

- import_format - the format of the data source where 0=delimiter-separated file, 1=fixed-length file (default is 0).

- field_separator - the delimiter between fields in the usage file. The valid values are either the character itself or the ASCII numeric value for the following characters: ampersand (&), asterisk (*), at sign (@), comma (,), dollar sign ($), exclamation mark (!), percent (%), period (.), pipe (|), or space ( ). The ASCII numeric value for a tab can be used.

Field section
Contains information about each column of the data file. You can use this section to create the fields in the Data Mediation profile. Each XML file can contain many field sections.

- field_name - database table column name (mandatory)

- display_name - display name of the field

- mandatory - mandatory status

  - 0 - both server and client are not mandatory.

  - 1 - server mandatory

  - 2 - client mandatory

  - 3 - both client and server mandatory

- data_type - data type

  - 0 - string

  - 1 - integer

  - 2 - float

  - 3 - date

  - 4 - decimal

  - 5 - double
    A data type of “double” is converted to “float” during import.

  - 6 - binary

- data_length - the length of this field

- data_format - the format of date data (only if data_type =3).
  A dash (-) can replace a slash (/)in the following formats: The separator between the date and time portion can be a slash (/), dash (-) or space. Upper or lower case letters can be used. For example, YYYY-MM-DD hh24:mi:ss is a valid format.

  - MM/DD/YY

  - MM/DD/YYYY

- MM/DD/YYYY HH:MI:SS
- MM/DD/YYYY HH24:MI:SS
- MM/DD/YYYY HH:MI:SS.MSS
- MM/DD/YYYY HH24:MI:SS.MSS
- DD/MM/YY
- DD/MM/YYYY
- DD/MM/YYYY HH:MI:SS
- DD/MM/YYYY HH24:MI:SS
- DD/MM/YYYY HH:MI:SS.MSS
- DD/MM/YYYY HH24:MI:SS.MSS
- YY/MM/DD
- YYYY/MM/DD
- YYYY/MM/DD HH:MI:SS
- YYYY/MM/DD HH24:MI:SS
- YYYY/MM/DD HH:MI:SS.MSS
- YYYY/MM/DD HH24:MI:SS.MSS

- default_value - the value for this field. The Catalog system uses this value, not the input record.
- start_position - if import_format=1 (fixed-length file), start_position is the starting position of the field in each record, starting at 1. If import_format=0 (delimiter-separated file), it is the field position starting with 1.
  For example:
  - For a fixed-length file, a record contains “abc001” and this field is the numeric portion. Therefore, the start_position is 3, and the end_position is 6.
  - For a delimiter-separated file, a record contains “abc,001” and this field is the numeric portion. Therefore, the start_position is 2, because this field is the second field. Also, the end_position is blank.
- end_position - required only when import_format=1. It is the ending position of a field in each record.
- status - status of the field (default is 1)
  - 0 - system (cannot delete)

- 1 - active
- 2 - inactive

Profile List

When a profile is created and the repository agent must process the usage data, the agent must be made aware of the new profile. The profile information is specified in the Profile List file that is named in the upload.list.file setting. This file is located in the USM_HOME\repagent\config folder.

The format of each record in the Profile List file is as follows:

```
profile_table_id, usage_file_name
```

- ***profile_table_id***
  Specifies the numeric ID value from the Data Mediation profile Source Table column, without the leading zeroes. For example, if the Source Table column contains entry usm_mr_itemp_001012, the *profile_table_id* entry in the Profile List file for this profile is 1012.

- ***usage_file_name***
  Specifies the full path and file name for the usage file corresponding to the profile referenced in the first parameter, for example, C:\Program Files\CA\Service Delivery\repagent\data\my_usage_data.txt.

Step 5 - Aggregate the Data

You can aggregate the data.

Follow these steps:

1. Select Accounting, Data Mediation.
2. Select Aggregation Status.
3. Complete the window options:
   - **Use selected period for aggregation**
     Aggregates data that is contained within a specific fiscal period (suggested). Only data falling within the specified date range is aggregated. Not selecting this option aggregates data for all fiscal periods.
   - **Advanced Option**
     Specifies multiple fiscal periods.
4. Click Start Aggregation.
5. (Optional) Click Refresh to check the Aggregation Status during data aggregation.
   The data is aggregated. To view the details, including history, for an invoice, navigate the Aggregation Summary pages for the account of interest. Alternatively, click Accounting, Account Management and click the action icon that is named View Invoice History for account name.

Data Mediation Aggregation Utility

You can start a data mediation aggregation using a command-line utility. For Windows, the startDMAggregation.bat file is located in the USM_HOME\scripts folder.

The syntax for using the startDMAggregation.bat (Windows) command is as follows:

```
startDMAggregation.bat [startdate] [enddate]
```

Specify the start date and end date in MM/DD/YYYY format.

Define Aggregation Logic

You can define the initial aggregation logic in the form of an SQL statement.

Follow these steps:

1. Click Accounting, Data Mediation, Profile Management.
   If the target table column is empty and the configuration status is “pending,” the initial aggregation logic for the profile is not yet defined. The presence of a target table entry and a configuration status of “Defined” indicate that the profile has been defined.

   Note: The Target Table column is visible when the Show more columns double arrow icon is clicked.

2. Click the Define Aggregation Logic icon.

3. Drag-and-drop each field from the data source into the target table field to define the logic to be used during aggregation.

4. Click Generate Query to generate the SQL Expression.

   Note: You can define the initial aggregation logic by using a SQL statement or procedure. Specify the initial aggregation logic to prepare the imported event usage data to include all of the server mandatory fields for the aggregation and cost allocation process. For example, suppose that you have usage data for each host in temporary tables for data mediation. You want to map the hosts to accounts using the data mediation reference tables. In that case, perform a join of these tables in the SQL procedure to prepare the event table.

5. Click Save.
   The aggregation logic is defined.

Define Multiple Aggregation

Data that is imported from an external source can be aggregated in multiple ways. To fulfill this requirement, you can define multiple profiles that are based on the same data set. This definition lets you use one set of external source data. You can then aggregate the external data in different ways to meet your business requirements.

Follow these steps:

1. Go to Accounting, Data Mediation, Profile Management.
2. Click Copy for the profile for which you want to define a new profile and different aggregation logic.
   A copy of the profile using the same name is created using the same source. The SQL Expression is not copied.
3. Click the new profile and define the alternate aggregation logic for this data source. Click Save.
   A different target table entry is created.

When data aggregation is called, the SQL query or procedure runs, resulting in two separate event tables. If the data in both tables is normalized properly, both data sets are aggregated successfully.

Note: The initial aggregation logic for a profile is run without regard to sequential order.

Step 6 - Generate Invoices

You can use data aggregation to generate invoices in Service Accounting Component. If you generate an invoice after an aggregation and again aggregate the data for the same fiscal period, the previously generated invoice has zero charges. These zero charges are due to the transactions being rolled back on aggregating again. You regenerate invoices to capture the new transactions. You can use invoice groups and can create invoices in batch mode. If two different data sets are involved at two different times, you can aggregate when the first data set is imported and again aggregate after the second data set is imported. You then generate invoices after all the data for that fiscal period has been received and verified.

Follow these steps:

1. Create profiles for each data set to mediate and then aggregate.
2. Import the data (files and external database) for the associated profile.
3. Define fiscal periods depending on the business model.
4. Aggregate data so that the metric result tables and the Service Accounting Component transactions are created. Repeat the aggregation process if any new data is imported or changed for that fiscal period.
5. After all the data is received and is aggregated, generate the invoices that reflect the aggregated data.

Data Mediation Reports

Several Data Mediation report data views are available:

Data Mediation - Profile List
Displays a list of Data Mediation profiles, including the following associated parameters:

- Index ID
- Profile Name
- Status
- Temp Table
- Event Table
- Data Import Type
- Profile Owner
- Description
- ID

Data Mediation - Rating Engine Queue Items
Displays rating engine queue items by the specified runtime variables. Enter the start and end date and times. The report displays the Data Mediation Rating Engine Queue items, along with the following associated fields:

- Index
- Group ID
- Queue Item ID
- Created Time
- Status
- Start Time
- Finish Time
- Metric Result ID
- Metric Result Table Name

Manage Chargeback and Pricing Models

This article contains the following topics:

Chargeback

Enterprises can define their services to allocate costs internally for budgeting and chargeback or to charge customers for them. Service Accounting Component supports various chargeback methodologies. Charges can be per transaction, or per session, and can vary by resource. The rates that are used can vary by service package and activity level. When CA Business Service Insight is integrated, the invoices that are based on real-time usage data can be generated. Adjustments can then be applied automatically to reflect any SLA violations.

Under most circumstances, the cost that is charged to a business unit is not disputed. The cost can be directly attributed to IT services that have a role in supporting its business operations. The primary focus is on whether or not the provided services and the corresponding costs are at the levels anticipated. In essence, business units want to be certain that they are getting everything that they are paying for. Business Units want to know how to distribute the burden of cost and how to lower it. Conversely, an organization must verify that all costs are recovered regardless of whether or not resources are fully utilized. The process of distributing the cost must be easily managed. The system that is put into place influences business unit behavior and demands.

Administrators can configure Service Accounting Component to specify chargeback and to use one or more of the following pricing models:

- Subscription-based Pricing (see page 3152)
- Usage-based Pricing (see page 3153)
- Tiered-based Pricing (see page 3153)
- Combined Approach (see page 3154)

Subscription-Based Pricing

Chargeback can be done regardless of actual consumption, but on a fixed basis using a specific unit of measure and unit cost. This method is known as subscription-based pricing. This strategy can be implemented by using any chargeable type service option element when defining services for a Business Unit. This element type allows for the specification of a unit cost, billing cycle, and quantity. Examples include subscription charges, such as $500 per month or $1000 per laptop.

This method is used when the true cost driver is unknown or it is too difficult to ascertain. Because the subscription is based on a controllable unit of specification, this approach provides the Business Unit with some control over cost expectation and a clear picture of their IT-related costs. But this method fails to meet any objectives pertaining to fairness. Disparate resource use is not accounted for, as the treatment of all subscribers is equal. This decoupling of service cost and usage translates into a system that tends to fail to motivate Business Unit behavior. So, subscription-based pricing does not guarantee the recovery of cost or that profit is generated.

Usage-Based Pricing

Usage-based pricing enables IT to charge back to Business Units cost based proportionately to their consumption of resources. This strategy can be implemented by using the Application type service option element and choosing the Usage Based selection for its Pricing Structure when defining services for a Business Unit. This element type allows for the specification of a unit cost and a metric type.

Import the usage-based data into the system using data mediation. Use this metric result to calculate the total cost of that service for an account. In addition to global account charges, these usage-based amounts can be processed on a per user basis.

Implementing usage-based billing involves knowledge and decision at multiple levels within an organization such as:

- Financial decisions determine how to present and price these services.
- IT technical decisions on where and how to collect and process useful usage data and how to handle exceptional cases like adjustments and promotions.

This method assumes that the associated resources are shared among several Business Units and their unit cost is fairly static. Consumption is directly linked to the cost incurred. For example, when services are set to employ weighted distribution as the means of distributing charges, lowering usage levels of these services does not always guarantee lower cost. One Business Unit can decide to cut usage, thus expecting a relative change in the cost that it is allocated. However, if all other Business Units that contend for the same resources also decide to cut back on usage, but at a higher rate, the original Business Unit is forced to pay more than it did previously. Although control can be a problem, this model affects business unit behavior.

Tiered-Based Pricing

Tiered-based pricing enables IT to charge back to business units based on levels of service. A tiered structure can be constructed associating various rates to level ranges. This strategy can be implemented by constructing a tiered type service group to contain these ranges and corresponding rates, and defining services to draw their costing information from them based on a passed value. You can use this value to look up and select the appropriate tiers.

Consider a tiered service group that contains two columns. In the first column, various ranges can be defined, such as numeric values 1-100, 101-1000. In the second column, associated rates can be defined. You can configure several service group elements to use this tiered service group to determine their cost.

For example, an application service group element can be created to use this tiered service group. To do so, select Tiered-Based as its Pricing Structure. During the cost calculation for this element, the metric value can be used to select the matching tier and use the corresponding rates. The unit specification at that rate can be derived in a number of ways, such a predefined fixed quantity or the metric value itself. Agreement service group elements can employ tiered service groups to attribute a cost that is based on the number of violations.

Combined Approach

The combined approach creates a chargeback procedure that is tailored to the needs of a specific organization. For instance, a particular organization can implement a system that influences service objectives by using a tiered-based pricing with assurance adjustments on top of a fixed recurring subscription charge. Here the aim is to strengthen the control a Business Unit has over the quality and equitability of a service, while providing for a great deal of stability and predictability of cost.

A differentiation can exist between services that are bound to the infrastructure of that organization and those that are not. These infrastructure services can be positioned to do chargeback that is based on a specified allocation method as in a 'per subscription' basis. Chargeback for the other services can be based on actual consumption using a fixed rate.

Implement Usage-Based Billing

This article contains the following topics:

Step 1 - Verify the Requirements for Services

Administrators can set up usage-based billing to charge for services that are based on consumption. Administrators use data mediation to import usage-based data. Then this data is used to calculate the cost of a service for a business unit, user, or account.

Verify the requirements for the services for which you are implementing usage-based billing. The service option groups being billed must include a service option that is configured as follows:

- Type = Application
- Pricing Structure = Usage Based
- Cost Type = Specify Value
  Do not select User Specified for the Cost Type if you are using usage-based billing through data mediation logical mapping. If you select User Specified for the Cost Type, then users can overwrite the default unit cost. The default unit cost is defined in the original service definition. However, data mediation logical subscription is designed to use the default unit cost that is defined in the service definition.
- Unit Cost = any numeric value
- Application = any available application (for example, Operating System Platform)
- Metric = any available metric (for example, Disk Quota Used (KB) Per User).

Step 2 - Create the Users and Account

To get started implementing usage-based billing, create one or more users and associate them to an account.

> **Note:** If the service activation is to be achieved through request management, then the user is automatically associated to the account.

Step 3 - Create an Application Metric

To create an application metric, see the section "Create an Application Metric" in Implement Data Mediation (see page 3139).

Step 4 - Create Data Mediation Profile

To create a data mediation profile, see the section "Create a profile" in Implement Data Mediation (see page 3139).

Step 5 - Define Aggregation Logic

To define the aggregation logic, see the section "Define Aggregation Logic" in Implement Data Mediation (see page 3139).

Step 6 - Import the Data

You can import database profiles as needed and can schedule them to occur later.

You can import data from a file or from an Ingres, SQL Server, or Oracle database table. Data is loaded into database tables when imported.

The database tables include the following types:

- **Reference tables**
  Contains reference data to be used as lookup tables (usm_mr_iref).
- **Temporary tables**
  Contains partial usage event data, meaning that all server mandatory fields are not present, implying that normalization can be necessary (usm_mr_itemp).
- **Event tables**
  Contains complete usage event data (usm_mr_ievent).
- **Metric result tables**
  Contains aggregated event data (usm_mr_iresult).

Step 7 - Aggregate the Data

To aggregate the data, see the section "Aggregate the Data" in Implement Data Mediation (see page 3139).

Mobility

This section contains the following articles:

PDA Interface

CA SDM supports ITIL terminology for the Personal Digital Assistant (PDA) interface. This interface lets end users create Requests, Incidents, and Problems, and lets them search for the following ticket types:

- Incidents
- Problems
- Requests
- Change Orders
- Issues

Analysts can use the PDA interface. This interface honors the role present in the *PDA Role* field of the Access Type of the contact.

The PDA Interface is displayed for on any unsupported device or browser.

Look up service for searching a contact works only on PDA browsers that support multiple tabs and multiple browser windows. Multi-tenancy works similar to the browser interface, but the drop-down list to select multi-tenancy is not provided. When you create the ticket, tenancy is based on the requestor, the affected enduser, and the analyst.

Automatic Priority Calculator (APC) helps in deciding priority while creating Incident/Problem, based on the attributes, urgency, impact, request area, and affected end user.

Note: The PDA Interface does not support attachments when you create tickets.

REST Sample Mobile User Interface

The REST sample mobile user interface provides two user interfaces: Analyst and Employee. This sample also supports the Administrator, Level 1 Analyst, and Employee roles. After you log in to CA Service Desk Manager, the Administrator and Level 1 Analyst roles view the analyst interface. The Employee role views only the employee interface. If an administrator disabled Automatic Priority Calculation, the Priority field appears on create and edit pages.

Important! This functionality applies only to the sample program provided in this release of CA Service Desk Manager. It is not a design that is restricted in the REST Web Services application itself.

Fields that use auto suggest require a value selection from the auto suggestion list, such as the assignee and Incident Area. If you do not select a value, the user input for that field clears.

Note: Navigate REST interfaces with the provided buttons, instead of using the browser back and forward options. For example, select Home or Cancel to return to a previous page.

Analysts can perform the following tasks:

- View Announcements.
  Default: Sorted by Posted Date
- View Incidents that CA Service Desk Manager assigned to the Analyst.
- View Assigned and Unassigned Incidents.
- Sort Incidents.
  Default: Sorted by Open Date.
- Search for an Incident.
- Create an Incident.
- Modify the Status, Urgency, and Impact of the Incident.
- View and update the Activity Log with a comment, or specify Callback or Research.
  Default: Sorted by Activity Date.

Employees can perform the following tasks:

- View Announcements.

- View open and closed Incidents that an end user created.
- Sort Incidents, such as by Open Date.
- Create an Incident.
- Update the Activity Log with a comment.
- Search for an Incident.
- Modify the Incident status from Open to Closed, or Closed to Open.

Deploy the REST Mobile Sample User Interface

The administrator enables REST Web Services during the product configuration. The administrator then copies files on the CA Service Desk Manager computer to enable the REST mobile sample user interface. The analyst uses the mobile interface to manage incidents that end users open in CA Service Desk Manager.

Follow these steps:

- Step 1 - Configure REST Web Services (see page 3158)
- Step 2 - Enable the REST Mobile Sample UI (see page 3159)
- Step 3 - Manage Incidents from the REST Mobile Sample Interface (see page 3159)

Step 1 - Configure REST Web Services

By default, REST Web Services are enabled in the CA Service Desk Manager configuration. However, if the REST Web Services are not enabled at the time of CA Service Desk Manager installation, configure the REST Web Services.

Follow these steps:

1. Execute pdm_configure from the command-line interface. On Windows, click **Start**, **Programs**, **CA**, **Service Desk Manager**, **Configure**.
   The configuration dialog opens.
2. Confirm the configuration information for the **General Settings**, **System Accounts**, **Database**, and **Web Interface** dialogs.
   The **REST Web Services** dialog opens.
3. Enable the **Configure REST Web Services** option.
4. Specify the **REST Tomcat Port**.
   Default: 8050
5. Specify the **REST Tomcat Shutdown Port**.
   Default: 8055
6. Click **Next** and continue the CA Service Desk Manager configuration.
   The configuration completes.

Step 2 - Enable the REST Mobile Sample UI

CA Service Desk Manager disables the REST Mobile Sample user interface by default to prevent undesired access to the MDB. The administrator enables this interface manually.

Follow these steps:

1. Locate the following directory on the CA Service Desk Manager computer where REST web services is installed and configured:

   ```
   $NX_ROOT/samples/sdk/rest/mobiledemo
   ```

2. Copy this directory to the following location:

   ```
   $NX_ROOT/bopcfg/www/CATALINA_BASE_REST/webapps
   ```

   Note: You do not have to restart Tomcat.

   The REST Mobile Sample user interface is enabled.

3. (Optional) If you want to disable the REST sample user interface, remove the mobiledemo directory from /webapps.

Step 3 - Manage Incidents from the REST Mobile Sample Interface

The analyst or an employee views the REST mobile sample interface on their mobile device to manage incidents in the queue. For example, the analyst opens Incident 30 to log an internal-only comment.

The analyst or the employee can also download attachments.

Follow these steps:

1. Open the following URL on your mobile device:

   ```
   http://hostname:REST-Tomcat-port/mobiledemo/login.html
   ```

   The sample REST mobile interface login page opens.

2. Log in to CA Service Desk Manager using your credentials.
   The REST mobile analyst home page opens.

3. Select **Assigned Incidents**.

4. Select an Incident, such as Incident 30.

5. Select **Create Activity** on the detail page.

6. Select **Log Comment** from the drop-down list.

7. Select **Yes** from the **Internal** option.

8. Enter a comment and select **Save**.

CA Service Management Mobile Application

CA Service Management Mobile Application is a common interface to access some of the core features of CA Service Desk Manager and CA Service Catalog from your mobile device. The following mobile capabilities are available in CA Service Management Mobile Application:

Service Desk

The *Service Desk* capability enables the logged in user to access the following CA Service Desk Manager core features:

- View the count of the tickets from CA Service Desk Manager on the Home screen when you log in. You can view incidents, requests, problems, issues, and change orders only. The badge count on each tile shows the new and updated ticket counts since last refresh.

  Note: The Home screen does not display all the tickets from CA Service Desk Manager. By default it shows all the tickets that are assigned to all the users. This default filter can be changed.

- Tap a ticket type tile from the Home screen to view the list of tickets. Filter each ticket type to view only selected information. For example, tap the Filter icon from the Incident list and select Assigned - High Priority. The list is refreshed to show the selected incidents only.

  Note: Filters that are customized on the CA Service Desk Manager server and are displayed on the CA Service Desk Manager Scoreboard is also displayed in this capability.

- Search for ticket. Tap on the search area and enter the search keyword. The search results are displayed as you type. You can search for a ticket that is based on the ticket number or summary of the ticket.

- Tap a ticket to view the details. You can also view the attachments and activity logs (if any).

- Tap More Actions to perform actions on a ticket:

  - Escalate or update status or transfer ticket to another user.

- Add a comment to this ticket.
- Add an attachment to the ticket. Allowed size for the attachment is 3 MB or less. This capability only supports .jpeg, .jpg, and .png image formats.

- Change the refresh interval (**Default:** four minutes). Tap system menu, Settings, Preferences, Service Desk. Increase or decrease the Polling interval.
- Choose the features to be displayed in this capability. For example, the logged-in user can choose to view the incidents only. Go to the Settings screen and tap Features. Swipe to enable or disable a feature.

My Tasks

The *My Tasks* capability is used to respond to pending workflow tasks. This capability provides the mobile user with all the information required to complete the task.

The logged-in user can access the following core features of this capability:

- View the following tasks:
  - Pending tasks from the following workflow engines that are integrated with CA Service Desk Manager:
    - CA Service Desk Manager Classic Workflow
    - CA Process Automation
  - Workflow tasks that are assigned to the user. If the logged in user is part of the PAMAdmins group, the user can view and respond to any CA Process Automation tasks from the *My Tasks* capability.
  - Workflow tasks that are assigned to a group that the user belongs to.
    - For CA Service Desk Manager Classic Workflow, tasks that are assigned to the CA Service Desk Manager group are not displayed. Only tasks that are assigned to individuals are displayed.
    - If the logged-in user is part of the PAMAdmins group,the user can view and respond to any CA Process Automation tasks from the *My Tasks* capability.
  - Workflow tasks for which the user is requested to respond, regardless of the CA Service Desk Manager ticket assignee or requester. For example, a user who is not directly involved with CA Service Desk Manager performs a financial approval task.

Note: If a workflow engine is down and if the user is not using the related work item, *My Tasks* does not display the work items or an error message. When the workflow engine starts working, the related work items are visible to the user. But if you are already using a work item and the server goes down, then *My Tasks* displays an error report.

- View a bar chart showing the number of pending tasks that are awaiting input, as per the time the task has been pending. This bar chart allows the user to identify new tasks and identify how long they have been waiting.

- View the list of tasks that are filtered by pending time. Tap on the bar on the graph or use the pull down at the top of the screen. For example, tapping on Last Hour bar displays all the tasks that are created or modified in the last one hour and are pending for approval.

- Search for a pending task; enter the search text in the Search area. The search result is updated as you type. You can search using ticket numbers, priorities, or keywords from task descriptions.

- View the work item details by tapping on a task in the list. When you see the details, you can perform the following actions:

  - View the input form of the work item. Custom approval forms are automatically available on the mobile device without any modification. They are reformatted for rendering on the mobile device.

  - Understand more about the work item by tapping the ticket icon to view the related CA Service Desk Manager ticket information. This information can include business justifications, implementation and backout procedures, contact, assignee, information, priority, SLA, and severity.

  - Call or email the requester by tapping on the phone number or email address that is listed on the related ticket tab. This information is displayed only if the CA Service Desk Manager ticket contains this contact information.

  - Download and view attachments for the related change order ticket. Install other viewer software on your mobile device to open the downloaded document, if necessary. To view attachments from the web application of the CA Service Management, turn off the "block popups" option in the web browser.

- Respond to the work item. Enter the required information in the detail form and tap **Submit**. The next task is automatically opened for your response, if multiple tasks are pending.

- Upon request from support, enable debugging information by selecting the system menu, Settings, Preferences, My Tasks. Tap the Tracing drop-down to select an option. Choose the "on" option to enable the debugging information. Choose the "verbose" option for more detailed information. You can view the logging information in the $NX_ROOT\log\approve.log directory on the CA Service Desk Manager server. Disable the option to avoid server overhead when you have completed the support session.

- Change the date and time format by tapping the system menu, Settings, Preferences, My Tasks and by choosing a Date Time Format. The changed date and time format is only reflected once you refresh the capability.

- Refresh the current list of work items by tapping the system menu in the upper right-hand corner of the task list page and choose Refresh.

- Change the refresh time interval which specifies how often the *My Tasks* tile is updated, by changing the Polling interval found on the Preferences, *My Tasks* page.

- Enable response timeout option wherein a message is prompted to the logged in user if the capability does not respond within a specified time. As a logged in user, you can set this time (in minutes) from the system menu, Settings, Preferences, My Tasks. By default the Timeout in minutes option is set to two minutes. You can change this setting. If the capability does not respond within this scheduled timeout, an error message is displayed. After clicking OK on the message prompt, the user is directed back to the login page of the *My Tasks* capability.

Unified Self-Service

The *Unified Self-Service* capability enables the logged-in user to access the following core features of Unified Self-Service on a mobile device:

- View the count of the latest questions on the Home screen, that are posted from Unified Self-Service. The posts are categorized according to tags such as Recommended, Latest, Following. By default you view the Latest questions.
- (If Unified Self-Service is configured with CA Service Desk Manager) View the count of the tickets that you created on the Home screen. The tickets can be request or incident, as configured by the system administrator on the Unified Self-Service server.
- Tap on the question tile from the Home screen to view the related posts.
- Search for a post from all sources. Enter your search criteria in the Search text box and tap Enter to display the search results from all sources. From the drop-down, you can select Global to look from all the data sources that enabled on the Unified Self-Service server. You can also select Questions to look from the questions that are listed in this capability.
- Search for requests or incidents.
- Tap a question to view the detailed post. Tap More Actions to:
  - Reply to this post
  - Follow or unfollow this post
  - Share the post
  - Open a service desk ticket if the post does not answer your questions.

  Note: To add new fields in the request form, the system administrator has to configure the fields on the Unified Self-Service server. The same configured fields are displayed on the Unified Self-Service capability. The number of fields that can be configured on the Unified Self-Service is five. For more information about how to configure the fields, see Administering CA Self Service (see page 1679) section.

- Change the refresh interval (**Default:** four minutes). Tap system menu, Settings, Preferences, Self Service. Increase or decrease the Polling interval.

- Choose the features to be displayed in this capability. For example, the logged-in user can choose to view the Questions only. Go to the Settings screen and tap Features. Swipe to enable or disable a feature.

Create Ticket

The *Create Ticket* capability is available only for CA Service Desk Manager users. You can create a request or an incident.

Note: A Non-employee CA SDM user can use the **Affected End User** field to create a ticket on behalf of other users.

Catalog

The *Catalog* users can perform the following tasks from their mobile devices:

- Browse and search the catalog
- Complete and submit requests for service offerings (services)
- Add notes or attach images to their requests
- View the status and other details of their requests, including requests submitted from both the browser interface and the mobile application
- Cancel their requests

Request managers can perform the following tasks from their mobile devices:

- View their requests pending approval and approve or reject them
- Add note or attachments to those requests

Note: A Non-business CA Service Catalog user can use the **Affected End User** field, that is available on the Report An Issue Offering page, to create tickets on behalf of other users.

Localization Support for Mobile Application

CA Service Management Mobile Application supports the following 12 languages.

- English
- French
- Dutch

- Simplified Chinese
- Spanish
- Brazilian Portuguese
- Japanese
- Italian
- German
- Finnish
- Swedish
- Danish

If you are using CA SDM, observe the following:

- CA SDM does not support Finnish, Danish, Swedish, and Dutch locales.
- CA SDM supports the French Canadian locale but the CA Service Management Mobile Application does not support it.

When you upgrade to current release of the mobile application, the default language is set to English. You can set your preferred language. To change the language settings, navigate to **Settings**, **Preferences**, **Locale Settings**.

Some mobile application forms that are generated appear with labels based on the CA SDM server side data. In such instances, the data language depends on the CA SDM server locale set by the Administrator. For example, if CA SDM server locale is set in Japanese, and the Mobile Application locale is set in French, the forms with data labels from the CA SDM server side will appear in Japanese.

Verify the Prerequisites for CA Service Management Mobile Application

CA Service Management Mobile Application is certified for the following mobile operating systems:

- iOS
- Android

For information about the supported versions of the operating system, see the Supportability Matrix (https://wiki.ca.com/display/CASM1401/Supportability+Matrix) .

As an administrator, verify the following requirements before you configure CA Service Management Mobile Application:

- To access Unified Self-Service capability, install and configure CA Open Space 3.0 or higher to the CA Service Desk Manager server.
- To access Service Desk capability:
  - Associate the logged in users for Analyst Queue with the REST Web Service API role. Ensure that the *Administration*, *Security*, Stored Query, and *Reference* function accesses of this role are assigned with the View or Modify access levels. For more information about function access, access level and roles, see the Administering CA Service Desk Manager (see page 1302) section.
  - Install “Status_Policy_Violations” option on the CA Service Desk Manager Server with “Reject” as its value to ensure that the condition attached to the status transition rules are validated correctly.

Note: When CA Service Desk Manager users use the mobile application, they see that the status is updated even when the condition attached to the status transition rule fails. For example, consider a scenario when the “Status_Policy_Violations” is set to “Warn”, and the status transition rule states that there must be an assignee assigned to the Incident while updating from “OPEN” to “ACKNOWLEDGED”. In this scenario, the status is still updated to “ACKNOWLEDGED”, even if there is no assignee for the Incident.

To ensure that such an issue does not occur, install "Status_Policy_Violations" option on the CA SDM Server with "Reject" as its value.

- To access Catalog capability, ensure that you have deployed mobile access (see page 3166).

Deploy Mobile Access for CA Service Catalog

This article contains the following topics:

Step 1 - Verify Prerequisites for Mobile Access

Review the following prerequisites for mobile access:

- Understand the terminology in this article:
  - Services and forms that you design for catalog users and request managers to access from mobile devices are *mobile services* and *mobile forms*.
  - Services and forms that you design for catalog users and request managers to access from the web browser of a tablet, laptop, or desktop are *browser services* and *browser forms*.
- Ensure that you know how to design services and forms in CA Service Catalog.

- Familiarize yourself with how request managers approve and reject requests in CA Service Catalog.

Step 2 - Follow the Guidelines and Requirements for Creating or Updating Services

Meet the following requirements as you design your mobile services:

- Select the option that is named **Available from mobile devices**, on the Service Details tab.
- Specify *one* service option per service and you can add *one* form to that service option.
  After you add the form, save your changes and complete all other applicable fields on the Service Option Details tab. Keep in mind the following considerations and limitations:
  - You can add a reservation, and it *is visible* on a mobile device.
  - You can also add the following elements: CA Business Service Insight contracts, cost and pricing elements (such as rate elements), and additional elements (such as text elements). These elements are supported; however, they are *not visible* on a mobile device.
- If you use images, meet these requirements:
  - Use one of the following formats: BMP, PNG, JPEG, or .JPG.
  - Verify that the file size is less than 30 KB.
  - Verify that the dimensions are 50 x 50 pixels or smaller.

Guidelines for Services and Forms

Follow these guidelines as you design mobile services and mobile forms:

- Keep services and forms short and simple.
- Keep all names and descriptions short.
- Use the following predefined mobile-enabled services and their forms as models:
  - View My Assets (for Mobile Users)
    This service lets catalog users view their assets in CA APM.
    This service requires that CA Service Catalog and CA APM are integrated.
  - Report an Issue
    This service lets catalog users report an issue in CA Service Desk Manager, for example, a hardware or software problem.
    This service requires that CA Service Catalog and CA Service Desk Manager are integrated.

  To access these services, import the Service Management Content Pack. For more information about how to use this content pack, see the *Using the Service Management Content Pack* article. To access this article, log in to CA Service Catalog and select Administration, Tools, Links.
- *Only when necessary*, consider creating two forms and two services: one service and form for browser access and another service and form for mobile access. *When necessary* means that the browser service and form contain multiple or complex elements that are not supported on

mobile. For example, the browser service contains multiple service options and the browser form contains a table.
For examples, see the View My Assets and View My Assets (for Mobile Users) services in the content pack.

(Optional) Specify the Order in which Services Appear

You can optionally use the Sort Number field on the Service Details tab to specify the order in which services appear. The order of appearance is sequential, from lowest to highest. For example, three services with sort numbers of 1-3 are the first three services that appear when a user opens the catalog from a mobile device.

Note: When users view services from a mobile device, a single sort order applies across all folders. In contrast, when users view services from a desktop, laptop, or tablet, the sort order applies to each folder individually.

Customizations That Are not Supported

Mobile services do *not* support the following customizations:

- Custom approval statuses
  Use *only* default approval statuses for mobile services.
- Tiered service option groups

Step 3 - Follow the Guidelines and Requirements for Creating or Updating Forms

Follow these requirements and guidelines when you design mobile forms.

General Guidelines

The requirements and guidelines for services (see page 3167) include general guidelines about using forms.

Guidelines for Fields

To achieve the most efficient display and maximize user productivity, automatically specify the most common options as the default options. For example, use JavaScript expressions and the user profile to pre-fill fields for user attributes, such as name, address, phone number, and so forth. Similarly, if the user location is available, pre-fill it also.

Requirements for Labels

If you use labels (see page), test them thoroughly on mobile devices. Labels appear to catalog users who view services and submit requests. However, labels do *not* appear to request managers who approve and reject requests. Therefore, use the Description field of a service option (rather than a label) to convey important information about the form or service option to request managers.

The Full Width attribute of a label is automatically set to True when a form appears on a mobile device. This automatic setting optimizes the use of space on a mobile screen.

If you use an image as the value for a label, the maximum size of the image is 50 x 50 pixels or smaller.

Elements That Do Not Apply

Do *not* use the following elements on mobile forms because they do not apply:

- All tables (Static Table (see page 2921) or Dynamic Table (see page 2923))
- Dual list (see page 2919)
- Column layout (see page)
- Lookup Field (see page 2920)

Attributes That Do Not Apply

The following attributes do not function when users display the form on a mobile device. However, you can optionally include these attributes on a form that users access from both mobile and non-mobile devices. In such cases, these attributes work as designed for non-mobile access but do not function for mobile access:

Element	HTML Attributes	JavaScript Attributes
All elements	Hint, Style, Tab index, Text direction, Tooltip	onBlur, onKeyDown, onKeyPress, onKeyUponMouseDown, onMouseMove, onMouseOut, onMouseOver, onMouseUp
Check box	Box label	onFocus and onClick
Date Time	Time Format	onFocus and onClick
Field set	Collapsed and Label Width	Not Applicable
Radio group	Orientation	Not Applicable
Radio option	Not Applicable	onFocus and onClick
Select box	Minimum Search, Multi-Select, Page Size, List Width, and Height	onFocus and onClick
Slider	Message	onFocus and onClick
Spinner	Number Format	onFocus and onClick

Form Attributes That Do Not Apply

The following form attribute does not apply: CSS class.

Date Formats

Mobile services and forms support the date formats available for the business unit.

Mobile services and forms support custom JavaScript functions that set the value and format of the date.

Custom JavaScript

Important! Mobile applications typically provide access to more personal data than web browsers on a tablet, laptop, or desktop. Mobile applications also typically have more security concerns. Exercise caution when you use custom JavaScript in forms for services that users access through mobile devices. Verify that all custom JavaScript is safe and secure and does not violate the privacy of any users.

Mobile forms do not support custom JavaScript that uses either of the following techniques:

- JQUERY
- Communication between the form and CA Service Catalog web DOM elements

Approval Process

When request managers use a mobile device to view requests pending approval in their queues, the following fields and forms do not appear on the requests:

- Fields to specify data, either by entering text or selecting a value
  Examples include fields for specifying a cost or for selecting a cost center or priority level.
- Fields or forms that include a condition
  Examples include JavaScript conditions that hide or disable fields or forms based on the request status.
- Complex forms with custom JavaScript activated during the approval process

When a form contains an element or attribute that does not apply to mobile devices, a warning message appears to the request manager. The message explains this condition and advises the request manager to view and act on the request using the web browser of a tablet, laptop, or desktop. However, the request manager can still approve or reject the request using a mobile device. Therefore, as a best practice, verify that mobile-enabled services contain *no* unsupported elements or attributes.

Step 4 - Test the Services and Forms

Test the services and forms to verify that they function correctly on mobile devices.

Follow these steps:

1. From the iTunes and Google Play Store websites, download and install the mobile application on the following devices. The mobile app is CA Service Management.

   - iPhone and iPad running iOS 6.1 or higher
   - Mobile devices running Android operating system 4.0 or higher

2. Verify that your mobile services and forms appear and function correctly on these devices. For example, verify that catalog users can browse the catalog and can submit requests. Similarly, verify that request managers can view, approve, and reject their requests pending approval.

3. Verify that you can access and update services from the mobile application on iPhones and Android phones.

(Optional) Enforce Approvals Compatibility After Upgrade

To access the *My Tasks* capability with the latest features and have a consistent user experience, set the NX_MOBILE_WFM_FORCE_CLIENTVERSION_UPGRADE to Yes.

When this option is set, users attempting to log in to the previous version of this capability are rejected. The users are instructed to upgrade this capability.

Follow these steps:

1. Log in to the CA Service Desk Manager server and open the NX.env file.
2. Add the following variable in this file:

   ```
   NX_MOBILE_WFM_FORCE_CLIENTVERSION_UPGRADE
   ```

3. Set the variable value to Yes.
4. Save the file.
5. Restart the CA Service Desk Manager server.

(Optional) Set Form Fields as Non-Mandatory

By default, all input fields in the *My Tasks* capability that are derived from the CA Process Automation workflow engine are mandatory. The system administrator can make these fields non-mandatory.

Follow these steps:

1. Log in to the CA Service Desk Manager server and open the NX.env file.
2. Add the following variable in this file:

   ```
   NX_MOBILE_WFM_ITPAM_ALL_FIELDS_ARE_REQUIRED
   ```

3. Set the variable value to No to make the fields non-mandatory.
4. Save the file.

The form fields have been set as non-mandatory.

Access the CA Service Management Mobile Application

As a user, you can install the CA Service Management Mobile Application as the *native mobile application* on your mobile device.

Follow these steps:

1. Access the Google Play (for Android) or App Store (for iOS).
2. Search for CA Service Management.
3. Install the CA Service Management application.
   The CA Service Management icon is displayed on your mobile phone after successful installation.
4. Provide the following information to CA Service Management mobile application users as per your deployment requirements based on whether you have a single CA Service Management product (either CA SDM or CA Service Catalog) or combination of these products installed at your end:

   a. **CA Service Management Integrated Environment**
   If you have installed both CA SDM and CA Service Catalog, use the Unified Self-Service (USS) URL to access the integrated product capabilities.

   > **Note:** Ensure that the data source URLs for CA Service Catalog, CA SDM REST Services, and Unified Self-Service are accessible from your mobile application.

   b. **CA Service Desk Manager Environment**
   If you have installed only CA SDM, use the CA SDM Rest Service URL *http (s)://<SDM_HostName>:<rest_port>* to access the product capabilities:

   > **Note:** Ensure that the CA SDM Rest Services URL is accessible from your mobile application.

   c. **CA Service Catalog Environment**
   If you have installed only CA Service Catalog, use the Service Catalog Web service URL to access the product capabilities.

   You have successfully deployed and are able to access from your mobile application the appropriate product capabilities.

Configure the Mobile Attributes for CA SDM Tickets

CA SDM Administrators can configure new mobile attributes on the CA SDM Server. End users can view these attributes in the mobile application UI while editing or creating a ticket. Administrators can add any mandatory or custom attributes on the CA SDM Web UI while creating a ticket and make these attributes available to mobile application users. The end users can view these attribute fields on the mobile application ticket UI and fill in the required information.

Note: Mobile attributes for CA SDM tickets is supported on CA Service Management Mobile App 3.1.3 and onwards.

For example, in the CA SDM Web UI, if the Administrator has configured a category attribute as mandatory, this will restrict mobile users to create a ticket as the category field is not available out of the box on create/edit ticket. Hence, in order to be consistent with the CA SDM Web UI, the administrator can add the same attribute as part of mobile attribute in the CA SDM server.

To create mobile attributes for CA SDM tickets, complete the following steps:

Follow these steps:

1. Log in to CA SDM as an Administrator.
2. Navigate to **Administration**, **Service Desk**, **Mobile Attributes**.
3. Click **Create New** to create a mobile attribute.
4. Select an **Object Type** from the drop-down list.
5. Select an attribute for the object type from **Select an Attribute**.
   You can also search for the object type attribute from the Activity Association List page.
6. Save the form.
   CA SDM users can view this mobile attribute while editing or creating a ticket through their mobile applications.

Restricted Object Type Attributes for Mobile Applications

Currently, few CA SDM object type attributes are not available for CA SDM mobile application users. Restricted object type attributes are as follows:

- Requests/Incidents/Problems (see page 3174)
- Change Orders (see page 3174)
- Issues (see page 3175)
- Edit CA SDM Tickets (see page 3176)

Requests/Incidents/Problems

For CA SDM requests/incidents/problems, list of object type attributes that are not displayed in mobile application UI are as follows:

- ACTIVE
- ACTIVE PREVIOUS
- Assignee Previous
- Charge back ID
- close date
- group previous
- impact previous
- incident priority
- Last Target Closed Time
- Last Target Hold Time
- Last Target Resolved Time
- Last Target Start Time
- Open Date
- Priority Previous
- Request/Incident/Problem Area Previous
- Status Previous
- Resolve Date
- Severity Previous
- Tenant
- Type
- Urgency Previous

Change Orders

For CA SDM Change Orders, list of object type attributes that are not displayed in the mobile application UI:

- ACTIVE
- ACTIVE PREVIOUS
- Assignee Previous
- Group Previous
- Impact Previous
- Last Target Closed Time
- Last Target Hold Time
- Last Target Resolved Tim
- Last Target Start Time
- Priority Previous
- Status Previous
- OPENDATE
- Resolve Date
- Tenant

Issues

For CA SDM Issues, list of object type attributes that are not displayed in the mobile application UI are as follows:

- ACTIVE
- ACTIVE PREVIOUS
- Assignee Previous
- Group Previous
- Last Target Closed Time
- Last Target Hold Time
- Last Target Resolved Tim
- Last Target Start Time
- Priority Previous
- Status Previous

- opendate
- Resolve Date
- Tenant

Edit CA SDM Tickets

While editing CA SDM tickets, list of mobile attributes that are not displayed since the user has control on these attributes from the action menu available on the CA SDM ticket page:

- assignee
- group
- priority
- status

Call Service Desk from your Mobile Device

CA SDM mobile application users can use the the Call Service Desk feature to contact the CA Service Management service desk or help desk. CA SDM Administrators can configure a phone number to contact the service desk using the CA SDM Options Manager. By default, the Call Service Desk option is kept in an enabled state. Navigate to **Administration**, **Options**, **Call Service Desk** to enable or disable this feature.

If your CA SDM setup is tenanted, Call Service Desk uses the phone number specified on the **Telephone Number** or **Alternate Phone Number** fields for a tenant. However, if these fields are empty and not having any phone numbers, the default phone number set by the Administrator is used by the Call Service Desk feature.

To enable or disable this feature and configure the phone number, the following Call Service Desk options are added to the CA SDM Options Manager:

- call_service_desk_default_phone_number
- call_service_desk_mobile_enable
- call_service_desk_tenant_phone_number_field

Note: Only CA SDM administrators can configure these options.

For more information on how you can configure these options, see the Call Service Desk Options for CA SDM Options Manager (see page 1303).

CA Service Management Mobile Application-Server Side Patch Information

CA Service Management Mobile Application-required server side patch release information is as follows:

Note: Visit CA Support to download the CA Service Management Solution and Patches as required by you.

CA Service Management Mobile Application Features	CA Service Desk Manager Release 12.7	CA Service Desk Manager Release 12.9	CA Service Desk Manager Release 14.1	CA Service Catalog 12.9	CA Service Catalog 14.1
Multi-Tenancy Support for CA SDM	▪ Windows: RO70531 ▪ Linux: RO70536 ▪ Solaris: RO71008 ▪ AIX: RO70614	▪ Windows: RO70654 ▪ Linux: RO70655 ▪ Solaris: RO70656 ▪ AIX: RO70657	Not Applicable	Not Applicable	Not Applicable
Custom Query Support for CA SDM	Contact CA Customer Support for details.	▪ Windows: RO71086	Not Applicable	Not Applicable	Not Applicable

		▪ Linux: RO71087 ▪ Solaris: RO71088 ▪ AIX: RO71089			
Mobile Attributes Support for CA SDM	Contact CA Customer Support for details.	▪ Windows: RO77338 ▪ Linux: RO77339 ▪ Solaris: RO77340 ▪ AIX: RO77341	Not Applicable	Not Applicable	Not Applicable
Call Service Desk Functionality	Not Supported	▪ Windows: RO	CA Service Management 14.1.01	Not Applicable	Not Applicable

				82288 Cumulative Patch ▪ Linux: RO82289 ▪ Solaris: RO82290 ▪ AIX: RO82291	
Create Ticket On Behalf of using Affected End User field	Not Applicable	Not Applicable	Not Applicable	CA Service Catalog Content Packs (http://www.ca.com/us/support/ca-support-online/product-content/recommended-reading/product-related-technical-information/ca-service-catalog-content-packs.aspx)	CA Service Catalog Content Packs (http://www.ca.com/us/support/ca-support-online/product-content/recommended-reading/product-related-technical-information/ca-service-catalog-content-packs.aspx)

Enable or Disable Community on Mobile Devices

As a USS administrator, you can enable or disable the Community on the mobile devices.

Follow these steps:

1. Open the *US4SM\OSOP\tomcat-7.0.40\webapps\itsm\ ITSM_Configuration.json* file in edit mode.

2. Add the *disable_uss_community* property at the end of the existing properties and define either of the values:

    a. *false*, to enable Community.

    b. *true*, to disable Community.

```
{ "id": "osop",
"url": "*",
"disable_uss_community":"true"
}
```

Note: By default, Community is enabled.

3. Save the file.

Reporting

This section contains the following articles:

Reporting Using CA Service Desk Manager

Contents

CA SDM provides a variety of built-in reporting capabilities and options including the ability to do the following:

- Print forms for assets and individual change orders, issues, incidents, problems, and more.
- Generate Summary and Detail Reports (see page 3230) for lists of change orders, issues, incidents, problems, requests, configuration items.
- Generate Analysis Reports (see page 3230).

You generate reports based on the table and views (see page 2617)in your CA SDM database.

Report Methods Setup

Report methods let you specify where report results are to be sent when you select a report. Examples are the summary and detail reports available on the Reports menu and the reports available from the Analysis menu. Several predefined report methods are provided, and you can modify them.

Report Formatting

Using the dataent.fmt file found in $NX_ROOT/fig/cfg (UNIX) or installation_directory\fig\cfg (Windows) you can customize various data formats on the reports you print. You can view and modify this file using any text editor (Windows users should use WordPad to edit the file).

The following lines in the file control some of the date and time formats:

```
default_date = "long_date"
short_date = "M/D/YY// Enter a date as MM/DD/YY"
long_date = "MM/DD/YYYY// Enter a date as MM/DD/YY"
default_tod = "hour_12"
hour_12 = "h:mm:ss a(am,pm)// Enter a time of day as hh:mm:ss am/pm"
hour_24 = "HH:mm:ss// Enter a time of day as 00:00:00 - 23:59:59"
hms_12 = "h:mm:ss a(am,pm)// Enter a time of day as hh:mm:ss am/pm"
hms_24 = "HH:mm:ss// Enter a time of day as 00:00:00 - 23:59:59"
default_date_time = "date_time12"
date_time12 = "M/DD/YYYY h:mm:ss a(am,pm)// Enter a date and time as MM/DD/YY hh:mm:
ss am/pm"
date_time24 = "M/DD/YYYY HH:mm:ss// Enter a date and time as MM/DD/YY 00:00:00-23:59:
59"
```

The following code is an example of how you can change these lines to support European dates and times:

```
default_date = "long_date"
short_date = "D/M/YY// Enter a date as DD/MM/YY"
long_date = "DD/MM/YYYY// Enter a date as DD/MM/YYYY"
default_tod = "hour_24"
hour_12 = "h:mm:ss a(am,pm)// Enter a time of day as hh:mm:ss am/pm"
hour_24 = "HH:mm:ss// Enter a time of day as 00:00:00 - 23:59:59"
hms_12 = "h:mm:ss a(am,pm)// Enter a time of day as hh:mm:ss am/pm"
hms_24 = "HH:mm:ss// Enter a time of day as 00:00:00 - 23:59:59"
default_date_time = "date_time24"
date_time12 = "M/DD/YYYY h:mm:ss a(am,pm)// Enter a date and time as MM/DD/YY hh:mm:
ss am/pm"
date_time24 = "M/DD/YYYY HH:mm:ss// Enter a date and time as MM/DD/YY 00:00:00-23:59:
59"
```

Note: If you are using pdm_extract to export data from the CA SDM database to another system, and want to extract data to use the date format specified in the dataent.fmt file, use the -d flag when you invoke pdm_extract.

Data Analysis Setup

An interactive viewer provides an extensive set of tools for adjusting how the report data is viewed. You can drill to various levels of detail, such as from the group, to the assignee, or to the actual requests.

The interactive viewers lets you do the following:

- Change the appearance of the report by presenting the data in a different "block" format, such as a pie chart. For example, by right-clicking in the report and selecting "Turn table to," report presentation features appear.

- Perform different tasks, such as sorting, creating report breaks, calculating, filtering, and ranking the report.
- Share information with other users and groups.

Publish and Distribute Reports

Business Intelligence Launch Pad users can save report data in Excel, PDF or CSV format, and then distribute it to a file location, an inbox, email address, or FTP site.

When a report is approved for use within CA SDM, it is moved in to the public section making it available to authorized users. Security can be assigned to folders and documents to specify whether they can be accessed globally, by specific roles or by individuals. Security is administered in the BusinessObjects Central Management Console.

CA Business Intelligence Reports

CA Business Intelligence is a web-based component that packages Business Objects technology, integrated with CA SDM and a variety of common data sources, such as SQL Server, Oracle, and Open Database Connectivity (ODBC).

CA Business Intelligence uses BusinessObjects Enterprise as the default reporting system. Predefined reports are provided for CA SDM, Knowledge Management, and Support Automation.

With CA Business Intelligence reporting, users can do the following:

- Customize existing reports
- Drill down on Business Objects report data to show the data beneath charts and summarized groups
- Export instances of reports to different output formats
- Build ad hoc reports
- Publish new reports and distribute them to authorized users
- Schedule reports to run at specified times
- Use dashboard reporting to monitor daily operations for all CA SDM ticket types.

Access to Reporting is restricted through CA SDM Data Partitions Security.

Reporting Scenarios

CA Business Intelligence integrated with BusinessObjects Enterprise supports the following reporting scenarios:

- **Role-based reporting** -- From the CA SDM Reports tab, authorized users can view reports defined for their role, then click the Business Intelligence Launch Pad button to manage their personal reports in Business Intelligence Launch Pad. CA SDM uses the Business Intelligence Launch Pad interface to collect, organize, and present information in report formats. In Business Intelligence Launch Pad, predefined reports are grouped in public folders.

- **Web-based reporting** -- Web-based reports are predefined reports in CA SDM, Knowledge Management, CMDB, and Support Automation. They are developed with either Web Intelligence or Crystal Reports. The reports are accessed in Business Intelligence Launch Pad and can be used as models for defining site-specific reports.

- **Ad hoc reporting** -- Ad hoc reports are created and administered from Business Intelligence Launch Pad using a Web Intelligence plugin-based interface. You can store and manage reports in a personal workspace (My Folders). Ad hoc reporting is intended for users who want to create basic reports easily without writing queries.

- **Dashboard reporting** -- Dashboard reporting lets you monitor daily operations for all CA SDM ticket types (request/incident/problem, change order, or issue) in Business Intelligence Launch Pad. Each report contains analytics about the top performers working on active tickets, so you can monitor their progress. You can work with individual predefined dashboard reports or use the corporate dashboard to view all CA SDM daily operations in a single view.

- **Feature and Sample Reports** -- Feature and Sample reports that appear in the public section in Business Intelligence Launch Pad are provided by BusinessObjects Enterprise to illustrate the process of creating new reports in Web Intelligence. For more information, see *BusinessObjects* documentation.

Role-Based Reports

Contents

CA SDM presents role-based reports in two reporting frames on the Reports Tab. Each frame provides graphical views that let users drill down on report data to show the data beneath charts and summarized groups. You can manage role-based reports and display new BusinessObjects reports on the Reports tab. You can drill down

The Reports List page contains details of reports that are available for use. You click the Reports List icon that appears in the selected frame to display this page.

Define Role-Based Reports for the Role

You can manage the report web forms that display on the Reports List page when a user assigned to this role is logged into the system.

Follow these steps:

1. From the Administration tab, navigate to Security and Role Management, Role Management, Role List.
   The Role List page appears. The following default roles are available for Reporting:

   - Change Manager
   - Customer Service Manager
   - Knowledge Manager
   - Knowledge Analyst
   - Service Desk Manager
   - Incident Manager
   - Problem Manager

2. Select *one* of the Reporting roles from the list.
   The Role Detail Form page appears. This page contains the following tabs:

   - **Authorization**
     Allows you to define the authorization level assigned to the role.
   - **Function Access**
     Defines role access to each CA SDM functional area.
   - **Web Interface**
     Customizes the web interface for the role by defining the web pages and online help content the users can access.
   - **Knowledge Management**
     Specifies the Knowledge Management privileges for the role
   - **KT Document Visibility**
     Specifies which document statuses the role is allowed to view (for example, draft, retired, and published).
   - **Tabs**
     Defines the tabs that appear when a user assigned to this role is logged in to CA SDM.
   - **Report Web Forms**
     Defines the report web forms that are available to this role.

- **Go Resources**
  Specifies which record types appear in the "Go" drop-down list for the role. On the Role Detail page, select the Report Web Forms tab.

3. Click the Report Web Forms tab.
   The Reports Web Form List page appears. This page contains details of reports available for use.

4. Click Update Web Forms.

5. Enter the search criteria to display the web forms and click Search.

6. Select the web forms you want to display for this role. You can select multiple items.

7. When you have selected all the forms you want, click Select Button.

8. Click OK.
   The Role Detail page appears, with the selected web forms listed on the Report Web Forms tab.

Display New Reports on the Reports Tab

When a report is approved for use within CA SDM, it is moved in to the public section in Business Intelligence Launch Pad making it available to authorized users. To add the report to CA SDM, the administrator must perform some additional steps.

You can display new reports created in CA Business Intelligence on the CA SDM Reports tab. Use the following tools to accomplish this task:

- Web Screen Painter
- Role Management

Before you begin, do the following:

- Install and configure CA Business Intelligence so it works with CA SDM.
- Established user permissions, roles, and authentication (see page 3205) options for your reporting environment.

Step 1 - Create Two Web Form Records to Call the New Reports

By default, the Reports tab contains two reporting frames that let authorized users display new reports. In this step, you will create two web form records and define the URLs that point to the new reports.

Follow these steps:

1. From the Administration tab, navigate to Security and Role Management, Role Management, Web Forms.

2. Click Create New and click Save.

3. Fill in the following fields:

   - **Web Form Name**
     Specify a name that identifies the web form. This is a required field.
     Example: Asset List report

   - **Record Status**
     Specify active.

   - **Code**
     Specify a unique code value that identifies the web form to the system. After the code is defined, it cannot be changed.
     Example: asset_list

     > **Note**: Make a note of the value you enter in the Code field.

   - **Type**
     Select Report.

   - **Description**
     (Optional) Enter a brief description of the web form.

   - **Resource**
     Specify the URL that calls the new report.

     > **Example**: Open the Asset List web form from the Web Form list in Role Management and specify the URL that appears in this form.

     ```
     $BOServerURL?sPath=[Home],[Public+Folders],[CA+Reports],[CA+Service+Management],[CA+Service+Desk],[Asset]
     &sDocName=Asset+List&sViewer=htmlBOServerURL?sPath=[Home],[Public+Folders],[CA+Reports],[CA+Service+Desk],
     [Asset]&sDocName=Asset+List&sViewer=html
     ```

4. Repeat steps 1-3 to create a second web form record that will call the second report URL. Make a note of the value entered in the Code field.

Step 2 - Create a Mutliframe Page and Assign the New Reports

In Web Screen Painter, create a multiframe web page with two vertical frames called a Frameset. Then, assign the web form records created in step 1 to this Frameset.

> **Note**: You can create this page with any number of frames. Be aware that adding additional frames will limit visibility on the Reports tab.

Follow these steps:

1. In Web Screen Painter, select File, New.
2. Fill in the interface and form group fields as appropriate.
3. Select multiframe.template from the File Name list.
4. Click New.
5. Select Controls, Insert Frameset.
6. Do not change the default settings and click OK.
7. Right-click the left vertical frame and select Properties from the short-cut menu.
   The Properties - Frameset dialog box appears.
8. Select the blank field next to the web_form_name attribute, then click the (...) button.
   The Enter Web Form Name dialog box appears.
9. Specify the code value of the first report.
   Example: asset_list
10. After the report web form name is found, click Validate.
11. Right-click the right vertical frame, specify the code value of the second report, then validate the report.
12. Save the multiframe.htmpl page. Make a note of this file name.
    Example: report_mframe.htmpl
13. Select File, Publish.
    Publishing makes the form available to all CA SDM users. For the Analyst role, the file is available in the following location: Program Files/CA/Service Desk/Site/mods/www/htmpl /web/analyst/report_mframe.htmpl.

Note: When searching for multiframe web forms in CA SDM, navigate to Security and Role Management, Role Management, Web Forms on the Administration tab. The Code column specifies the web_form_name on the Properties tab for a multiframe form in Web Screen Painter.

Step 3 - Create a Start Page for the Reports Tab

In Role Management, create a start page to call the multiframe web page created in Step 2.

Follow these steps:

1. From the Administration tab, navigate to Security and Role Management, Role Management, Web Forms.
2. Click Create New.

3. Complete the following fields and click Save:

   - **Web Form Name**
     Specifies a name that identifies the web form. This field is required.
     Example: start page

   - **Record Status**
     Specifies active or inactive.

   - **Code**
     Specifies a unique code value that identifies the web form to the system. After the code is defined, it cannot be changed.
     Example: start_page

   - **Type**
     Specifies HTMPL.

   - **Description**
     (Optional) Specifies a brief description of the web form.

   - **Resource**
     Specifies the URL that calls the new report.
     Example: Select the Administrator Reports Multiframe record on the Web Form List page. Specify the URL that appears in this form. At the end of this path, specify the new multiframe page (report_mframe.htmpl).

     ```
     $cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMPL=report_mframe.htmpl
     ```

Step 4 - Create a Reports Tab Record and Assign the Start Page

In Role Management, create a new Reports tab and specify the start page created in step 3.

Follow these steps:

1. Select Security and Role Management, Role Management, Tabs on the Administration tab.

2. Click Create New.

3. Complete the following fields and click Save:

   - **Tab Name**
     Specify the name that identifies the tab within the administrative interface. For example, the tab name appears on the Tab List page.
     Example: Reports Tab

   - **Code**
     Specify the code that identifies this tab to the system. Once the code is defined, it cannot be changed.
     Example: reports_tab

   - **Record Status**
     Specify active.

- **Display Name**
  Specify the name that appears on the tab's graphical presentation in the user interface.
  Example: Reports Tab

- **Starting Page**
  Specify the initial web form that appears in the main window when a user selects this tab.
  Example: start page

The form appears in the Web Form List page.

Step 5 - Assign the Tab Record to a Role Record

In Role Management, assign the Reports tab to the desired role listed on the Role Detail page. When a user assigned to this role logs in to the system, they will see the new Reports tab in the web interface.

Follow these steps:

1. Select Security and Role Management, Role Management, Role List on the Administration tab.

2. Select the desired role from the Role list.

3. On the bottom of this page, select Tabs, then Update Tabs.
   The new tab appears on the Tab List.

Step 6 - Create a Start Page for the Business Intelligence Launch Pad Button

You have the option of including the Business Intelligence Launch Pad button that opens Business Intelligence Launch Pad in a new window on the Reports tab. This option is controlled through the Starting Page option that appears on the Reports tab record.

Follow these steps:

1. From the Administration tab, navigate to Security and Role Management, Role Management, Web Forms.

2. Click Create New.

3. Complete the following fields and click Save:

   - **Web Form Name**
     (Required) Specifies a name that identifies the web form.
     Example: Business Intelligence Launch Pad page

   - **Record Status**
     Specifies active or inactive.

   - **Code**
     Specify a code value that identifies the web form to the system.

   - **Type**
     Specifies HTMPL.

- **Description**
  (Optional) Describes the web form.

- **Resource**
  Specifies the URL that calls the reporting frames.
  Example: Select the Administrator Business Intelligence Launch Pad record on the Web Form List page. Specify the URL that appears in this form. At the end of this path, specify the new Reports tab start page (start_page).

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMPL=show_report_frames.htmpl+KEEP.report_form=start_page
```

Step 7 - Assign the Business Intelligence Launch Pad Button Start Page to the Reports Tab Record

In Role Management, assign the Business Intelligence Launch Pad button start page created in step 6 to the Reports tab record.

Follow these steps:

1. Select the new Reports Tab web form record from the Tab List page in Role Management.
2. Select Edit.
3. Specify the new Business Intelligence Launch Pad button start page in the Starting Page field.
4. Click Save.
   When a user opens the Reports tab, the Business Intelligence Launch Pad button appears in the top right corner of the form.

Work with Report Data

Reports that you access from the Reports List are developed with either BusinessObjects Web Intelligence or Crystal Reports.

Depending on the type of report that is deployed and the functions that are enabled by your administrator, you can perform a number of different activities, such as drilling and printing reports.

Note: When you work with reports in Business Intelligence Launch Pad, you can use additional features that are unique to working with Crystal Reports and Web Intelligence.

Ad Hoc Reports

Contents

Ad hoc reports are developed in Business Intelligence Launch Pad using Web Intelligence. You can create ad hoc reports. For more information about ad hoc reporting, see the BusinessObjects Enterprise documentation. To access the documentation, click the help icon in Business Intelligence Launch Pad.

Web Intelligence Interface

In Business Intelligence Launch Pad, Web Intelligence provides a custom reporting tool and it is intended for users who want to create basic reports easily without writing queries. Web Intelligence uses predefined report models and templates that manage data connections, querying, and data relationships, so you need only drag and drop data fields onto a template to create tabular or matrix reports. You can use all Business Intelligence Launch Pad features that are described in the *Business Intelligence Launch Pad User documentation*. A Web Intelligence document references a BusinessObjects object named a universe to create reports. You build new reports on BusinessObjects universes. CA Business Intelligence provides the CA SDM universe with the product.

How Ad Hoc Reporting Works

Ad hoc reporting works as follows:

1. You start the ad hoc report by first selecting the CA SDM universe in Business Intelligence Launch Pad.

2. The universe maps to the CA SDM database containing corporate business information. When you connect to a universe, Web Intelligence automatically launches the document editor selected on the Web Intelligence Document Preferences page in Business Intelligence Launch Pad.

> **Note:** For information on setting preferences, see the *Business Intelligence Launch Pad User's documentation*.

3. Using the universe, you build queries to retrieve data to use in a report from objects grouped in folders called classes. Each class can also contain one or more subclasses. Subclasses contain objects that are a further subcategory of the objects in the upper level of the class. Classes and Objects are presented in a tree structure (hierarchy) in the Data tab.

   Note: For instructions on how to build queries for Web Intelligence documents, see the BusinessObjects Enterprise documentation.

4. After you have built your query, by adding the required objects to the Result Objects pane, and defined query filter properties, you are ready to run the query. When you run a query, the universe asks the database to retrieve the data that corresponds to the demands of each of the objects in the query. You run a query by clicking Run Query on the toolbar.

   Important! When selecting objects for your query, always choose objects, measures and filters from only one universe base class and its subclasses. If you include objects, measures and filters from multiple universe base classes in a query, you might receive unexpected results and poor performance.

Before you Begin

This section provides high-level information to help you define preferences and other options. It also provides some considerations for creating new reports.

Define Web Intelligence Options

Ensure that you define Web Intelligence Document Preferences to suit your query and reporting needs before you begin creating new reports.

Follow these steps:

1. Click the Preferences button on the Business Intelligence Launch Pad toolbar.

2. Click the Web Intelligence Document Preferences tab.
   The Web Intelligence Document Preferences page appears.

3. In the "Select a report panel" area, select the report panel that you want to use when you create or edit Web Intelligence documents.

4. Select other options as appropriate.

5. Click OK.
   Business Intelligence Launch Pad displays the page you were on previously. For more information about preferences and options, see the *Business Intelligence Launch Pad User's documentation*.

Define Drill Options

You set your drill options in Business Intelligence Launch Pad. When you change your drill options, the changes are implemented the next time you start Drill mode.

Follow these steps:

1. On the Business Intelligence Launch Pad toolbar, click Preferences.
   Click the Web Intelligence Document Preferences tab.

2. The Web Intelligence Document Preferences page appears.

3. In the Select a view format section, select HTML or Interactive.

Define Query Properties

You can set properties for the query that can optimize the time taken for the query to run or the amount of data returned. Properties are grouped together in sections on the Query Properties page in the Result Objects pane.

To limit the number of rows returned to reports

1. Click Query Properties in the Query toolbar.
   The Query properties window appears.

2. Type the number of maximum rows you want to be retrieved.

To limit the run time for queries

1. Click Query Properties in the Query toolbar.
   The Query properties window appears.

2. Type a Maximum retrieval time in seconds.

Considerations for Creating a New Report

When creating a new report, the following criteria should be considered:

- The fields selected from Result Objects are the selection columns for the SQL query and reports.
- Do not mix fields of one class with another, because the reports may not work properly if you do.
- Restrict the number of columns required for the report. Choosing too many columns may degrade the report performance.

Create a Basic Report

You can create a new report for CA SDM to add new fields, queries and query filters other than the ones in the existing reports.

This section provides introductory information to help you create a new report using BusinessObjects.

Select the CA SDM Universe

You start the report by first selecting the CA SDM universe in Business Intelligence Launch Pad. The universe maps to the CA SDM database containing corporate business information. When you connect to a universe, Web Intelligence automatically launches the document editor selected on the Web Intelligence Document Preferences page in Business Intelligence Launch Pad.

Follow these steps:

1. Click New, Web Intelligence Document from the menu bar.
   The New Web Intelligence Document page appears.

2. Select the CA SDM universe in the Universe column.

   The Web Intelligence document appears along with the universe information in the left pane.

Define Data Retrieved by Queries

In the universe, objects are grouped into folders called classes. Each class can also contain one or more subclasses. Subclasses contain objects that are a further subcategory of the objects in the upper level of the class. Classes and Objects are presented in a tree structure (hierarchy) in the Data tab.

You can build one or more queries to use in your report as follows.

Follow these steps:

1. Drag and drop the objects from the Data tab (left pane) to the top right pane under Results Objects.
   The object appears in the Result Objects pane.

2. Drag and drop the fields to the bottom right panel under Query Filters.

3. (Optional) click Add Query to build a new query.

   Note: For instructions on how to use the report panel to build queries for Web Intelligence documents, see the *Building Queries Using the Web Intelligence HTML Query Panel* documentation.

Run Queries

After you have built your query, by adding the required objects to the Result Objects pane and defined query properties, you are ready to run the query. When you run a query, the universe asks the database to find the data that corresponds to the demands of each of the objects in the query. You run a query by clicking Run Queries on the toolbar.

View the SQL Generated by Queries

You can view the SQL generated by WebI for the query.

Click View SQL on the Query toolbar. The SQL Viewer window appears. In this window you can inspect the SQL behind the query that you have made.

Edit Queries In Existing Reports

You can edit the queries on which your report is based.

Follow these steps:

1. Open the document that you want to view.
   Click Document actions, and then select Edit.

2. The report appears and displays the queries that are defined for the document.

Save and Distribute Reports

You can save report data in Excel, PDF or CSV format, then distribute it to a file location, your Inbox, an email address or FTP site.

When a report is approved for use within CA SDM, it is moved to the Public section, thereby, making it available to authorized users. Security can be assigned to folders and documents to specify whether they can be accessed globally, by specific roles or by individuals. Contact your administrator for more information.

Note: For information on publishing and distributing reports, see BusinessObjects documentation.

Report Drill Analysis

Report drill analysis allows you to look deeper into the reasons behind results displayed. In Drill mode, you can:

- drill on tables
- drill on section cells
- drill on charts
- change how drilled results are filtered
- drill beyond report results
- save drilled results and ending Drill mode
- use query drill

To start analyzing reports using Drill, you need to switch to Drill mode. For more information, see BusinessObjects documentation.

Example of Ad Hoc Reports

You can work with Web Intelligence and query examples to create ad hoc reports using the default CA ServiceDesk. When you create a report, make sure that you save your report at regular intervals. If the Web Intelligence connection session times out, you will lose your report modifications.

Example - View All Open Priority 1 and 2 Requests for All Users

In this example, you specify prompt values that gather additional data before generating the report.

Follow these steps:

1. Click New, Web Intelligence Document from the menu bar.
   The New Web Intelligence Document page appears.

2. Select the CA ServiceDesk in the Universe column.
   The Web Intelligence document appears along with the universe information in the left pane.

   Note: To improve navigation, close the Attached Service Type folder in the left pane.

3. Locate and then expand the Request, Request Detail folders in the left pane. Use the scroll bar to locate folders.

4. Select each of the following objects, then drag and drop them from the left pane to the top right pane under Results Objects.

   - Summary
   - Priority Symbol
   - Customer Combo Name

5. Select the following objects, then drag and drop them to the bottom right panel under Query Filters. Close the Request Detail folder when you are finished.

   - Status Symbol
   - Priority Symbol

6. Expand the Request Filters folder, then drag and drop the Customer Combo Name with Userid filter to the bottom right panel under Query Filters.

7. In the Query Filters pane, click the In list arrow on the Status Symbol filter, and select the Equal to operator.

8. Select Value(s) from list from the Operand Type menu.
   The List of Values dialog box appears.

9. In the Status Symbol list, select Open, then click the green arrow.
   The value appears in the Value(s) Selected field.

10. Click OK.

11. In the Query Filters pane, click the In list dropdown on the Priority Symbol filter, and select the In List operator.

12. In the Priority Symbol list, multi-select 1 and 2, then click the green arrow.
    The values 1 and 2 appear in the Value(s) Selected field.

13. Click OK.

14. Click Run Query on the toolbar to generate the report.

> **Note**: Since the Customer Combo Name with Userid quick filter uses the Prompt function, the Prompts dialog box appears. This dialog allows you to gather additional data before the report is generated.

15. In the Prompts window, select the first option ALL, then click the green arrow button.
    All user names appear in the Select Customer list.

16. Click Run Query to generate the report.
    The report appears in a new window.

17. Double-click the report's title and type Priority 1 & 2 Open Requests for All Users in the text box. You can change the font size to 16 or other sizes.

18. To change other aspects of the report, click the Properties tab.

19. To sub-group the data by Customer Last Name, right-click any data cell in the Customer Last Name column, and select Set as Section.

20. Click Save and specify a location using the Save As option.

Example - View All Open Requests that Do Not Include a Status of Work In Progress

In this example, you specify the Count reporting function to return the total number of open requests.

Follow these steps:

1. Click New, Web Intelligence Document from the menu bar.
   The New Web Intelligence Document page appears.

2. Select the CA ServiceDesk in the Universe column.
   The Web Intelligence document appears along with the universe information in the left pane.

> **Note**: To improve navigation, close the Attached Service Type folder in the left pane.

3. Locate and then expand the Request, Request Detail folders in the left pane. (Use the scroll bar to navigate folders.)
4. Select each of the following objects, then drag and drop them from the left pane to the top right pane under Results Objects.
   - Status Symbol
   - Ref Num
   - Summary
5. Select the Status Symbol object, then drag and drop it to the bottom right panel under Query Filters. Close the Request Detail folder.
6. Expand the Request Filters folder, then drag and drop the Active filter to the bottom right panel under Query Filters.
7. In the Query Filters pane, click the In list arrow on the Status Symbol object, and select the Not Equal to operator.
8. Select Work in Progress from the Operand Type menu.
9. Click Edit Report on the main toolbar.
   The Report Viewer opens.
10. In the report, select the Ref Num column. This action enables the Insert Sum command on the Reporting toolbar.
11. Click the Insert Sum command, then select Count from the menu.
12. In the report, right-click the =[Status Symbol] cell, then select Set as Section from the context menu.
13. Click Refresh Data on the main toolbar to run the report.
14. Click Save.
    The report displays the total number (count) of requests that *do not* have a status of Work in Progress.

Example - View All Closed Requests in the Last 30 Days for Users Whose Last Name Begins with "C"

In this example, you specify prompt values for the Close Date and Customer Last Name that return all closed requests based on these values.

Follow these steps:

1. Click New, Web Intelligence Document from the menu bar.
   The New Web Intelligence Document page appears.

2. Select the CA ServiceDesk in the Universe column.
   The Web Intelligence document appears along with the universe information in the left pane.

   Note: To improve navigation, close the Attached Service Type folder in the left pane.

3. Locate and expand the Request, Request Detail folders in the left pane. Use the scroll bar to navigate folders.

4. Select each of the following objects, then drag and drop them from the left pane to the top right pane under Results Objects.

   - Ref Num
   - Close Date
   - Customer Last Name
   - Summary

5. Select each of the following objects, and drag them to the bottom right panel under Query Filters.

   - Status Symbol
   - Close Date
   - Customer Last Name

6. Click the In list arrow on the Status Symbol filter and select Value(s) from list from the Operand Type menu.
   The List of Values dialog box appears.

7. Select the following values in the Status Symbol list:

   - Closed
   - Closed-Unresolved
   - Close Requested
   - Problem-Closed
   - Problem-Fixed
   - Resolved

8. Click the green arrow.
   The values appear in the Value(s) Selected field.

9. Click OK.

10. In the Query Filters pane, click the In list arrow on the Close Date object and select the Between operator.

11. Click the In list arrow and select Prompt from the first and second Operand Type menus.

12. Click the In list arrow on the Customer Last Name object and select the Matches pattern operator.

13. Click the In list arrow and select Prompt from the Operand Type menu.

14. Click the Prompt Properties icon that appears next to the In list arrow.
    The Prompt dialog box appears.

15. In the Prompt text field, enter a pattern for Customer Last Name.

16. Click OK.

17. Click Run Query on the toolbar to generate the report.

    Note: Since the Close Date and Customer Last Name objects use the Prompt function, the Prompts dialog box appears. This dialog allows you to gather additional data before the report is generated.

18. In the Prompts window, select or type the prompt values for each prompt as follows:

    - Enter Close Date (Start): Specify a date that is 30 days earlier than today's date.
    - Enter Close Date (End): Specify today's date.
    - Enter a pattern for Customer Last Name: Specify C%.

19. Click Run Query to generate the report.
    The report appears in a new window.

20. Double-click the report's title and type View All Closed Requests in Last 30 Days for Users Whose Last Name Begins with "C" in the text box. You can change the font size to 16 or other sizes.

21. To change other aspects of the report, click the Properties tab.

22. Click Save and specify a location using the Save As option.

Dashboard Reports

You can use dashboard reporting to monitor daily operations for all CA SDM ticket types (request /incident/problem, change order, or issue), Knowledge Management, Support Automation, and CMDB in Business Intelligence Launch Pad. Each report contains analytics about the top performers working on active tickets, so you can monitor their progress.

With dashboard reporting, you can:

- View summary and detail information about active tickets by priority, analyst, category, or group.
- Find out how many tickets were resolved within a particular time frame and much more.
- Edit, print, track, and save reports in other formats, such as .xls and .pdf.

You can work with individual predefined dashboard reports or use the corporate dashboard to view all CA SDM daily operations in a single view. The corporate dashboard shares vital information about daily operations for all ticket types (request/incident/problem, change order, or request) by priority, analyst, category, or group.

Note: When you work with dashboard reporting, you can use the Business Intelligence Launch Pad features that are described in the Working with Dashboard and Analytics section of the *Business Intelligence Launch Pad User's documentation*. To access the documentation, click the help icon in Business Intelligence Launch Pad.

Web Based Reports

Contents

CA Business Intelligence installs a set of web-based, predefined reports for CA SDM and Knowledge Management. They are developed with either BusinessObjects Enterprise Web Intelligence or Crystal Reports. The reports can be used as models for defining site-specific reports.

These reports are contained in folders that are automatically deployed to the CA Business Intelligence reporting server after installation.

Security can be assigned to folders and documents to specify whether they can be accessed globally, by specific roles, or by individuals.

Business Intelligence Launch Pad includes documentation that describes how to use Business Intelligence Launch Pad. To access the documentation, click the help icon in Business Intelligence Launch Pad.

Business Intelligence Launch Pad Interface

From the CA SDM Reports Tab, analysts and managers can work with reports defined for their role or manage their personal reports by clicking the Business Intelligence Launch Pad button. From Business Intelligence Launch Pad, users can access Crystal Reports and Web Intelligence Documents, and other objects, and organize them to suit their preferences.

The features that are available in Business Intelligence Launch Pad vary by content type, but in general, the user can view information in their web browser, export it to other business applications (such as Microsoft Excel), and save it to a specified location.

Note: The folders and objects that users see in Business Intelligence Launch Pad are dependent on their group (role) assignment.

You can navigate the folders in the left-hand pane of the Business Intelligence Launch Pad window to view, schedule, modify, or run the report or to view the history and properties for a report. From the Start menu, select All Programs, CA Business Intelligence 4.1, Java Business Intelligence Launch Pad. In the left pane, navigate the folder structure-Public Folders/CA Reports/CA Service Management/CA ServiceDesk. Click the folder that corresponds to the type of report you want to view. Click the report name for the type of information you want to see.

Important! If you are using the Oracle database and want to generate All Change Impact Report, CIs Relationships Report, and Root Cause Analysis Report, then click Oracle (These Reports will work on Oracle Only) from the CMDB folder to access the reports. If you generate these reports from the SQL Server folder, the reports are not generated and an error message is displayed. Similarly, if you are using the SQL database and want to generate All Change Impact Report, CIs Relationships Report, and Root Cause Analysis Report, then click SQL Server (These Reports will work on SQL Server Only) from the CMDB folder to access the reports.

Business Intelligence Launch Pad Preferences

Users can set general preferences to specify that Business Intelligence Launch Pad should start with one of their personal dashboard pages designed with Web Intelligence's My Business Intelligence Launch Pad tool. They can also set their personal Web Intelligence and Crystal Reports viewing preferences.

Schedule Reports

Business Intelligence Launch Pad supports scheduling of reports. For ad hoc reporting, scheduled reports are stored in the My Folders section. If a report is set to "refresh on open" the system will access the database to obtain the latest information each time the end user views the report. Users can schedule reports to run at certain times.

Administrators can define calendars to reflect appropriate scheduling dates. For example, a user can select a calendar using the "When" option (for timing and frequency) that will display available business days and ignore non-working days.

Note: For more information on scheduling reports, see BusinessObjects documentation.

With scheduling, users can:

- Specify the timing and frequency of the schedule (now, hourly, daily, and weekly, for example).
- Specify the destination, such as an inbox, file location or email recipient.
- Indicate which inboxes the report should be sent to.
- Specify the output, such as Web Intelligence, Crystal Report, Microsoft Excel, and Adobe Acrobat.
- Specify caching options. By default, the document results are stored on the Output File Repository Server. Users can choose to have the system cache the report on the Web Intelligence Report Server by selecting a cache format and locale.
- Select a server group to process the request. If a defined event is selected, the object will run only when the additional condition or event occurs.

Note: If CA SDM data partitions are used to manage data restrictions in Business Intelligence Launch Pad's public folder section, scheduled reports contained in public folders must be defined for each user.

You can schedule a report to run at a specific time of the day, week, or month. You must have the appropriate authorization to perform scheduling. Right-click a report and select Schedule specify the appropriate settings and click Schedule.

Access Your Personal Folders or Inbox

You can access objects in your personal folders or inbox.

Follow these steps:

1. On the Navigation panel toolbar, click Show Folders.
   Business Intelligence Launch Pad folders are displayed in the Navigation panel. By default, My Folders and Public Folders are displayed.
2. Expand My Folders.
3. Click Favorites or Inbox.

Reporting Components

BusinessObjects Enterprise and its associated tools, coupled with BusinessObjects Crystal Reports 2013 are the backbone of the CA Business Intelligence architecture.

Although Crystal reports are delivered as the primary component of CA Business Intelligence, the report creation and maintenance tool, Crystal Reports 2013, is not delivered as part of CA Business Intelligence.

Note: Microsoft Access predefined reports are no longer developed or provided with CA SDM.

You can use the following components to administer, monitor, and configure the CA Business Intelligence reporting environment:

- **CA SDM Database/ Domsrvr / ODBC Driver --** Report data is stored in a SQL Server or Oracle CA SDM database. BusinessObjects reporting applications (Crystal Reports and Web Intelligence) access the database using an ODBC driver that connects directly with the CA SDM object engine (domsrvr). All CA SDM security, including data partition and tenancy restrictions, is automatically applied to reports, but not to your reporting environment. You can set up your reporting environment so it works with existing data partitions in CA SDM.

  Note: For information on how to establish data partitions security for your reporting environment, see How to Set Up Data Partitions Security for Reporting (see page 3205).

- **Central Management Server (CMS) --** The central repository that stores all objects used in every reporting process.

- **Central Management Console --** An administrative component that provides access to all BusinessObjects administration functions. Using the CMC, you can deploy reports and assign user access and folder permissions for Business Intelligence Launchpad. User permissions, roles, and authentication options must be established for your reporting environment using the CMC.

  Note: User permissions, roles, and authentication options must be established for your reporting environment before you use CA Business Intelligence. For more information on defining security, see Security and Authentication (see page 3205).

- **BusinessObjects Universe --** Describes the classes (tables) and objects (columns) which are used in reports. The CA SDM universe is installed and configured during the installation. At the completion of the installation, the universe connection is assigned to various groups and users in CA SDM.

- **Universe Design Tool --** A BusinessObjects component that lets you modify the CA SDM Universe, which is a metalayer between CA SDM schema, and BusinessObjects reporting tools. The Import /Export Wizard facilitates object population or extraction within the CMS.

- **Default Predefined Reports --** Predefined reports are web-based CA SDM and Knowledge Management reports developed with either Web Intelligence or Crystal Reports. The reports can be used as models for defining site-specific reports.

- **Business Intelligence Launchpad --** Business Intelligence Launchpad is a web interface that allows authorized CA SDM users to interact with web-based predefined reports by viewing, running, and scheduling report types including, but not limited to, Web Intelligence and Crystal Reports. Reports are contained in folders in the public section in Business Intelligence Launchpad.

- **Ad Hoc Reports --** Ad hoc reports let you create and administer reports using a Web Intelligence plugin-based interface. This tool is intended for users who want to create basic reports easily without writing queries.

  Note: For ad hoc reporting usage examples, see Ad Hoc Reports (see page 3190).

- **Dashboard Reports** -- Dashboard reports let you monitor daily operations for all CA SDM ticket types (request/incident/problem, change order, or issue) in Business Intelligence Launchpad. Each report contains analytics about the top performers working on active tickets, so you can monitor their progress.

- **CA SDM Reports Tab --** Authorized users can view their role-based reports on the CA SDM Reports tab, then click the Business Intelligence Launchpad button on this tab to manage their personal reports in Business Intelligence Launchpad.

  Note: For information on how to manage role-based reports and display new reports on the Reports tab, see Web-Based Reports (see page 3201).

Replicated Database for Offline Reporting

To manage potential performance issues that may affect the reporting components installed with CA SDM, you can create a replicated database for offline reporting purposes.

Note: For more information about creating a replicated database for offline reporting, see the sample documentation and scripts delivered in the NX_ROOT\samples\reporting directory.

Security and Authorization

This article contains the following topics:

The default security configuration for BusinessObjects Enterprise is performed through the CA Business Intelligence configuration. The configuration determines the security policies of folders, universes, universe connections and tools. It also provides methods for adding users and mapping them to groups, and setting some preference options.

Specifically, the CA Business Intelligence reporting configuration involves:

- Setting up security
- Deploying reports
- Deploying universes
- Configuring Web Intelligence settings

At the completion of installation, the universe connection is assigned to various groups and users in CA SDM.

The administrator can log on to the BusinessObjects CMC and modify the default settings at any time. Users are authorized access to Business Intelligence Launch Pad folders based on the CA Business Intelligence group to which they belong.

Groups and Users

The Groups listed in the following table will be added to the Central Management Server (CMS) during the CA Business Intelligence configuration. They relate to CA SDM roles with the same names. During the configuration phase, an optional check box was available to indicate whether sample users are added to the CMS. If it was selected, your default CMS configuration includes one sample user for each group. In the CMC, you can use these sample users as models when you establish user permissions and authentication options for your reporting environment.

Group Name	User Name
Change Manager	Change Manager User
Customer Service Manager	Customer Service Manager User
Knowledge Manager	Knowledge Manager User
Knowledge Analyst	Knowledge Analyst User
Service Desk Manager	Service Desk Manager User
Incident Manager	Incident Manager User
Problem Manager	Problem Manager User
Support Automation Admin	Support Automation Admin User
Support Automation Analyst	Support Automation Analyst User

CA SDM Data Partitions in Business Intelligence Launch Pad

Consider the following information about the relationships between CA SDM data partitions and Business Intelligence Launch Pad:

- The analyst connects to CA Business Intelligence through the Reports tab in CA SDM or in Business Intelligence Launch Pad with the access type of a default reporting role.
- The CA SDM login credentials *must* match the Business Intelligence Launch Pad credentials. The administrator sets an authentication method such as secLDAP or secEnterprise. CA SDM logs in to CA Business Intelligence, which then logs in to CA SDM through the ODBC.
- The CA Business Intelligence analyst login associates with the CA SDM login. CA Business Intelligence uses this CA SDM login and the reporting role associated with the access type of the login. If the analyst does not have an associated CA SDM login, CA Business Intelligence uses the system default. The system default is defined in the ODBC parameters in the Universe Designer and the reporting role of the access type.
- To restrict a user from viewing a report, the administrator can disable access to the report or the folder that contains it.

Universe and Universe Connections

The default configuration also includes the security policy for accessing the CA SDM universe and universe connections. To allow full access, all of the default groups are defined to have Full Control access.

Group Name	Access Level
Change Manager	Full Control
Customer Service Manager	Full Control
Knowledge Analyst	Full Control
Knowledge Manager	Full Control
Service Desk Manager	Full Control
Incident Manager	Full Control
Problem Manager	Full Control
Support Automation Admin	Full Control
Support Automation Analyst	Full Control

Report Folders

The default configuration comes with a set of folders containing predefined reports for CA SDM and Knowledge Management. Each CA SDM group is configured to have access to a subset of these folders.

Folder Name	Group Name	Access Level
Aggregate	Change Manager	View
	Customer Service Manager	View
	Knowledge Manager	No Access
	Knowledge Analyst	No Access
	Service Desk Manager	Full Control
	Incident Manager	View
	Problem Manager	View

Folder Name	Group Name	Access Level
Asset	Change Manager	View on Demand
	Customer Service Manager	View
	Knowledge Manager	No Access
	Knowledge Analyst	No Access
	Service Desk Manager	Full Control
	Incident Manager	View
	Problem Manager	View
Change Order (includes all sub-folders)	Change Manager	Full Control
	Customer Service Manager	No Access
	Knowledge Manager	No Access
	Knowledge Analyst	No Access
	Service Desk Manager	View
	Incident Manager	View
	Problem Manager	View
Issue (includes all sub-folders)	Change Manager	No Access
	Customer Service Manager	Full Control
	Knowledge Manager	No Access
	Knowledge Analyst	No Access
	Service Desk Manager	No Access
	Incident Manager	No Access
	Problem Manager	No Access
Request (includes all sub-folders)	Change Manager	No Access
	Customer Service Manager	No Access
	Knowledge Manager	No Access
	Knowledge Analyst	No Access
	Service Desk Manager	Full Control
	Incident Manager	View
	Problem Manager	No Access
Knowledge Management	Change Manager	No Access
	Customer Service Manager	View
	Knowledge Manager	Full Control
	Knowledge Analyst	View
	Service Desk Manager	Schedule
	Incident Manager	View
	Problem Manager	View
Survey	Change Manager	No Access
	Customer Service Manager	No Access
	Knowledge Manager	View
	Knowledge Analyst	No Access
	Service Desk Manager	Full Control
	Incident Manager	View
	Problem Manager	View
Incident and Problem Management	Change Manager	No Access
	Customer Service Manager	No Access
	Knowledge Manager	View
	Knowledge Analyst	No Access
	Service Desk Manager	Schedule
	Incident Manager	Full Control
	Problem Manager	Full Control

Access Levels

The default configuration includes the following access levels for groups and users:

- **No Access**
  Sets all permissions to Not Specified.

- **View**
  Allows the user to see the folder, report or universe. If the report contains data, the user can open and interact with it. If the report does not contain data, the user cannot refresh the report. By default, the user can edit the report and save to a personal folder and refresh it there. You can explicitly prevent users from copying corporate documents to personal folders by setting an individual right that denies "Copy Objects to another folder".

- **Schedule**
  Allows a user to schedule a report but not refresh it in real time.

- **View On Demand**
  Allows a user to refresh a report in real time. When the report is a Web Intelligence document, the user also needs View On Demand access to the Universe and Universe connection to perform the refresh.

- **Full Control**
  Allows a user to create new reports within a folder, modify existing reports or delete items.

- **Advanced**
  When the preceding access levels do not meet your needs, we provide more granular access by choosing advanced.
  When a user or group's access level is set to Advanced, more granular control of rights is available than those assigned through the selection of View, Schedule, View On Demand or Full Control.

BusinessObjects folders use inherited security. You receive the same authority in lower level folders as that of the top folder level that was assigned to you or your group, unless overriding restrictions are applied at lower levels. Default authorizations are provided at the folder level and group level. Users will inherit the rights of their group for all objects in the folder and subordinate folders.

CA Business Intelligence is installed with two groups: Administrators and Everyone. The Everyone group is assigned an Access Level of Schedule which allows scheduling and viewing of all report objects.

Point an Existing CA Business Intelligence Server to a CA SDM Server

If you have an existing CA Business Intelligence server, you can point it to a CA SDM server as follows:

1. Create 32 bit DSN and 64 bit DSN on CA Business Intelligence Server (see page).
2. Configure the Universe (see page 3211).
3. Export the Universe (see page 3211).
4. Launch Business Intelligence Launch Pad to verify the connection.

Create 32 bit DSN and 64 bit DSN on CA Business Intelligence Server

Follow these steps:

1. Launch odbcad32.exe from the following locations:
   - (for 64bit DSN) C:\Windows\System64
   - (for 32bit DSN) C:\Windows\System32
2. Select the System DSN tab and click Add.
   The Create New Data Source page appears.
3. Select CA Service Desk Manager and click Finish.
   The DataDirect OpenAccess ODBC Setup page appears.
4. Specify casd_*servername* in the ODBC Name field.
5. Click Advanced.
   The Advanced page appears.
6. Click Add.
   The Open Access Database Setup page appears.
7. Complete the following fields:
   - **Name**. Specify casd_*servername*.
   - **IP Address**. Specify the *servername* or IP address.

     Note: Ping *servername* to determine its IP address to use the IP address instead of *servername*.
   - **Port**. Specify 19987.
   - **Type**. (Optional) Specify the database used on the server. This field is only used as reference information.
8. Click OK.
9. Select casd_*servername* from the Database drop-down list.
10. Click OK.
    The ODBC data source is created.

Configure the Universe

After you create the ODBC data source, you need to configure the universe by establishing a connection between CA SDM and CA Business Intelligence. CA Business Intelligence Release 4.1 Client tools are required to configure the universe.

Follow these steps:

1. Launch Universe Design Tool and login as administrator.
2. Click File, Import.
3. Browse and select your CA SDM universe and click OK.
4. Click File, Parameters.
5. Click Edit.
6. Specify the username and password of the CA SDM privileged user, such as ServiceDesk.
7. Select casd_*servername* from datasource name and click Next.
8. Click Test Connection to verify that the CA SDM universe communicates with CA Business Intelligence.
9. Click Next, Next, Finish.
   The universe is configured.

Export the Universe

A universe is available to Web Intelligence users only when you export the universe to the repository. Commonly, you import a universe, make changes, then export the updated universe. This method ensures that the CMS (repository) version is synchronized with the file version. If you create a linked universe, you export it to the repository.

When you save a universe, you update the version in the repository file system. However, saving does not update the CMS version. When you export a universe, the update of the version in the repository file system is synchronized with the update of the universe in the CMS. The universe is then available to users.

CA Business Intelligence Release 4.1 Client Tools is required to export the universe .

Follow these steps:

1. Select File, Export, then perform one of the following actions:
   - Select a universe folder from the folder drop-down list.
   - Click the Browse button and select a universe folder in the folder browser.

   You want to export the universe to this folder.

2. (Power Users only)If you want to lock the universe, double-click the universe name.
   A locked universe appears with a padlock symbol. To unlock a universe, double-click it again.

3. (Power Users only)Click a group in the "Groups" list, which is the user group that uses the exported universe.

4. Click a universe in the "Universes" list. The "Universes" list shows the names of the active.

5. If you want to export other universes that are not open:

   a. Click the Add Universe button.

   b. Use the browser to select the other universes.

   c. Click OK.

   The universe is exported to the repository and is also available in the Universe folder that you selected.

Set Up Data Partitions Security for Reporting

This article contains the following topics:

Access to CA Business Intelligence reporting is restricted through CA SDM Data Partitions Security. All CA SDM security, including data partition and tenancy restrictions, is automatically applied to reports.

Data partition security for your specific reporting environment is not applied during the configuration phase. You set up your reporting environment so it works with existing data partitions in CA SDM.

Use the following tools to accomplish this task:

- **BusinessObjects Central Management Console** (CMC) -- Lets you administer BusinessObjects Enterprise user authentication and permissions.

- **Universe Design Tool** -- Lets you modify the universe for CA SDM, Knowledge Management, CMDB, and Support Automation, which is a metalayer between CA SDM schema, and reporting tools.

- **CA SDM Security and Role Management** -- Lets you set up data partitions security to determine what data users can access.

Add the CA SDM Privileged User to CMC

The universe connection is configured by default to use the Service Desk Privileged User and Password when accessing data. This user should be added to the CMC as a new CA Business Intelligence user. There are two purposes for adding this user. First, you need this user if you plan to set up data partition security for reporting and second, it allows you to use this user when initially testing reports from the CA SDM Reports tab. The Reports tab requires a user who is defined to both CA SDM and CA Business Intelligence.

Use the instructions provided in the *CA Business Intelligence Documentation* to add your CA SDM users to the CMC and configure the CA SDM Privileged User account.

Define Universe Database Credentials

The universe must use the database credentials associated with the BusinessObjects user account.

Note: Verify that you sign on to the Universe Design Tool using the Privileged User account and not the Administrator User account.

To define universe database credentials

1. From the Start menu, browse to All Programs, BusinessObjects, BusinessObjects Enterprise, Universe Design Tool.
2. Log on to the Universe Design Tool.
   The Universe Design Tool window appears.
3. Select File, Import.
   The Import Universe dialog appears.
4. Select the CA SDM, Knowledge Management, CMDB, or CA ServiceDesk folder from the drop-down list.

   Note: If this is the first time you are using the Universe Design Tool, select Browse, CA Universes.

5. Verify the file path for the import folder in the Import Folder box.
6. Click OK.
   The universe window appears.
7. Select File, Parameters.
   The Universe Parameters dialog appears.
8. On the Definition tab, click Edit.
   The Login Parameters dialog appears.
9. Select the Use database credentials associated with Business Objects user account check box.
10. Click Next, Test Connection, and step through the universe connection dialogs that appear.

11. Click OK to finish.

12. Select File, Export.
    The Export Universe dialog appears.

13. Select the universe that you want to use from the Domain drop-down list.

14. Select Everyone from the Groups list

15. Click OK to export universe changes.

Establish Data Partitions

In Security and Role Management, create a data partition constraint that will restrict the database record access for all report users assigned to the data partition.

Note: For information on establishing data partitions constraints, see Data Partitions Setup.

Write CA Business Intelligence Reports

Contents

You can write CA Business Intelligence reports for CA SDM.

CA SDM ODBC Driver

Business Objects reporting applications (Crystal Reports and Web Intelligence) access data using an ODBC driver that connects directly with the CA SDM object engine named the domsrvr.

This connection provides a number of benefits:

- SELECT statements used by BusinessObjects reports reference objects and attributes using their CA SDM names (in other words, their Majic names). For example, a SELECT statement for a report on contacts could be written:

```
SELECT combo_name FROM cnt WHERE last_name LIKE 'smith%'
```

- The CA SDM ODBC driver maps attributes like combo_name and objects like cnt to their corresponding DBMS name or names.

- All CA SDM security, including data partition and tenancy restrictions, is automatically applied to reports. All connections between BusinessObjects and CA SDM are associated with a CA SDM contact, and the CA SDM ODBC edits input SELECT statements to enforce the security restrictions associated with the end-user reporting role. BusinessObjects does not connect directly to the database.

- The CA SDM Attribute Alias feature "flattens" or de-normalizes the CA SDM database. Attribute aliases are additional attributes in CA SDM objects that allow a query to reference attributes in joined tables without an explicit join, allowing the base table to be used as if it were a reporting view.

- The CA SDM ODBC driver supports date literals in queries, and automatically translates values in CA SDM internal date format to a standard DBMS date.

Important! The CA SDM ODBC driver is supported only for BusinessObjects reporting (Crystal and Web Intelligence). CA SDM does not provide a standalone ODBC client, and does not recommend use of the ODBC driver with applications other than BusinessObjects.

Write SQL for BusinessObjects Reports

All SQL statements used by BusinessObjects reports are processed by the CA SDM ODBC driver. The ODBC driver supports standard SQL 92 SELECT statements with the following changes and extensions:

- CA SDM object names are used in place of DBMS table names, and CA SDM attribute names are used in place of DBMS column names.

- A CA SDM attribute alias name can be used anywhere in the query where a column name is valid. The ODBC driver replaces the attribute alias reference with one or more joins.

  Note: For more information, see Attribute Aliases (see page 3217).

- CA SDM DERIVED attributes (such as combo_name) can be used in the selection list only. They are not supported in any other part of the query, including in the WHERE clause.

  Note: Many Combo Name With Userid objects have been provided in the universe, such as the Customer Combo Name With Userid object used as a filter in the sample ad hoc report provided in the *CA Business Intelligence Documentation*. These objects allow Combo Name to be used as filter prompts in ad hoc queries with Web Intelligence, to overcome the limitation of including Combo Name in the WHERE clause. They present both Combo Name and Userid in the filter prompt, but use only the selected Userids in the resultant SQL query.

- Queries can contain date literals in either of the forms:

```
d'yyyy-mm-dd hh:mm:ss xm' (where xm is either am or pm)

ts'yyyy-mm-dd hh:mm:ss'
```

These literals can be used anywhere in the query. The ODBC driver automatically converts them to CA SDM internal date format (the number of seconds from midnight January 1, 1970).

PDM Functions

To assist in working with specialized CA SDM features and data types, the ODBC driver extends SQL to support a number of additional query functions. All driver-supported functions begin with the string "Pdm", and are known as PDM functions as described in the following table:

PDM Functions	Description
PdmAddDays([date,] count)	When used with one argument, adds the number of days in its argument to today's date and returns the result. When used with two arguments, adds the number of days in its second argument to the value of the date column specified in its first argument and returns the result. This function may be used anywhere in the query
PdmAddMonths([date,] count)	When used with one argument, adds the number of months in its argument to today's date and returns the result. When used with two arguments, adds the number of months in its second argument to the value of the date column specified in it first argument and returns the result. The single argument form can be used anywhere in the query. The two-argument form can be used only in the selection list
PdmDay ([date])	When used with no arguments, returns the current day as an integer. When used with one argument, returns the day associated with the value of the date column specified in its argument. The zero argument form can be used anywhere in the query. The one-argument form can be used only in the selection list.
PdmDownTime(slaName, workshift, startDate, endDate)	Calculates the downtime between two dates under the specified SLA and workshift. This function can be used only in the selection list.
PdmMonth ([date])	When used with no arguments, returns the current month as an integer from 1 to 12. When used with one argument, returns the month associated with the value of the date column specified in its argument. The zero argument form can be used anywhere in the query. The one-argument form can be used only in the selection list.
PdmMonthName ([date])	When used with no arguments, returns the localized name of the current month ("January", "February", and so on). When used with one argument, returns the localized name of the value of the date column specified in its argument. The zero argument form can be used anywhere in the query. The one-argument form can be used only in the selection list.
PdmDay ([date])	When used with no arguments, returns the current day as an integer. When used with one argument, returns the day associated with the value of the date column specified in its argument. The zero argument form can be used anywhere in the query. The one-argument form can be used only in the selection list.
PdmSeconds(date)	Returns the value of the date column specified in its argument in its raw form as the number of seconds from midnight January 1, 1970. This function can be used only in the selection list. The argument is required.

PDM Functions	Description
PdmString (column)	Returns the string equivalent of value of the column specified in its argument. This function can be used with UUID, date, or string columns. It can be used only in the selection list.
PdmToday()	PdmToday() [timeAdj [, day [, month [, year]]]]) Evaluates to today's date (in seconds from 1/1/1970), adjusted according to the arguments: timeAdj: -1 -- adjust time to beginning of day (0:00:00); +1 -- adjust time to end of day (23:59:59) day: negative -- adjust date by number of days specified positive -- set day to absolute value specified (or to last day of month, whichever is less) month: negative -- adjust date by number of months specified positive -- set month to absolute value specified (or to December (12), whichever is less) year: negative -- adjust date by number of years specified positive -- set year to absolute value specified Adjustments are applied in the order year, month, day. A zero or omitted argument is ignored.
PdmYear ([date])	When used with no arguments, returns the current year as a four-digit integer. When used with one argument, returns the year associated with the value of the date column specified in its argument. The zero argument form can be used anywhere in the query. The one-argument form can be used only in the selection list.

Attribute Aliases

Attribute aliases are additional attributes in CA SDM objects that reference data from joined tables using Majic dotted join syntax (where the syntax srelname.attrname is a reference to attribute attrname in the table referenced by foreign key srelname. A large number of predefined attribute aliases are provided with CA SDM Release 12.9, with names that typically are the same as the corresponding Majic join, with underscores replacing the dots that indicate the join. For example, the following SELECT statement might be used for a report that lists information about the request assignees:

```
SELECT ref_num, assignee_combo_name, assignee_organization_name
   FROM cr WHERE customer_last_name LIKE 'smith%'
```

The CA SDM ODBC driver automatically builds joins as required to access the tables referenced by attribute aliases. A user in the CA SDM administrator role can easily add new attribute aliases online, providing a column-at-a-time way to extend the view corresponding to an object.

To access the Attribute Alias table, select the Administration tab, and browse to CA SDM, Codes, Attribute Aliases.

pdm_isql Interactive SQL

A command line utility, pdm_isql, is provided with CA SDM to allow interactive entry of SQL SELECT statements. SELECT statements entered into pdm_isql are sent to the CA SDM ODBC driver, allowing you to test SQL SELECT statements outside of BusinessObjects.

To use pdm_isql

1. Ensure that $NX_ROOT/bin is in your path.

2. Enter the command:
   pdm_isql

3. At the pdm_isql prompt, enter the command:
   connect *username*password@casd_hostname*
   (Where *username* and *password* are valid CA SDM login credentials, and the host name is the host name of a CA SDM server with a web engine.)

4. Enter SQL select statements followed by a semicolon.

Key Performance Indicators

Contents

Key Performance Indicators (KPIs) are metrics you can use to identify areas of your service management environment that can require administrative attention or configuration tuning.

Use the CA SDM web interface to configure your KPI definitions. The data they produce is stored in the CA SDM database and is available for producing web-based reports (see page 3201).

Note: In addition to defining KPI queries, you can configure the KPI daemon to retrieve CA SDM ticket data whenever a ticket is opened, closed, or certain fields are modified.

By defining and monitoring a planned set of KPIs, you can measure progress toward your organization's performance-related goals, and gather valuable data for driving strategic decisions about your IT environment.

Note: For information about the KPI database tables, see Technical Reference (see page 3821).

KPI Types

CA SDM supports three KPI types:

- **System KPIs** are installed with the product. You can customize them to meet your needs, but you cannot create new System KPIs.
- **Stored Query KPIs** call a stored query to retrieve metrics from the database. You can create custom Stored Query KPIs, or modify the predefined examples installed with the product.
- **SQL KPIs** allow you to incorporate a complete SQL query directly into the KPI. You can create custom SQL KPIs, or modify the predefined examples installed with the product.

Note: KPIs, whether predefined or user-created, cannot be deleted. When a KPI is no longer needed, you can deactivate it by setting the Record Status to inactive.

Predefined KPIs

Several KPIs of each type are installed with CA SDM. You can use the predefined Stored Query and SQL KPIs with their original definitions, or as models for your custom definitions.

You can use the predefined System KPIs with their original definitions, or modify some of their fields to meet your needs.

All predefined KPIs are installed as Inactive. For a KPI to begin functioning in your system, it must be set to Active. Navigate to Service Desk, KPIs on the Administration tab and search for the inactive KPI. Open the KPI and click Activate.

Important! Multiple versions of a KPI with the same name cannot be active at the same time.

Create a KPI

You can create custom Stored Query KPIs to produce Count metrics, and SQL KPIs to produce Count, Sum, Max, or Duration metrics.

Important! You cannot create new System KPIs; however, you can edit the predefined System KPIs to meet your needs.

Note: If multi-tenancy is installed, select the appropriate tenant from the drop-down list. The public (shared) option creates the object for all tenants.

Follow these steps:

1. Click CA SDM, KPIs on the Administration tab.
   The KPI List page appears.

2. Click Create New.
   The Create New KPI page appears.

3. Enter a name for the KPI and select either Stored Query or SQL from the dropdown list. Click Continue.
   The Create New KPI page displays the KPI fields. The following table describes the KPI fields. The Sys. S.Q. and SQL columns indicate the KPI types each field belongs to (System, Stored Query, or SQL).

Field	Sys.	S. Q.	SQL	Description
KPI Name	X	X	X	Identifies the display name for the KPI. Not editable.
Type	X	X	X	Defines the record as a System, Stored Query, or SQL KPI. Not editable.
Keep Existing Version	X	X	X	Specifies that the current version of the KPI record will be retained if the record is updated. Editable when the @NX_ALWAYS_KEEP_KPI_VERSIONS setting in the NX.env is set to No.
Version	X	X	X	Identifies the version number of the KPI record. The version number is incremented automatically each time the record is updated. Not editable.
Record Status	X	X	X	Specifies whether the KPI is active (gathering data) or inactive (not gathering data). Editable only by using the "Edit in List" feature on the KPI List page.
Metric Type	X	X	X	

Field	Sys.	S. Q.	SQL	Description
				Specifies the type of calculation the KPI will perform: Stored Query KPIs are always Count. System KPIs can be Count or Duration. SQL KPIs can be Count, Sum, Max, or Duration. Editable for SQL type KPI only. **Note:** The calculated duration is based on a change to values in a ticket in real time, not in business hours.
Refresh Time	X	X	X	Specifies the time interval for retrieving KPI metrics from the database. The value is editable. Refresh time is specified in HH:MM:SS format.
Process Type	X			System KPI (see page 3222) metrics can be derived from the following CA SDM processes: **domsrvr** -- Object Manager **bpvirtdb** -- BOP Virtual Database Server **db_agents** -- Database agents **webengine** -- The CA SDM web client
System Name	X			The internal name of the System KPI. Not editable.
User Context		X	X	(Optional) Specifies the userid of a CA SDM contact. The contact's role and tenant assignments are used to determine data partitioning for the metrics produced by the KPI. The value is editable.
Stored Query		X		The name of the stored query called by this KPI. The value is editable. **Note:** The stored query definition must be active and have the KPI Usage option enabled.
SQL Query			X	The SQL code for the query. The value is editable. **Note:** When you save a SQL KPI record, the syntax of your SQL query is validated. An error message appears when the code is invalid. If your SQL code does not include an aggregate, the KPI daemon logs error messages and does not return data to the kpi_data table.
Description	X	X	X	(Optional) Provides a detailed description of the KPI. The value is editable.

4. Click Save.

Note: When you save the initial definition for a SQL KPI, the syntax of your SQL query is validated. An error message is displayed if the code is invalid.

KPI Daemon

The KPI daemon manages the retrieval, organization, and storage of KPI metric data. The daemon runs continuously, and collects data at specified intervals from various system resources.

When the refresh time of a KPI is reached, the KPI daemon interacts with other system components as follows:

- **System KPI** -- Sends a request to a target daemon (webengine, domsrvr, bpvirtdb, or db_agents) to retrieve count or duration data.
- **Stored Query KPI** -- Sends a request to the domsrvr to collect count data.
- **SQL KPI** -- Sends a request to the domsrvr to collect count, sum, max, or duration data.

When the KPI daemon receives the requested data, it stores the resulting metrics in the database.

Note: The calculated duration is based on a change to values in a ticket in real time, not in business hours.

System KPIs

System KPIs enable you to collect metric data related to the operation of CA SDM processes.

The following process types are supported:

- **domsrvr** -- The CA SDM Object Manager (server process). The Object Manager also caches various records and tables for clients.
- **bpvirtdb** -- The BOP Virtual Database server enables operation of multiple Object Managers in the CA SDM environment. The Object Managers connect to the virtual database which arbitrates their access to database agents. For example, when retrieving a new range of ticket reference numbers, the virtual database ensures that only one Object Manager at a time accesses the table containing the reference numbers.
  Depending on your CA SDM configuration, the Object Managers connect to the virtual database of the following servers:
- Conventional: All Object Managers running on primary or secondary server connect to the virtual database of the primary server.

- Advanced availability: All Objects Managers connect to the virtual database of the same server that it is running on. For example, object managers running on the application server connect to the virtual database of the application server only.

The virtual database also performs caching of database information for Object Managers.

- **db_agents** -- Database agents perform SQL queries, and handle other interactions between CA SDM and the database management system (DBMS). Database Agents adhere to the CA SDM database schema, and translate the SQL code to the form required by the particular DBMS (for example, Oracle).

- **webengine** -- The CA SDM component that connects web browsers to an Object Manager through a pdmweb cgi running on a Microsoft IIS or Apache Tomcat web server.
Depending on your CA SDM configuration, there must be a web engine for WSP on the following servers for WSP Schema Designer to write schema files:

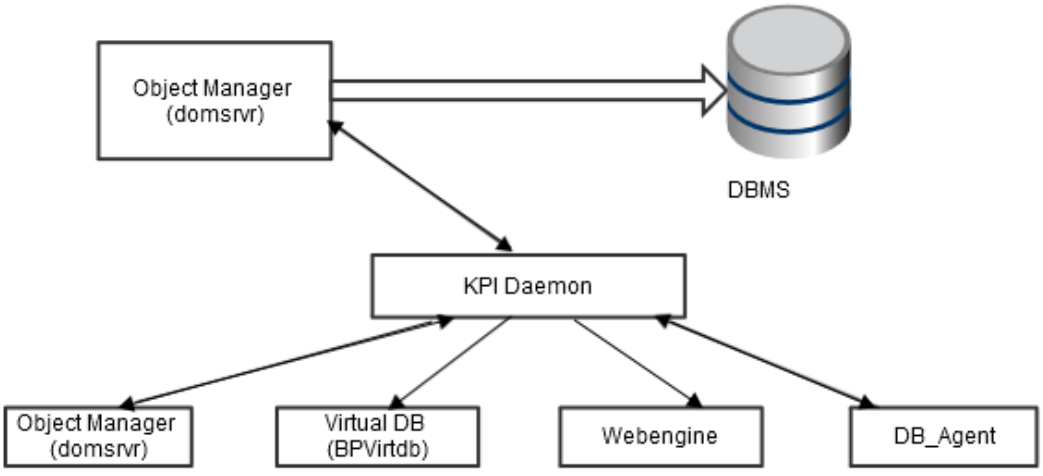
- Conventional: Primary server

  - Advanced availability: Background server

  Web engines are the true client of an Object Manager for user client web browsers. Web engines cache .htmpl web forms for connected users. You can manipulate the cache using the pdm_webcache utility and see client connection statistics using the pdm_webstat utility.

Note: For more information about these processes, see the *Implementing CA Service Desk Manager (see page 398)*.

The following diagram illustrates data flow for System KPIs.



Each system KPI produce one of the following metric types:

- Count
- Duration

System KPI Examples

- This example produces a count of the update requests sent to BOP Virtual Database:

```
updateCt
```

- This example reports how long requests for updates, inserts, and deletes to BOP Virtual Database took to complete:

```
virtdbUpdateResponseDt
```

Stored Query KPIs

With Stored Query KPIs you can generate reports based on count metrics retrieved from the CA SDM database.

CA SDM provides a set of predefined stored queries. Many of them are useful just as they are. You can also customize them to meet your needs, or use them as models for writing your own queries.

All Stored Query KPIs have a Count metric type.

Note: You can use stored queries to produce counter fields for your web interface Scoreboard, or KPI metrics, or both. To use a stored query in a KPI definition, the query must be enabled for KPI usage. For more information, see Stored Query Setup.

Stored Query KPI Examples

- This example produces a count of the open change orders at the assignee's location:

```
@cnt.location.name Changes
```

- This example produces a count of the workflow tasks that will violate an SLA before midnight of the current day:

```
Issue Workflow Tasks that will Violate an SLA today
```

SQL KPIs

SQL KPIs provide more flexibility than Stored Query KPIs. With SQL KPIs you can write your own queries to the CA SDM database to produce the following types of metrics:

- Sum
- Count

- Max
- Duration

> **Note:** Your SQL code must comply with SQL92 syntax.

The following considerations apply to SQL KPIs:

- To see the SQL code for these example queries, open the query definitions from the KPI List page.

  > **Note:** For instructions, see the *Online Help*.

- The @ symbol is not supported in SQL KPIs. Instead, use syntax as shown in the following example and an attribute alias:

  ```
  SELECT * FROM cr WHERE assignee_last_name = "Smith"
  ```

  For this example, you could use a predefined attribute alias. The Attribute Alias Detail page appears as follows:
  " Object Name = cr
  " Alias Name = assignee_last_name
  " Status = Active
  " Alias Value = assignee.last_name

Examples: SQL Query KPI

- This predefined example produces the sum of the estimated costs of all pending change order workflow tasks:

  ```
  Est Cost Sum of Pending Change Workflow Tasks
  ```

- This predefined example produces a count of the active change orders that have been closed and reopened:

  ```
  Count of Reopened Change Orders
  ```

Retrieve Ticket Data

To allow reporting on how long tickets remain in the various processing states, you can configure the KPI daemon to retrieve CA SDM ticket data whenever a ticket is opened or closed, and whenever any of the following fields values are changed:

- Active
- Assignee

- Area or Category
- Group
- Impact
- Organization
- Priority
- Root Cause
- Status
- Service Type

To enable ticket retrieval, install the KPI Ticket Data Table option available in Options Manager KPI folder.

The collection of data from new and updated tickets is enabled. The ticket data is written into the usp_kpi_ticket_data database table, and is available for generating web-based reports.

Note: For instructions, see the *Online Help*.

The following considerations apply to ticket retrieval:

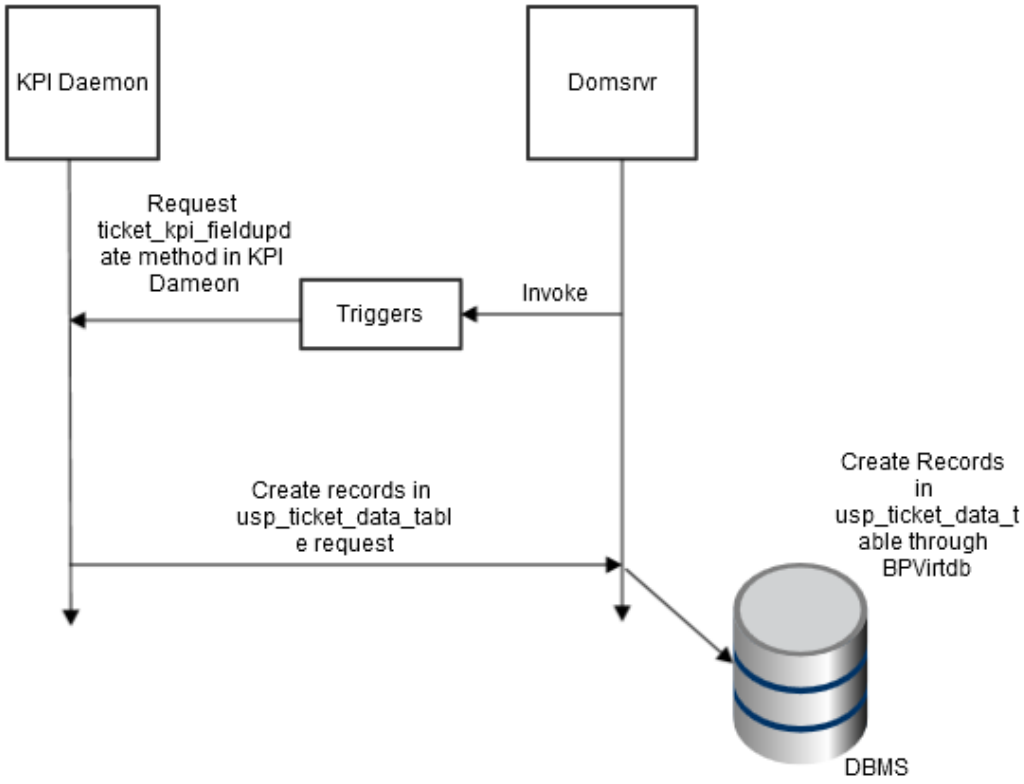
- The KPI daemon may take up to 30 minutes to populate the ticket information to the usp_kpi_ticket_data table.
- The support_lev field allows tracking of Service Type processing when the classic_sla_processing option is installed. The classic_sla_processing option enables the Service Type processing from CA SDM version 6.0 and earlier.
- Enabling this feature may result in degraded CA SDM performance.

KPI Ticket Data Flow

The KPI Ticket Data Table feature works on a trigger mechanism. When the kpi_ticket_data_table option is installed, the KPI daemon begins monitoring CA SDM ticket objects to track the following events:

- Open new ticket
- Check in changes to one or more monitored fields
- Close ticket

When one of these events occurs, a POST_CI trigger fires. The trigger sends a BPMessage with a trigger attribute list to KPI daemon, and adds the returned data to the usp_kpi_ticket_data table, as illustrated in the following data flow diagram.



KPI Ticket Data Table Record Types

There are five operation types in the usp_kpi_ticket_data table:

- INIT (0)
- NO_INIT_REC (1)
- REOPEN (2)
- UPDATE (3)
- CLOSE (4)

The type value (integer value shown in parentheses) is stored in the operation field. The end_time of the previous record is stored in the prev_time field. The ktd_duration field stores the duration, which is calculated as end_time minus prev_time. The previous record is defined in the following rules:

1. The INIT record indicates a ticket has been created.
2. An UPDATE record is created for each update to a ticket. It gets prev_time from a previous UPDATE record to the same ticket field if a previous UPDATE record exists. Otherwise, it gets prev_time from the INIT, NO_INIT_REC or REOPEN record, depending on which record has an end_time value closest in time to the UPDATE record.

3. The CLOSE record is the same as UPDATE.

4. If a ticket is reopened, a single REOPEN record is created to show the Active field value. The REOPEN record gets prev_time from a previous CLOSE record for the same Active field.

5. If a ticket was created before turning on the Options Manager option, it may have records for updates but without an INIT record. The program in this case creates a NO_INIT_REC record and gets prev_time from the first non-INIT record it encounters.

Note: For complete documentation of the table fields, see the *Technical Reference (see page 3821)*.

Troubleshooting

You can diagnose problems you might experience with KPI usage.

Verify that the KPI Daemon is Running

To verify that the KPI daemon is running, run the pdm_status command-line utility as follows:

```
pdm_status
```

Examine the output for for the following:

```
KPI Daemon myserver  Running  myserver 3568  Wed Feb 06 07:23:53
```

NX.env File

Review the $NX_ROOT/NX.env file to verify that the basic KPI configuration is correctly set.

If you have installed the KPI Ticket Data Table option, the NX.env file includes the following:

```
#########################################################################
# NX_KPI_TICKET_DATA_TABLE
# Enable the collection of changed fields from ticket objects
# (like Requests, Issues and Change Orders) to write record entries
# into the usp_kpi_ticket_data table.
#########################################################################
@NX_KPI_TICKET_DATA_TABLE=Yes

#########################################################################
# NX_KPI_FUZZ_TIME
# Specifies a tolerable delay for each KPI within which kpi_daemon
# sends a request to retreive KPI data when this kPI's refresh time
# is timeout
#########################################################################
@NX_KPI_FUZZ_TIME=20
```

Note: The default value of @NX_KPI_FUZZ_TIME is 20 seconds. You can modify this value within the range of 0 to 40 seconds. If you set this variable to a value higher than 40, 40 seconds will be used.

```
########################################################################
# NX_ALWAYS_KEEP_KPI_VERSIONS
# The keep_version attribute in Kpi table is displayed on the KPI
# Detail Edit form as a checkbox. The NX_ALWAYS_KEEP_KPI_VERSIONS
# option specifies that checkbox is read-only and is always checked.
########################################################################
@NX_ALWAYS_KEEP_KPI_VERSIONS=Yes
```

Turn on KPI Daemon Tracing

Use the pdm_logstat utility to turn on trace logging to monitor KPI daemon activity.

To turn on KPI daemon tracing, run the following command:

```
pdm_logstat -f cache_table_mgr.c VERBOSE
```

To turn off KPI daemon tracing, run the following command:

```
pdm_logstat -f cache_table_mgr.c
```

Examine the stdlog.0 file for entries pertaining to KPI daemon activity.

The following example shows normal KPI daemon connections to the host computer and the domsrvr:

```
02/06 05:42:14.58 garbo-2k3-bb kpi_daemon 2432 SIGNIFICANT kpi_daemon.c  117
KPIDaemon ready for action!
02/06 05:42:14.80 garbo-2k3-bb domsrvr 792 SIGNIFICANT connmgr.c 2314 Connecting
client kpi_daemon:garbo-2k3-bb
02/06 05:42:14.81 garbo-2k3-bb kpi_daemon 2432 SIGNIFICANT main.c 220 KPI daemon
connected with domsrvr
```

The following example indicates an error in a KPI named webSessionCT:

```
01/16 13:24:46.74 jed web:local 2152 ERROR sys_kpi.c 96 Invalid KPI metric type:
1382180215 (KPI name:webSessionCT)
```

The following examples show KPI daemon activity:

```
02/06 07:23:50.47 garbo-2k3-bb  kpi_daemon 3568 TRACE cache_table_mgr.c 427 Cache
Table manager created Kpi_Obj (KPI dob record_id:9003) (KPI type:2)
02/06 07:23:50.53 garbo-2k3-bb kpi_daemon 3568 TRACE cache_table_mgr.c  427 Cache
Table manager created Kpi_Obj (KPI dob record_id:9103) (KPI type:1)
```

Note: For information about KPI types, see KPI Ticket Data Table Record Types (see page 3227).

Summary and Detail Reports

CA Service Desk Manager has built in summary and detail reporting options. To print or view summary and detail reports, you must first select the records you want to include in the report. You can select specific records for a report using the search feature of the list windows. To generate the report, select Summary or Detail from the Reports drop-down menu.

For example, from the Request List page you can enter search criteria to create a list of requests that you can then use to generate a report.

You can also print a single page detail report for each record by choosing Print Form from the File menu within any detail window. To print a report for a newly created record, you must first save the record.

Generate Analysis Reports

The Administration Tab provides built-in analysis reports for a global and detailed perspective on the service desk process

- Request Area or Issue Category reports provide you with the number of requests or issues opened in the specified period for each request area or issue category. This report is sorted alphabetically by request area or issue category.
- Request or Issue reports provide you with statistics, such as number of requests or issues opened, number of requests or issues closed, average time open, and average time until closed, for a specified period. This report is sorted by date, oldest to newest.
- Request Area Priority or Issue Category Priority reports provide you with the number of requests or issues opened by priority in the specified period for each request area or issue category. This report is sorted by priority (highest to lowest) and then alphabetically by request area or issue category.

You can display the analysis report for today, for the past thirty days, year-to-date, and much more.

Follow these steps:

1. Choose the Administration tab.
2. Expand the Service Desk and Analysis nodes.
3. Choose Request or Issue.
4. Choose the appropriate report based on the time frame you want.

Reporting Using CA Service Catalog

Administrators use data objects, data views, and layouts to retrieve, format, and publish data, in both reports and other facilities, including forms, as follows:

1. Understand how data objects, data views, and layouts comprise reports:

   - The *data object* is the lowest layer. The data object defines the source of the data, the fields that make up each row of data, and the selection criteria.
     The data object produces a set of rows and columns of data that other facilities can use. These facilities include data views, forms, and runtime variables for other data objects.
     You can set permissions on a data object by business unit, functionality, and role.

   - The *data views* define the format of a data object for a report. You can present the rows and columns of a data object in a table, chart, or both. You can highly customize tables and charts.

   - The *layout* is a combination of data views, text, and images. The layout is best suited for presenting an overall view of business data.
     You can publish layouts as reports to the catalog. Users and accounts can request and subscribe to them.
     You can set permissions on a layout by business unit, functionality, and role.

2. Create and edit data objects (see page 3232), including these tasks:

   - Retrieve and display data from a data source.

   - Specify dynamic selection criteria that are based on system variables or user input.

   - Set up access to data objects according to role or business unit.

3. Create and edit data views (see page 3239), including these tasks:

   - Create custom charts and tables, including three-dimensional (3D) ones.

   - Provide summary level reports with drill-down capabilities to report details.

   - Combine views from multiple data sources, text, and images in the report layout.

4. Create and edit layouts (see page 3241), including these tasks:

   - Publish reports to the catalog (see page 3242), where they can be requested or subscribed to by users or accounts.

   - Publish reports to the dashboard library.

   - Set up access to reports according to role or business unit.

Note: Building reports requires knowledge of both the MDB schema and SQL syntax.

CA Service Catalog includes several predefined data objects, data views, and layouts to use as-is or as models.

This section contains the following articles:

- Manage Data Objects (see page 3232)

Manage Data Objects

This article contains the following topics:

Administrators can use data objects to define the data to use for a chart, table, or other facility, including a field in a form. A data object can have the following data sources:

- An ODBC-connected or JDBC-connected database management system (DBMS). Examples include SQL Server or Oracle database.
- A delimiter-separated value file.
- Any other data source that a Java report plug-in can access.

Note: When you create reports, ODBC-type data objects do not retrieve nvarchar-type fields. To retrieve nvarchar fields in the objects in your reports, use JDBC as the database connection type.

You perform the following tasks to manage data objects:

- View the data objects and organize them in folders.
- Become familiar with the runtime variables (see page 3232) in data objects.
- Add a query runtime variable (see page 3234) for use in a data object.
- Add a data object (see page 3234) or edit one.
- Use predefined data objects. (see page 3237)
- Delete a data object.

Runtime Variables

Data objects can use *runtime variables* to alter behavior and selection criteria dynamically.

For Query data objects, you can use runtime variables in the SQL query. As a prerequisite, define these runtime variables in the Variables list. That list includes default Query variables, and you can add your own.

For example, consider a report that is based on a SQL query that displays a list of users. The data object can take a Last_Name value as a runtime variable to indicate the starting characters of the last name. Users of the data object are prompted for the Last_Name value. You can use the runtime variable of type String that is named %Last_Name% in the SQL statement. Use this variable to restrict the results to user records that start with the value entered by the user. The following SQL statement provides a sample query:

```
SELECT first_name,middle_name,last_name FROM ca_contact WHERE (ca_contact.las
```

Note: Users are prompted for only the runtime variables in the SQL query.

For plug-in data objects, you can pass runtime variables to the Java class as name-and-value pairs. As a prerequisite, verify that the Java report plug-in class takes the name-and-value pairs for the plug-in data object.

For example, consider the com.ca.usm.reporting.Plugins.RequestFulfillmentReport plug-in class. This plug-in class takes a parameter of Date type named START_DATE. Therefore, START_DATE is required in the data object that uses this plug-in class. In this case, perform either of the following actions:

- Hard-code START_DATE as a constant.
- Prompt the user for the date START_DATE value and pass that value to the plug-in.

You can use contextual *system variables* with runtime variables:

- As default values when you prompt the user.
- As constant values to pass to the plug-in.
- As values to use in a query.

The contextual system variables are as follows:

Name	Variable
Current Day	%TODAY%
Previous Day	%TODAY%-Days(1)
Next Day	%TODAY%+Days(1)
First Day Of Month	%START_OF_CURRENT_MONTH%
Last Day of Month	%END_OF_CURRENT_MONTH%
First Day Of Year	%START_OF_CURRENT_YEAR%
Last Day Of Year	%END_OF_CURRENT_YEAR%
User Domain (Business Unit)	%USER_DOMAIN%
User ID	%USER_ID%

Add a Query Runtime Variable

You can add a custom runtime variable to use with a Query data object. An example is adding a query runtime variable that is a drop-down variable.

Follow these steps:

1. Click **Administration**, **Report Builder**.
2. Perform *one* of the following actions:
   - Add a data object
   - Edit an existing data object
3. Click **Create Data Object**.
   The Create Runtime Variable or Edit Runtime Variable dialog appears.
4. Specify the **Name**, **Datatype**, and other data in the fields provided.
5. Click **Create Variable**.
   The Catalog system saves your variable definition.

You can use the variable in an SQL query for a Query data object. Users are prompted to enter a value when they run the data object.

Note: When you add a query runtime variable that is a drop-down variable, the number of values in the resulting drop-down list is limited to 1000. If the report query returns more than 1000 values, the system truncates these additional values. So, the user cannot view them in the drop-down list. For more information about how to increase this value, see the Modify XSL, XML, JavaScript, and Image Files (see page 2018) section.

Add a Data Object

You can add and edit data objects to define the source and content to retrieve for a report.

Follow these steps:

1. Click **Administration**, **Report Builder**.
2. Click **Create Data Object**.
   The Data Object Properties page appears.
3. Perform the following actions:
   a. Select the Type of data object to create.

b. Complete the fields, specifying the detailed options for the data object (see page 3235). The exact fields that appear vary according to your selections for Type and Show Advanced.

4. Set the permissions for the data object, as follows:

   a. Click **Permissions**.

   b. Set the access levels according to role, business unit, and CA EEM user groups, as applicable.

   c. Click **OK**.

5. Click *one* of the following options:

   - **Save**
     Saves the new data object without displaying any data.

   - **Save & Test**
     Saves the new data object and displays the first 25 rows of the resulting data.

The Catalog system saves the new data object.

Note: You can also click Create Data View to create a data view from this data object.

Detailed Options for Data Objects

When you add or edit a data object, you complete the fields, specifying the detailed options for the data object. The exact fields that appear vary according to your selections for **Type** and **Show Advanced** on the page for adding or editing a data object. The following fields require explanation. These fields appear according to your selection for Type: Query, CSV File, or Plugin.

- **Query**
  Specifies the data to retrieve from a database query, as follows:

  - **Database**
    Specifies the name of the database connection. The default is mdb.
    Using the Query Builder, you can create a database connection definition that can use JDBC or an existing ODBC data source on the Catalog Component server. For ODBC, administrators must define this data source identically on each Catalog Component computer in your implementation. This requirement does not apply to JDBC. Therefore, we recommend JDBC.

  - **Table**
    Specifies a comma-separated list of tables for use in the SQL query. Use English characters *only* .

  - **Fields**
    Specifies the names of the database table fields to produce as data object columns.
    Use the Search icon to populate these names that are automatically based on the query in the

Query field. As a prerequisite, save the data object before you do so.
If you use an alias for a field in the query, you can use either name for the value of Fields. Use English characters *only*.

- **Query**
  Specifies the SQL query to use.
  Optionally click Query Builder for help defining the query.

  > **Note:** You can use the Query Builder to define new ODBC or JDBC data sources.

- **Pivot, DB Locking, *and* the Create Variables and Manage Variables buttons**
  See Advanced Fields at the bottom of this topic.

- **CSV File**
  Specifies the data to retrieve from a file in delimiter-separated value format, as follows:

  - **Fields**
    Specifies the names of the CSV file fields to produce as data object columns.

  - **CSV file**
    Specifies the path name of the CSV file. The path can be relative to %RPT_HOME% folder on the Catalog Component server.

    > **Note:** If you use multiple Catalog Component computers, this file must exist in the same folder on all of them.

  - **Delimiter**
    Specifies the delimiter that separates the values in the file. Select a value from the drop-down list.

  - **Pivot**
    See Advanced Fields at the bottom of this page.

- **Plugin**
  Specifies the data to retrieve from the output of a Java plug-in, as follows:

  > **Note:** For more information about plug-ins, select Administration, Tools, Links, and see the Plug-In Documentation.

  Enter the values for the fields that are shown for this type:

  - **Fields**
    Specifies the names of the plug-in output fields to produce as data object columns.

  - **Class Name**
    Specifies the full class name of the plug-in.

- **Arguments**
  Specifies the arguments for the plug-in.

- **Pivot *and* DB Locking**
  See Advanced Fields at the bottom of this page.

- Advanced Fields
  Selecting the Advanced check box exposes the following fields:

- **Pivot**
  Presents subtotals and counts of selected data.
  Select Pivot to display the Select Pivot Fields dialog and configure the parameters.
  This field applies to *all* selections for Type.

- **DB Locking**
  Specifies the type of database locking to use when reading from the database.
  Select a value from the drop-down list.
  For assistance, click the Help (question mark) icon next to this field.
  This field applies when the Type is Query or Plugin.

- **Manage Variables and Create Variable buttons**
  Manage existing variables and add new ones. You can use these variables in SQL queries.
  This field applies *only* when the Type is Query.

Pre-Defined Data Objects

CA Service Catalog has many predefined report data objects (data objects) that you can use in your reports. F

Note: Data objects in this list that mention CA CMDB, CA Service Desk Manager, or CA APM are applicable *only* if the named product is integrated with CA Service Catalog. Otherwise, the data object returns irrelevant data. For information about the integrations with these products, see the Integrating CA Service Catalog (see page 3425) section.

- **Requests associated to assets**
  Returns the requests that are associated to assets in the business unit that you specify.

- **Requests associated to change orders and configuration items, by business unit**
  Returns CA Service Desk Manager change orders and CA CMDB configuration items that are associated to CA Service Catalog requests in the business unit you specify.

- **Requests associated to change orders and configuration items, by user**
  Returns CA Service Desk Manager change orders and CA CMDB configuration items that are associated to CA Service Catalog requests for the user ID that you specify.

- **Requests by business unit**
  Returns all requests for the business unit and date range that you specify.

- **Requests by status**
  Returns all requests for the status and date range that you specify.

- **Requests by year and month**
  Returns the total number of requests for each month in the year that you specify.

- **Request fulfillment**
  Returns the amount of time that is taken to approve, fulfill, and complete all requests within the date range that you specify.

- **Request item fulfillment**
  Returns the following values:

  - The time that is used to approve, fulfill, and complete the request for the specified service option element.

  - Request SLA violation data for each request.

- **Request item fulfillment averages**
  Returns the following values:

  - The total number of requests that include the specified service option element.

  - The total time and the average time that is used to approve, fulfill, and complete the requested service option elements.

  - Request SLA violation data for each request item average.

- **Request item fulfillment by request ID**
  Returns the following values:

  - The amount of time that is taken to approve, fulfill, and complete each service option of the specified request.

  - Request SLA violation data for each service option

- **Request SLA Instances**
  Returns all request SLA instances, with their SLA warning and violation thresholds.

- **Services associated to asset models**
  Returns the CA APM asset models associated to services and service options in the business unit that you specify.

- **Services associated to configuration items**
  Returns the CA CMDB configuration items that are associated to service in the business unit that you specify.

- **Total requests by business unit**
  Returns the total number of requests that are created per business unit for the date range that you specify.

- **Total requests by month**
  Returns the total number of requests that are grouped by month for the year that you specify.

- **Total requests by status**
  Returns the total number of requests that are grouped by status for the date range that you specify.

Note: CA Service Catalog also provides predefined data objects for accounting, data mediation, financial reports, and metric events. For more information, see the comments that are supplied with the related data objects.

Manage Data Views

Administrators use data views to format the data from a data object and present it in tables and charts.

- Add, edit, delete, or view data views and assign them to folders.
- Export a data view in PDF or CSV (delimited) format.
- Manage off-line data views based on a data view.
- Set permissions to specify the level of access to a data view for each role.

You can add or edit a Data View.

Follow these steps:

1. Click Administration, Report Builder.
2. Click Data Views in the left menu.
3. Create a data view or edit an existing one.
4. Complete the fields and click Save. Use the Choose Data Object icon to select a data object to use for this data view.
5. (Optional) Configure how each field in the data object appears in a report: Click Column Rules to configure the presentation of a data view that appears as columns in a report. Select the column that you want in the Settings for Column field. Complete the fields and configure the settings on each tab.
   - Select Show Help to display help text for the tab.
   - Click Advanced to specify advanced settings.

Linking Tab

- **Link Items in Column *column-name* To Other Pages**
  Specifies whether to link the values in the column to another web page, either within or outside CA Service Catalog.
  Select this field to activate it and to open the fields under it for editing.

  - **Special**
    Specifies a link within CA Service Catalog to another data view, a report layout, or a GUI node.

  - **Link Address**
    Specifies one of the following options:

    - Another data view, a report layout, or a GUI node, if you used the Special link to add one.

    - A URL to a website or file share, if you did *not* use the Special field. Enter the URL manually.

    Also, the Link Address field optionally specifies a variable from the data object on which the data view is based. Click the Insert Variables icon to add a variable to this field.

Formulas Tab

- **Apply Formula to Column *column-name***
  Specifies whether to apply a JavaScript formula to the column value.
  Select this field to activate it and to open the fields under it for editing.

  - **Special**
    Specifies an image formula to apply on the data for the column. Use the formula to format a cell or row that is based on a value. Use the following format:

    ```
    IMG:image_file_path
    ```

    image_file_path specifies the folder and file name *under* the USM_HOME\view\webapps\usm folder.
    For example, the following line displays the add.gif image in the cell for the column:

    ```
    IMG:images/add.gif
    ```

    To include the cell text also, enter the column name variable within the single quotes. An example follows:

    ```
    IMG:images/add.gif]%Col1%
    ```

    If you use multiple Catalog Component servers, verify that this file resides in the same folder location on all servers.

  - **Column Formula**
    Specifies variable from the data object to use in the column formula. To use a variable, click the Insert Variables icon.
    Examples of formulas using JavaScript follow:

    ```
    100*%name%

    Math.max(%Col1%,%Col2%)
    ```

```
(10*%Col1%)+(20/%Col2%))+' Units'

%name%'.toUpperCase()
```

Translations Tab

- **Apply Translations to Column *column-name***
  Specifies whether to apply a translation formula to the column value.
  Select this field to activate it and to open the fields under it for editing.

  - **Translations**
    Substitutes a translated value for each data object value. You can optionally apply the translation before applying a formula to the column value.
    For example, a column can return data as integer value *1* which means opened, and *2* which means closed. You can apply translations that:

    - Display *Opened* in place of all values of type *1* in a column.
    - Display *Closed* in place of all values of type *2.*

Formatting Tab

- **Apply Formatting Settings to Column *column-name***
  Applies formatting to a column. Examples include font, justification, highlighting, and color.
  Select this field to activate it and to open the fields under it for editing.

Summary Tab

- **Summary**
  Adds summary information for the column.
  Select this field to activate it and to open the fields under it so that you can select them. The fields that you select appear in the summary of the report.

Manage Layouts

Administrators use layouts to present multiple report elements as one report. You can design custom layouts using data views, text, images, URLs, and other objects. You can specify positions, sizes, colors, borders, styles, and other settings.

- View layouts and organize them in folders.
- Manage off-line layouts that are based on a layout.
- Add or edit a layout. When you add or edit a layout, you can set its status. You can also set the permissions to specify the level of access of each role to the layout.

A layout defines the presentation of multiple report elements. Create and configure layouts to obtain the format you want for reports. You can use one of several sample layouts as a starting point. You can set permissions for the layout and optionally propagate those permissions to the underlying data views and data objects.

Follow these steps:

1. Click Administration, Report Builder, and select Layouts in the left menu.

2. Create or edit a layout.

3. Click one of the options to add the new element you want to the layout. For example, New Text or New Data View.

4. Drag the object to the location you want on the layout.

5. Configure the properties of the object by clicking the properties (i) icon and completing the fields.

6. Click Permissions and set the access levels according to role, business unit, and CA EEM user groups, as applicable, and click OK.
   The Set Permissions dialog closes, and you return to the Edit Custom Report Layout page.

7. Click Save and specify the status from one of the following options:

   - **Created**
     Specifies that the layout is visible *only* to the user who created it (the creator). No other user is permitted to view the layout, regardless of the permissions set for it. This option enables the creator to complete it before anyone else can access it.

   - **Available**
     Specifies that the layout is visible to the owner and to any user who is granted permissions to it.

8. Continue editing the layout as needed; save it periodically and when you are finished. Exit the Edit Custom Report Layout page by clicking Cancel.

Publish and View Reports

If you are using CA Service Catalog, you can publish a report to a catalog. After you do so, you can add the report to a service as a service option so that users can request the report. You can publish a report only if its status is *Available*.

Follow these steps:

1. Click Administration, Report Builder.

2. Select Layouts in the left menu.

3. Expand the folders by clicking the folder names or by clicking List View under Report Layout Objects.

4. Find the report that you want and click the Publish Report to the Catalog icon in the Action column.
   The Catalog system adds the layout as a service option to the Published Reports service option group.

5. View reports, as follows:

   a. Click Administration, Report Builder.

b. Expand the folder by clicking the folder names or by clicking List View.

c. Find and display the report that you want.

You can optionally add the service option for the report to a service when you define the service (see page 3001). As a result, users can request the report in the service.

After you have published a report, you and other users can view it. To view reports, you require access to the Reports menu option.

Follow these steps:

1. Click Administration, Report Builder.
2. Expand the folder by clicking the folder names or by clicking List View.
3. Find the report that you want and display it.

You have viewed the published report.

View the Business Value Dashboards

Business value dashboards aggregate smaller chunks of data into higher-level actionable information that enables IT Managers to make informed decisions. The dashboards correlate information across incident and request management that is required for executives users/mangers whose responsibilities span multiple functions.

CA Service Management provides two dashboards namely, Service Demand Dashboard and Operational Effectiveness Dashboard. Information that these business value dashboards provide is as follows:

- Service support metrics categorized by parameters such as time period, location, and organization unit. This information helps IT managers understand the prevailing pattern and plan capacity for upcoming months/quarters.
  For example, as an IT executive, you may want to understand the volume pattern of incidents or requests over the past three months to help you manage resources better. Also, you may want to identify the category of services which involved the maximum cost and cost pattern over the last six months.
  You can access the Service Demand dashboard to view this information.

- Demand for services categorized by parameters such as time period, location, and organization unit that provide insight into consumption of services in a specific category.
  For example, as an IT manager, you may want to know the categories (software, hardware, network and so on) which had the maximum number of incidents in the last one month and the category's incident/request volume of a team in a particular location.
  You can access the Service Demand dashboard to view this information.

- Functional effectiveness information that helps process managers analyse the performance of a support group the impact on cost.
  For example, as a process manager, you may want to analyse the performance of an L1 function (number of services resolved) in different locations and identify the reason for varying

performances of the teams. Also, in a support group, you may want to understand the number of incidents that were transferred from L1 to L2. If the number of escalations is high, the time and effort spent increases and thus results in a significant impact on cost and customer satisfaction. The information in the dashboard helps you identify any process changes/resource requirement /knowledge gaps required to enhance the performance of the various support groups and the functions.
You can access the Operational Effectiveness dashboard to view this information.

To understand how cost, effort, and volume of incident/request are calculated, see Important Metrics (see page 791). Each dashboard is a service offering that is exposed through CA Service Catalog and accessible through the Unified Self-Service interface.

Follow these steps:

1. Log in to Unified Self-Service as a user with permissions to access the dashboards. For example, Executive User.
   If Unified Self-Service is not installed, you can access the service offerings from the CA Service Catalog user interface.

2. In the Home page, click Request a Service.
   The Request Page Appears.

3. Under Categories, click Service Management Dashboards.

4. Click an appropriate service offering to see the related information.
   Note: The Service Demand dashboard displays only information based on products you installed. For example, if CA Service Catalog is installed the dashboard displays information related to requests only. Contact your administrator for more information.

Unified Self-Service

Unified Self-Service (formerly CA Open Space) is a community-based communication tool, which lets you connect and share knowledge with the people in your organization. Using this communication tool, you can post questions, get answers, share information, solutions, and ideas. A powerful search capability offers results from community conversations, SharePoint content, and external search engines, such as Google.

As part of CA Service Management, Unified Self-Service is integrated with CA SDM and CA Service Catalog as a self-service front end. If the community cannot provide the answer, you can open a request. You can also monitor the progress of requests in Unified Self-Service.

You can use shortcut keys to perform some basic navigation tasks quickly or to work without a mouse. The following table describes the available keyboard shortcuts:

TO DO THIS	PRESS
Go to Home page	CTRL+1
Go to Communities	CTRL+2
	CTRL+3

TO DO THIS	PRESS
Ask a Question	
Go to My Profile	CTRL+4
Reply to a Question	CTRL+5 **Note:** To use the keyboard shortcut to reply to a question (CTRL+5), you must be viewing the entire conversation.
Go to Questions	CTRL+6
Display Help	F1

Using the Unified Self-Service Home Page

The **Home** page displays an overview of the activity in Unified Self-Service.

You can view the following details:

- Requests you created that are currently not resolved. You can click a request to view more details about the request.
- Important announcements such as a scheduled maintenance activity.
- Recently posted or answered questions in the community. You can click a question to view or reply to the question.

You can also perform the following tasks:

- Report issues that require assistance from IT.
- Create requests when you need software, hardware, or any other service.
- Post a question in the communities to seek advice from others in the community.

Collaborate Using Communities

Communities are the different forums that your organization creates to help people connect and share information. You can perform the following tasks in the Communities page:

- View the communities that you are currently part of and the communities that your organization created for you to explore.
- Post or reply to questions in the communities that you have joined.
- Join communities that you are not a member of. Access to communities may require approval from your Administrator.

Follow these steps:

1. Log in to Unified Self-Service.
2. In the Menu bar, click My Communities.
3. To post a question in communities, complete the following steps:
    a. Click New Question and enter the question.
    You can alternatively click the Ask a Question tile on the Home page.
    b. At the bottom of the page, click Change to select the community that you want to post your question in.
4. Select a community to view the questions in the community.
5. To reply to a question, select the question and the click Reply.
6. To join a community, complete the following steps:
    a. Click All Communities.
    A list of communities is displayed.
    b. In the community that want to join, click Join.

Manage User Profile

Personalize your profile to enrich the community experience. You can perform the following tasks in the **My Profile** page:

- Add a photo to help connect with your community.
- Set your preferred display language. The Unified Self-Service user interface is displayed in the selected language but the user-generated content remains in the language in which it was entered.
- Set your notifications preferences to specify when you want to receive email and application notifications about Unified Self-Service activity.
- Add words that describe your interests and skills. These tags help Unified Self-Service alert you with questions that interest you or that you are qualified to answer.

Follow these steps:

1. Log in to Unified Self-Service.
2. Click My Profile from the drop-down list in the top right of the page.
3. Click Edit My Profile.
4. Specify the details and click Save.

Create a Request or Issue

Through Unified Self-Service you can view the details of requests and issues you created from a single location. The Requests page allows you to perform the following tasks:

- View the requests and issues you created.
  The My Recent Requests section displays requests and issues based on when a request/issue was last updated.

- Filter requests and issues based on their status.

When you face an issue, you can report it to IT help desk by creating a new issue. Also, if you need hardware, software, or any other service, you can create a request and select from a catalog of services available to you.

Follow these steps:

1. Log in to Unified Self-Service.

2. In the left Menu, click Create.

3. To create an issue, complete the following steps:

    a. Select Create New Issue. You can alternatively click the Report an Issue tile on the Home page.
    The Report an Issue page opens.

    b. Specify the required information and click Submit.

4. To create a request, complete the following steps**:**

    a. Select Create New Request. You can alternatively click the Request a Service tile on the Home page.
    The Request a Service page opens.

    b. Specify the required information and click Submit.

Explore Questions in Community

Through Unified Self-Service, you can view and post questions in community to learn from the community. You can also reply to questions posted from others in the community. The **Questions** page lets you do the following:

- Explore the latest questions posted, or those answers that the community has identified as the most helpful, or the questions that have been answered.

- Look through the unanswered questions that match the interests and skills in your Unified Self-Service profile. Unified Self-Service displays questions based on the tags (words that describe your interests and skills) you specify in your profile. For more information, see Manage Your Profile (see page 3246).
  Note: The **Recommended** section displays only the top 10 recommended questions.

You can perform the following actions on the questions:

- Reply to a question.
- In response to a question, create a request or report it as an issue. The details of the request are automatically filled based on the question.

Search for Information

Using the Unified Self-Service search, you can search for information from different data sources (as configured by the administrator) along with community message boards. For example, you can search for knowledge base articles in your organization or information from external knowledge stores like Google, organization knowledge stores like SharePoint.

View Resources that You Own

Through Unified Self-Service, you can view the resources such as software or hardware that you currently own.

Note: If you do not see the Resources page in the Unified Self-Service user interface, it is because your administrator has not configured it for you. Please contact your administrator for more information.

Follow these steps:

1. Log in to Unified Self-Service.
2. In the Menu bar, click My Resources.
   The Resources page lists the resource you currently own.

Manage User Password in Unified Self-Service

You can reset your password after expiry, from the Unified Self-Service (USS) console.

Note: This feature is supported only when USS is integrated with CA EEM.

Follow these steps:

1. Log in to the USS console using your current password.
   If your password has expired, the Change Password page is displayed.

2. Enter your old password, and then your new password in the respective fields.

3. Click **Save**.
   You are redirected to the login page after the password reset is successful. You can login using the new password.

Problem Management

Problems are difficulties encountered when following normal procedures. Records of problems are saved, along with the steps taken to correct the problems.

Note: Depending on your role, you may not have access to all the functionality described in this section. For example, some predefined roles can edit records but cannot create records.

Troubleshooting

The section contains the following articles:

Troubleshooting CA Service Management

Customization

Perform Customization

Any “modifications” or “adaptions” or “configurations” that are done administratively through the interface (web browser, command-line, Web Screen Painter) are “supported”, meaning CA Support can assist with the basic suggestions and troubleshooting. CA Support do NOT perform any changes for the customer. The customer is responsible for the changes made. For example, adding a field to a table and putting the field on a form through Web Screen Painter is a fully supported “modification”. Similarly, installing or uninstalling a feature through the Options Manager administration is a fully supported “configuration”. Anything to do with SPEL code, Java scripting (or any language scripting), or a customer-specific change to the underlying base code-line (done by CA Services or a Partner), is NOT supported by CA Support. The customer can perform these actions, but is responsible for the support, maintenance, and troubleshooting when an issue occurs. If such “customization” affect expected out-of-the-box behavior, CA Support will ask the customer to remove the customization and see if the behavior persists.

Retain Customization

When any form is modified, the customer changes are overwritten and has to be recreated. There is a process in the upgrade that attempts to detect and identify the differences in the forms, and reports it to the customer for their investigation. However, it is highly recommended to document your customization BEFORE you perform any upgrade. In some cases, a new feature may be similar to the user customization, so the user changes must be removed.

Unable to Install CA Service Management

If the CA Service Management installation fails, check the log files, take corrective actions, and retry the installation. If the installation still fails, proceed to integrate the required products or common components manually.

- Integrate CA Service Catalog with CA Service Desk Manager Manually (see page 3255)
- Integrate CA Service Desk Manager with Common Components Manually (see page 3262)
- Integrate CA Service Catalog with Common Components Manually (see page 3292)

Integrate CA Service Desk Manager with CA Asset Portfolio Management Manually

Important! Review the following section only if you want to manually integrate CA Service Desk Manager with CA Asset Portfolio Management when the automatic integration between the two has failed.

To manually integrate CA APM and CA SDM, follow these steps:

1. Enable Single Sign-On (SSO) from CA Asset Portfolio Management to CA Service Desk Manager (see page 3251)
2. Verify Single Sign-On (see page 3254)
3. Launch CA Asset Portfolio Management in Context From CA Service Desk Manager (see page 3255)

Enable Single Sign-On (SSO) from CA Asset Portfolio Management to CA Service Desk Manager

CA Service Management provides the following ways to enable SSO from CA Asset Portfolio Management (CA APM) to CA Service Desk Manager.

- Use the Web Service Access Policy File (see page 3252)
- Use the CA Service Desk Manager Administrator Credentials (see page 3252)

Both the mechanisms internally use the CA Service Desk Manager SOAP Web Services to achieve the SSO from CA APM to CA SDM. You can configure either one or both the mechanisms to achieve SSO from CA APM to CA SDM.

Important! Ensure that CA APM and CA Service Desk Manager are installed on the same database.

Note: CA APM uses the fallback mechanism during the Single-Sign On process. If both the mechanisms are configured, the Policy File mechanism is used. If the Policy file does not work, then CA Service Desk Manager Administrator credentials are used. If neither of these are successful, then the CA Service Desk Manager login screen is displayed on clicking the respective hyperlink in CA APM. If the CA APM user does not have valid access rights (role /group) in CA Service Desk Manager, the Single Sign-On login screen is displayed on clicking the CA Service Desk Manager links on the CA APM page

Use the CA Service Desk Manager Administrator Credentials

The CA Service Desk Manager admin credentials are used from CA APM to login to CA Service Desk Manager through the CA Service Desk Manager Web Services.

Follow these steps:

1. Log in to CA APM as an Administrator. Default user name is *uapmadmin*.
2. Click Administration, System Configuration, Service Desk Manager.
3. Enter the complete URL for CA Service Desk Manager SOAP Web Services in the following format:

   ```
   http://<ServiceDeskHostName>:<PortNum>/axis/services/USD_R11_WebService
   ```

4. Enter the CA Service Desk Manager Administrator login user name and password.
5. Click Save.

Note: Do not perform IISReset on the CA APM Web Server or CA APM Application Server.

Use the Web Service Access Policy File

You create the Access Policy file in CA Service Desk Manager and then use this file in CA APM. The Access Policy file contains encrypted policy details that are assigned to a CA Service Desk Manager user who has access to various capabilities in the CA SDM application.

Follow these steps:

1. Log in to the CA Service Desk Manager as an Administrator. Use the Administration tab to perform the following tasks:
   a. Create the Web Services Access Policy using the SOAP Web Services Policy option. Complete the following:
      i. Assign a name. The default name and code are CASM_POLICY; however, you can use any name as per your requirements.

ii. Assign a proxy user to this policy.

> **Note:** This proxy user must have administrative access to CA Service Desk Manager.

iii. Verify that the Allow Impersonate property of CA Service Desk Manager is set to Yes.
CA Service Desk Manager checks the access type of the CA APM user to be impersonated against the access type of the proxy user of the policy. If the access level of the CA APM user access type is less than or equal to the grant level of the proxy user access type, CA SDM replaces the CA APM user with the proxy user.

b. Generate the policy key file with the help of pdm_pki tool for the Web Services policy that you created.
In the Service Desk environment, open the Command Prompt and enter:

```
C:\>pdm_pki  - p CASM_POLICY  - f
```

The policy file CASM_POLICY.p12 is generated in the same folder.
The default/recommended name is CASM_POLICY.p12, but you can use any name as per your requirement.

c. Verify that the HashKey property is set to Yes in the newly created Web Services access policy. The system typically configures this setting automatically when you generate the policy key file.

d. Copy and save the policy key file to the CA APM default installation directory of the CA APM Web Server.

```
C:\Program Files (x86)\CA\ITAM
```

> **Note:** If you are using application clustering, copy the policy key file to the CA APM installation directory of every CA APM Webserver Component cluster node. If you re-configure the Policy in CA SDM, then you must re-generate the policy file and copy it to CA APM Web Server installed directory.

2. Log in to CA APM as an Administrator.
Default:*uapmadmin*.

3. Click Administration, System Configuration, Service Desk Manager.

4. Enter the complete URL for CA Service Desk Manager SOAP Web Services in the following format:

```
http://<ServiceDeskHostName>:<PortNum>/axis/services/USD_R11_WebService.
```

5. Copy the CA Service Desk Manager SOAP Policy file from CA Service Desk Manager Server to the CA APM web server installation folder. Default installation directory :

   ```
   C:\Program Files (x86)\CA\ITAM
   ```

6. Enter the file name of CA Service Desk Manager policy file that is copied on the CA APM Web server component installation folder.

7. Enter the CA Service Desk Manager policy code that is the policy name as configured in the CA Service Desk Manager Administration SOAP Web Services policy configuration page.

8. Click Save.

Note: Do not perform IISReset on the CA APM Web Server or CA APM Application Server.

Verify Single Sign-On

To verify that Single Sign-On from CA APM to CA Service Desk Manager has been enabled, click on any *one* of the following CA Service Desk Manager hyperlinks in the CA APM page:

- Log in to CA APM, Asset Details page and click on the CA Service Desk Manager link on the top
- Click Asset Relationships (menu on the left), CA Service Desk Manager Tickets links. A Criteria and Results page with Service Desk Ticket ID Column values in hyperlink is displayed in the results section. The hyperlinks are the entry point to CA SDM and display ticket details after you have successfully logged into CA SDM.
- Click on the Launch CA Service Desk Manager link in the Asset Viewer page. This launches the CA Service Desk Manager application.

View the Contact Update Details

You can view the contact update details for existing or new assets (known as configuration items in CA Service Desk Manager) in the following ways:

- Contact Update Details for existing Contacts in CA APM
  Ensure that you have enabled Single Sign-On from CA APM to CA Service Desk Manager (see page 3251) for existing contact details to be updated and reflected in CA Service Desk Manager Contact's Quick Profile.
- Contact Update Details for new Assets in CA APM
  In this release, if you have integrated CA APM and CA Service Desk Manager, new Assets that are created have the Contact details automatically saved and reflected in CA Service Desk Manager Contact's Quick Profile.

Launch CA Asset Portfolio Management in Context From CA Service Desk Manager

To launch CA APM in context from CA SDM, you need to add a Management Data Repository (MDR) in CA SDM to point to the proper CA APM URL.

Follow these steps:

1. Create an MDR in CA SDM with the following properties:
    a. Button Name: CA APM
    b. MDR Name: CA APM
    c. MDR Class: GLOBAL
    d. Hostname: CA APM Server Name
    e. Path: ITAM/Pages/Asset.aspx
    f. Parameters: assetid={federated_asset_id}
2. Click the CA APM button.
   The corresponding asset record opens in CA APM.

Integrate CA Service Catalog with CA Service Desk Manager Manually

Important! Review the following section only if you want to manually integrate CA Service Catalog with CA Service Desk Manager when the automatic integration between the two has failed.

CA Service Catalog integration with CA Service Desk Manager is achieved through catalog request fulfillment, which can be configured to automatically open CA Service Desk Manager requests or change orders.

If you are integrating CA Service Catalog and CA Asset Portfolio Management, the associated assets become configuration items on the related change order. The CA Service Desk Manager request and change orders can be viewed in the CA Service Catalog request's Related Tickets column.

Using the integration with CA Service Desk Manager, when a user requests a service from the catalog and it is approved, the fulfillment process could include identifying the correct existing asset and a CA Service Desk Manager change order could be opened assigning a configuration and delivery task to a technician for the asset.

Finally, you can also integrate CA Service Catalog and CA Service Desk Manager by configuring them to use the same common multi-tenant administration.

Set up the CA Service Catalog - CA Service Desk Manager Integration

The major tasks to integrate CA Service Catalog and CA Service Desk Manager follow. These tasks are explained in detail in the sections that follow.

1. Verify the Prerequisites for CA Service Catalog - CA Service Desk Manager Integration (see page 3256)

2. Understand the Key Terms (see page 3257)

3. Configure communication between CA Service Catalog and CA Service Desk Manager by ensuring that a CA Service Desk Manager primary server is properly defined to CA Service Catalog.
   A CA Service Desk Manager primary server is always required to view or open tickets or change orders. To configure CA Service Catalog so that a user can view a CA Service Desk Manager ticket (change order or request) while viewing a CA Service Catalog request, define the CA Service Desk Manager host specified when you select Administration, Configuration, Service Desk.
   In those configuration options, you must also update configuration details for the CA Service Desk Manager primary server.

4. You can optionally bypass user login by configuring CA Service Catalog and the CA products with which it integrates to use single sign-on.
   To configure CA Service Desk Manager to use single sign-on, configure it to use either CA SiteMinder or NTLM authentication on Windows.
   Similarly, to configure CA Service Catalog to use single sign-on, configure it to use either CA SiteMinder (see page 3425) or NTLM authentication on Windows.

5. (Optional) Configure the integrating products to open CA Service Desk Manager change orders during request fulfillment (see page 3258).

6. (Optional) Configure the integrating products to open CA Service Desk Manager service requests during request fulfillment.

7. (Optional) Synchronize notes and attachments (see page 3260).

Step 1 - Verify the Prerequisites for CA Service Catalog - CA Service Desk Manager Integration

To enable the integration between CA Service Desk Manager and CA Service Catalog, meet the following prerequisites:

- You must be familiar with the basic functions and administration of CA Service Desk Manager and CA Service Catalog.

> **Important!** Ensure that CA Service Catalog and CA Service Desk Manager share the same installation of the MDB, CA EEM, and CA Process Automation (if you are using CA Process Automation).

- Both CA Service Catalog and CA Service Desk Manager must be installed, configured, and running. Verify that CA Service Desk Manager has the latest service packs and patches applied.

- If you are using CA Process Automation as the process automation tool for CA Service Catalog and CA Service Desk Manager, verify that you:

  - Install and configure CA Process Automation.
    Verify that CA Process Automation has the latest service packs and patches applied.

  - Install and configure a CA Process Automation-CA Service Desk Manager connector on the CA Process Automation domain orchestrator computer. For more information, see your CA Process Automation administrator.

  - Integrate CA Service Catalog with CA Process Automation Manually (see page 3305). If your implementation of CA Service Desk Manager uses CA Process Automation and the ITIL content pack, review the Pre-Built CA Process Automation Workflows (https://wiki.ca.com/display/CASM1401/Pre-Built+CA+Process+Automation+Workflows) section.

  - Integrate CA Service Desk Manager with CA Process Automation manually (see page 3281).

Step 2 - Understand the Key Terms

This section describes several key terms that you should know when implementing an integration between CA Service Desk Manager and CA Service Catalog. In CA Service Desk Manager, requests, change orders, and related items are the types of tickets that you can open. CA Service Desk Manager defines requests, change orders, and related terms from both an ITIL and non-ITIL perspective.

For a CA Service Desk Manager customer who is *not* running ITIL, the possible ticket types to open up are as follows:

- Requests are requests for service from internal customers, or in the non-ITIL case could also represent a failure.

- Issues are same as the above except they are meant for external customers.

- Change orders are a request for some type of change to the environment.

For a CA Service Desk Manager customer who *is* running ITIL, the possible ticket types to open up are as follows:

- Requests are requests for service for internal customers.

- Issues are requests for service from external customers.

- Change orders are a request for some type of change to the environment.

- Incident is a disruption in service, meant to be restored as quickly as possible.

- Problem is for getting to the root cause.

The following is a typical scenario to distinguish between these ticket types on an ITIL installation:

1. An end user opens up an incident with the helpdesk because of problems connecting to email.

2. At the same time, other end users also open up incidents complaining of the same.

3. To restore service as quickly as possible, the email server is rebooted.
   End users can now connect to email. The incident(s) is resolved. Although rebooting the email server got the end users up and running, we still need to determine and fix the root cause. From here a problem is opened and attached to the incident(s) for additional research.

After research, the root cause looks to be that there is not enough RAM on the email server, so a change order is opened for the proper approvals to go through to add the additional RAM, this change order is then linked to the problem.

Step 3 - Open Change Orders During Request Fulfillment

During the fulfillment phase of the request life cycle, CA Service Catalog can open a CA Service Desk Manager change order. Be careful when activating rules to understand the full implications of your changes. For more information about the CA Service Catalog request life cycle, see the section Request Management from an Administrator Perspective (see page 2115).

To configure CA Service Desk Manager so that CA Service Catalog request fulfillment can open CA Service Desk Manager change orders, complete the following tasks:

1. If you are using CA Process Automation, update CA Process Automation-related settings (see page 3258).

2. Enable rule actions (see page 3259).

Update CA Process Automation Settings

Update these CA Process Automation-related settings to complete the process of configuring CA Process Automation to support the opening of change orders in CA Service Desk Manager during request fulfillment.

Follow these steps:

1. In CA Process Automation, perform these steps:

   a. Access the Service Desk SRF folder (CA SDM/SRF).

   b. Edit the HWSW_FilledFromInventory SRF.

   c. Add the <chgcat> tag to this SRF.

   This step updates the SRF to process change orders in CA Service Desk Manager.

2. In CA Process Automation, perform these steps:

   a. Click Configuration, Domain, Modules, and click Lock.

   b. Double click Edit CA ServiceDesk Module.

c. Enter the ServiceDeskWebService URL, for example, http://hyderabad129:8080/axis/services/USD_R11_WebService.

d. Enter the user name and password of the CA Service Desk Manager administrator.

e. Save and click Unlock.

3. In CA Service Desk Manager, perform these steps:

a. Select Options Manager, Change order Manager, Category_Defaults.

b. Install the Category_Defaults option.

c. Restart CA Service Desk Manager.

This step updates CA Service Desk Manager to process change orders from CA Service Catalog according to your specifications.

You have updated the CA Process Automation-related settings.

Enable Rule Actions

To cause CA Service Catalog to open a CA Service Desk Manager change order during request fulfillment, you must enable several rule actions that are disabled by default.

Follow these steps:

1. Select **Administration**, **Events-Rules-Actions**.

2. Click the Event Type named **Request/Subscription Item Change**.

3. Click the rule named **When Category is Hardware and Status is Filled from Inventory**.
The list shows the CA Process Automation actions that you can use with this rule. Use the remaining steps as a model to modify your start request forms (SRFs) and processes.

4. To enable the CA Service Desk Manager change orders, disable the **Launch FilledFromInventory SRF for Hardware** action and enable the **Launch HWSWFilledFromInv_SDM SRF** action.

a. Click the Edit icon for the action named **Launch FilledFromInventory SRF for Hardware** .

b. Select **Disabled** from the **Status** drop-down list and click OK.

c. Click the Edit icon for the action named **Launch HWSWFilledFromInv_SDM SRF**.

d. Select **Enabled** from the **Status** drop-down list and click OK.

The Rule Action screen is displayed showing the **Launch FilledFromInventory SRF for Hardware** action disabled and the **Launch HWSWFilledFromInv_SDM SRF** action enabled.

5. Repeat the previous steps for the rule named **When Category is Software and Status is Filled from Inventory**.

Activate all rules (see page 562) except **When Status is Pending Fulfillment** for the entire complex request life cycle involving CA Service Desk Manager to work correctly.

Step 4 - Synchronize Notes and Attachments

If you have configured CA Service Catalog to create a ticket (change order or incident) in CA Service Desk Manager when a catalog user submits a request for certain services, each ticket is associated with a specific service option in the requested service. You can enhance the integration by synchronizing notes and attachments to be copied from a service option its related ticket. You can specify this synchronization to occur both before and after the ticket is created. This synchronization helps provide the latest information about the request to the CA Service Desk Manager staff (for example, the analysts) who process the related ticket.

Follow these steps:

1. Enable the CA SDM options, as follows:

    a. Log in to the CA SDM web UI from the following server, depending on your CA SDM configuration:
    Conventional: Primary server
    Advanced availability: Background server

    b. Select Options Manager, CA Service Catalog from the Administration tab.

    c. To enable the integration, install the following options:
    casc_aty_sync

    Specifies the type of activity logs to be synchronized from CA SDM to CA Service Catalog. If this field is left blank, Log Comment activity logs are synchronized. To synchronize other activity log types, (such as, Escalate, Update Status) enter the respective log type codes, separated by comma.

    casc_endpoint

    Specifies the CA Service Catalog Web Services URL.

    Format: http://<CA_Service_Catalog_hostname>:<CA_Service_Catalog_portnum>/usm/services.

    (Optional) **casc_session_timeout**

    Specifies the time in minutes for which the CA Service Catalog web services session will be cached.

    Range: 20 to 60 mins.

    casc_user

Specifies the CA Service Catalog administrator username that is responsible for making the web service calls to CA Service Catalog. This user must exist in EEM against which CA SDM is configured.

casc_user_password

Specifies the password of the CA Service Catalog user as entered in the casc_user option.

(Optional) **casc_ws_retry**

Specifies the number of retries to synchronize a CA SDM ticket update (activity logs/ attachments/status) with CA Service Catalog, if there is a failure. Enter -1 to try indefinitely, until the synchronization succeeds. As a system administrator you can define the time interval after which you want the failed ticket update to be retried again.

Run the following command to define the time interval:

```
pdm_options_mgr -c -a pdm_option.inst -a option.inst -s NX_CASC_RETRY_INTERVAL -
v [time interval in minutes]
```

By default this time interval is set to 15 minutes. If you do not set any value or provide a non-numeric value to this variable, the failed update is retried according to the default time interval (15 mins.).

Range: -1 to 50

casc_integrated

Enables the self-service integration.

Important! Restart CA SDM services for the options to work.

The options are installed successfully.

2. From CA Service Catalog, click the Event Type named Request/Subscription Item Change, and proceed as follows:

    a. Click the rule named When Category is Hardware and Status is Filled from Inventory.

    b. Select the action named Launch HWSWFilledFromInv_SDM SRF and click the Disable button on the Actions bar.
    This step disables the default fulfillment action, which does *not* support the synchronization of notes and attachments.

    c. Select the action named Launch HWSWFilledFromInv_SDM_SYNC SRF and click the Enable button on the Actions bar.
    This action synchronizes both notes and attachments between service options and tickets *before* the ticket is created.

d. Click Done.
You return to the Event Details page.

3. Perform these actions, using the previous step as a model:

   a. Open the Document Create Event Type.

   b. Enable the rule named When attachment is added to Service Catalog request.

   c. Enable the action named Launch PAM SRF to sync attachments.

   This action synchronizes attachments between service options and tickets *after* the ticket is created. That is, if a catalog user adds an attachment to a service option after submitting the request, this action passes the attachment to the related ticket.

4. Perform these actions:

   a. Open the Notes Create Event Type.

   b. Enable the rule named When note is added to Service Catalog request.

   c. Enable the action named Launch PAM SRF to sync notes.

   This action synchronizes notes between service options and tickets *after* the ticket is created. That is, if a catalog user adds a note to a service option after submitting the request, this action passes the note to the related ticket.

Integrate CA Service Desk Manager with Common Components Manually

This article contains the following topics:

Integrate CA Service Desk Manager with CA Embedded Entitlements Manager Manually

Complete the following steps if you are not able to integrate CA SDM and CA EEM through the CA Service Management installer:

1. Ensure that you have installed CA EEM (see page 283).

2. Depending on the CA SDM configuration, log in to the following server:

   - Conventional: Primary server

- Advanced availability: Background server

3. Install the following options:

   - **use_eiam_authentication**
     Allows use of EEM authentication when users log in to CA SDM / Knowledge Management and the access type authentication is set to OS.

   - **use_eiam_artifact**
     Allows EEM artifact to be used when users log in to CA SDM / Knowledge Management using URL.

   - **eiam_hostname**
     Specifies the hostname of the server where EEM is running. Required for EEM user name and password or artifact authentication.

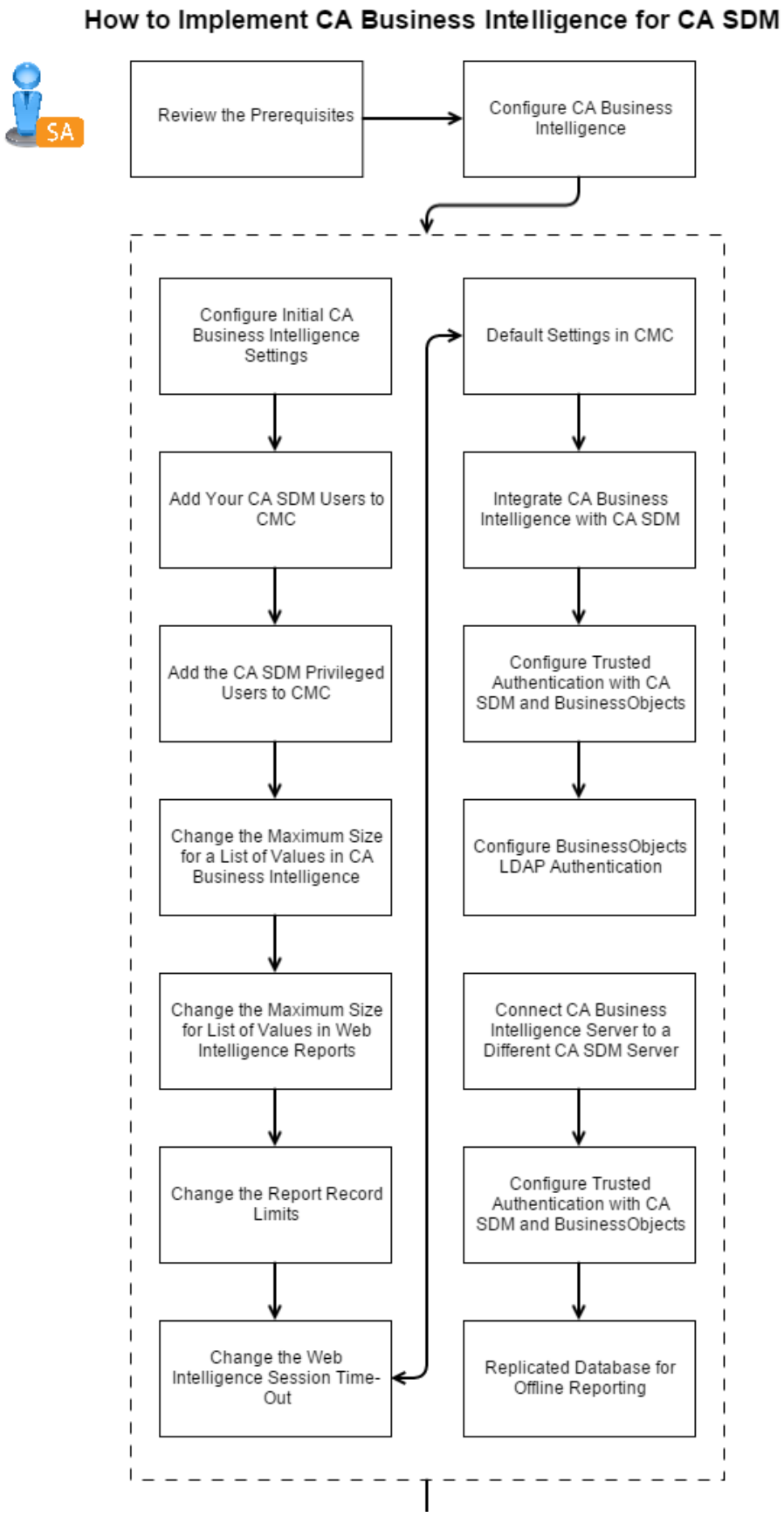
4. Restart CA SDM services (see page 913) and add the CA SDM privileged user in EEM.

At the end of this topic, you have successfully integrated CA EEM with CA SDM.

Integrate CA Service Desk Manager with CA Business Intelligence Manually

CA Business Intelligence is a set of reporting and analytic software that CA SDM uses to present information and support business decisions. CA SDM uses CA Business Intelligence to integrate, analyze, and then present the information through various reporting options. To generate reports from CA SDM, an administrator must install, configure, and integrate CA Business Intelligence with CA SDM.

The following diagram shows how you can implement CA Business Intelligence for CA SDM:


How to Implement CA Business Intelligence for CA SDM
SA
Review the Prerequisites
Configure CA Business Intelligence
Configure Initial CA Business Intelligence Settings
Add Your CA SDM Users to CMC
Add the CA SDM Privileged Users to CMC
Change the Maximum Size for a List of Values in CA Business Intelligence
Change the Maximum Size for List of Values in Web Intelligence Reports
Change the Report Record Limits
Change the Web Intelligence Session Time-Out
Default Settings in CMC
Integrate CA Business Intelligence with CA SDM
Configure Trusted Authentication with CA SDM and BusinessObjects
Configure BusinessObjects LDAP Authentication
Connect CA Business Intelligence Server to a Different CA SDM Server
Configure Trusted Authentication with CA SDM and BusinessObjects
Replicated Database for Offline Reporting

Follow these steps:

Verify Prerequisites

Review the following prerequisites before you plan to implement CA Business Intelligence for CA SDM:

- CA SDM uses CA Business Intelligence 4.1 SP3.
- The installation of CA Business Intelligence requires Central Management Server (CMS) installed on port 6400.
- The CA SDM users requiring access to reports must be added to the CMS Administrator list before using the reports.
- We recommend the SAP BusinessObjects users having an existing installation of BusinessObjects, to install and configure the CA Business Intelligence.

- If you are using Firefox to view the reports, see the CA Business Intelligence documentation (https://docops.ca.com/display/CABI41SP3/Hardware+and+Software+Requirements+for+Installation) to verify the recommended version.
- See the CA Business Intelligence documentation (https://docops.ca.com/display/CABI41SP3/Upgrade+JDK+and+JRE+in+CABI+4.1+SP3) for the supported version of JRE.
- If you are using advanced availability configuration, you have a separate server to install CA Business Intelligence.

Configure CA Business Intelligence

You can configure CA Business Intelligence after a successful installation. You perform mandatory settings to be able to generate reports from CA SDM. You require some mandatory configurations like Adding users and setting security parameters before integrating CA Business Intelligence with CA SDM.

Configure Initial CA Business Intelligence Settings

This step loads the CA SDM universe and reports and creates groups. The step also optionally creates one user for each group and establishes group authorizations.

Note: (For Linux/ UNIX/ AIX/ Solaris) After CA SDM installation, you need to create srvcdesk user in CA Business Intelligence Release 4.1 SP3 and assign it to the following groups manually:

- Change Manager
- Customer Service Manager
- Incident Manager
- Knowledge Analyst
- Knowledge Manager
- Problem Manager
- Service Desk Manager
- Support Automation Admin
- Support Automation Analyst

Follow these steps:

1. Launch the CA Service Management installer.

2. Select **CA Business Intelligence (CA BI) Configuration for CA Service Desk Manager** option from the **Select the required Installer** screen.

   Note: Depending on the server where you run CA Business Intelligence configuration, the configuration performs the following tasks and you need the following DNS:

   - (Server where CA Business Intelligence 4.1 SP3 is only installed) Configuration imports the OOTB Universe, Reports, Groups/Users and installs 32 bit ODBC or 64 bit ODBC Client. Create 32bit/64bit DSNs pointing to the CA SDM machine.
   - (Server where CA Business Intelligence 4.1 SP3 and CA SDM are installed) Configuration imports the OOTB Universe, Reports, Groups/Users and installs 64 bit ODBC Client. Create 64bit DSN pointing to CA SDM machine.
   - (Server where CA Business Intelligence 4.1 SP3 and Client Tools are installed) Configuration imports the OOTB Universe, Reports, Groups/Users and installs 32 bit ODBC/64 bit ODBC Client. Create 32bit/64bit DSNs pointing to CA SDM machine.
   - (Server where CA Business Intelligence 4.1 Client Tools is installed) Configuration installs 32 bit ODBC Client. Create 32bit DSN pointing to CA SDM machine.
   - (Server where CA Business Intelligence 4.1 Client Tools and CA SDM are installed) Configuration does not perform any action. Required 32 bit ODBC Client and DSN are already available.

3. Complete the fields on the CA Business Intelligence configuration UI. If you installed CA Business Intelligence on a different computer than CA SDM, the following fields appear on the CA Business Intelligence configuration:

   Service Desk Primary Server: Provide the host name of the CA SDM server depending on your configuration:

   - **For conventional:** primary server
   - **For advanced availability:** application server

   ODBC Port: Specifies the port number of the CA SDM ODBC driver. **Recommended:** 19987.
   ODBC Install Location: Specifies the custom location for the ODBC installation when it is different from the default location.

4. Verify the CA Business Intelligence configuration.

Configure Failover Settings

This process is only applicable for advanced availability configuration. If multiple application servers are configured, you can configure failover settings. You configure failover to redirect active user sessions to the other application server. You can also configure load balancing between multiple application servers.

Follow these steps:

1. Invoke the command prompt as an administrator.
2. Execute odbcad32.exe from the following location on the CA Business Intelligence server:
   - (For 32but DSN) C:\Windows\System32
   - (For 64bit DSN) C:\Windows\SysWOW64

   The DataDirect OpenAccess SDK ODBC Driver Setup dialog opens
3. Enter the application server details in the **General** tab.
4. Enter the alternate application server details in the **Failover** tab with the following syntax: (Host=AppServer1:Port=19987,Host=AppServer2:Port=19987,..)
5. Select **Load Balancing** to distribute the load among the server. The load is balanced between servers whose details are provided in the **General** tab and the **Failover** tab. The servers are picked randomly.

   Note: Select Force SQL_DRIVER_NOPROMPT for failover or load balancing configuration.

6. Click **Apply** and **OK**.
   You have configured the post configuration settings for the advanced availability configuration.

How to Configure Date Range Values and Join Parameters

After you install CA Business Intelligence, complete the following tasks:

- Configure the date range values so that the date range filters in CA Business Intelligence work correctly.
- Configure the join parameters so that universe outer joins are supported.

Follow these steps:

1. On the computer on which CA Business Intelligence server has been installed, navigate to the following location:

   ```
   C:\Program Files (x86)\CA\SC\CommonReporting4\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\odbc\extensions\qt
   ```

2. Using a text editor, open the odbc.prm file and navigate to the <Configuration> section. Locate the following line to configure date range values:

   ```
   <Parameter Name="USER_INPUT_DATE_FORMAT">{\d 'yyyy-mm-dd'}</Parameter>
   ```

3. Modify the line to include "hh:mm:ss am/pm" as shown in the following example:

   ```
   <Parameter Name="USER_INPUT_DATE_FORMAT">{\d 'yyyy-mm-dd hh:mm:ss am/pm'}<
   /Parameter>
   ```

4. Open odbc.prm from the Program Files (x86)\CA\SC\CommonReporting4\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\odbc directory.

5. Locate the following line to configure join parameters:

   ```
   <Parameter Name="EXT_JOIN">YES</Parameter>
   ```

6. Locate the following and replace NO with YES:

   ```
   <Parameter Name="FULL_EXT_JOIN">YES</Parameter>
   <Parameter Name="LEFT_EXT_JOIN">YES</Parameter>
   <Parameter Name="RIGHT_EXT_JOIN">YES</Parameter>
   ```

7. Update OUTERJOINS_GENERATION" "NO" to "FULL_ODBC" in odbc.prm file located at \extenstions\qt. Add the following three lines after the OUTERJOINS_GENERATION parameter:

   ```
   <Parameter Name="LEFT_OUTER"></Parameter> <Parameter Name="RIGHT_OUTER"><
   /Parameter> <Parameter Name="OUTERJOINS_COMPLEX">Y</Parameter>
   ```

8. Save the odbc.prm file.

9. Restart the Business Objects Enterprise services.
   Date range values and join parameters are configured. Date range filters work with CA Business Intelligence and universe outer joins are supported.

Update the Custom Universe Link

Important! This step applies only if you are migrating from CA Business Intelligence 3.3 to CA Business Intelligence 4.1.

If you have Custom Universe based on the OOTB Universe, refresh the link with CA Service Management 14.1 Universe.

1. Launch Universe Design Tool from the machine where CA Business Intelligence Release 4.1 SP3 client tools are installed.

2. Copy the backup Custom Universe to this machine.

3. Click File, Open.

4. Click File, Parameters.
5. Click the Links Tab
6. From the Name column, click the universe of your product,
   The Change Source button is enabled.
7. Click the Change Source button.
8. Select the location of the universe file.

   Note: The .unv file is typically located in the CA Universes folder.

9. Click Open, OK.
   The universe link is updated.
10. Export the custom universe.

Add Your CA SDM Users to CMC

The CMC is an administrative utility that lets you control users access to Business Intelligence Launch Pad and other BusinessObjects applications. With CMC, you can assign security and user access permissions to folders and documents.

Note: During the configuration phase, an optional check box indicates whether sample users are added to the CMC. If you selected this option, your CMC contains several sample users. You can use these samples as models when defining user permissions and authentication options for your reporting environment. For more information about sample users, see Security and Authorization (see page 3205).

Follow these steps:

1. From the **Start** menu on the **CA Business Intelligence server**, select **CA Business Intelligence 4.1**, **Central Management Console**.
   The **CMC Management Console** page opens.
2. Type the privileged user name and password.
3. Click **Log On**.
   The **CMC Home page** opens.
4. Click **Users and Groups** in the **Organize** section of the CMC home page.The time-out value determines how long the IEnterpriseSession.logon() lasts.
5. Click **Manage, New, New User**.
   The **New User** dialog opens.

6. Select **Enterprise** from **Authentication Type** drop down list from the **CMC** home page. Access the Central Management Console (CMC) to enable Trusted Authentication.

7. Under **Account Name**, specify the CA SDM User ID.

8. On the **Properties** tab, specify your password information and settings as follows:

   - **Password**
     Enter the password and confirm. The maximum password length is 64 characters. This password must be mixed-case, at least six characters long, and cannot contain the word administrator in any form. The password should also contain at least two of the following character types:

     - Uppercase
     - Lowercase
     - Numeric
     - Punctuation

   - **Password never expires**
     Select the check box.

   - **User must change password at next logon**
     This check box is selected by default. If you do not want to force users to change the password the first time they log in, clear the check box.

9. To restrict data access for the reports with data partition or tenancy constraints, select the **Enable Database Credentials for Business Objects Universes** check box. In the fields that display, specify the CA SDM account name and password of the user, and then confirm the password.

10. Click the **Actions, Members Of** to specify the groups that the user must belong to.

11. Click the **Join Group** to view the available groups. By default the user is a member of the Everyone group.

12. In the **Available groups** area, select one or more groups.

13. Click the **>** arrow to add the group(s).

14. Click **OK**.
    The **Members Of** dialog appears and lists the groups in which the user is a member.

Change the Maximum Size for a List of Values in CA Business Intelligence

When you install CA Business Intelligence, the maximum number of values that can be returned in a batch for a list of values in the Crystal reports is set to 5,000 records. For performance reasons, you can change the size so that the list of values is in several batches of this size or less.

Note: For information about improving the performance of the Web Intelligence Report Server, see your BusinessObjects documentation.

Follow these steps:

1. Create the following registry key:

   ```
   HKEY_CURRENT_USER\Software\SAP BusinessObjects\Suite XI 4.0\Crystal Reports\DatabaseOptions\LOV
   ```

   Note: The created registry key overrides the settings of the HKEY_CURRENT_USER\Software\SAP BusinessObjects\Suite XI 4.0\Crystal Reports\DatabaseOptions registry key.

2. Add a string value as **MaxRowsetRecords**.

3. Set the value of MaxRowsetRecords to the maximum number of values that you want for the report. For example, a value of 2000 returns up to 2000 values in the lowest level of a cascading parameter.

   Note: The value zero (Unlimited) does not work with BusinessObjects Enterprise or Crystal Reports Server. If MaxRowsetRecords is set to zero, whenever Crystal Report is accessed from Business Intelligence Launch Pad it takes more time to populate the values. Setting the value to zero displays the maximum list of values.

4. Restart the affected service or application, as required.

Note: These registry keys do not affect the **List of Values** that are returned when a report is based on a Universe.

Change the Maximum Size for a List of Values in Web Intelligence Reports

When you install CA Business Intelligence, the maximum number of values that can be returned in a batch for a list of values in the Web Intelligence reports is set to 50,000 records. For performance reasons, you can change the size so that the list of values is in several batches of this size or less. For information about improving the performance of the Web Intelligence Report Server, see your BusinessObjects documentation.

Follow these steps:

1. Log in to **Central Management Console**.

2. Click **Servers**.
3. Right-click **Web Intelligence Processing Server** and select **Properties**.
4. Increase the value of **Maximum List Of Values Size** (entries).
5. Save and restart the Web Intelligence Processing Server.

> **Note:** Setting large number for **Maximum List Of Values Size** (entries) may affect the performance of Web Intelligence. We recommend to set the appropriate number according to the system performance.

Change the Report Record Limits

When you install CA Business Intelligence, the number of records that the server retrieves from the database when a user runs a query or report in Crystal reports is automatically set to 20,000 records. You can change the setting so users running reports receive the record sets they expect. For complete details about administrative tasks you can complete for the Crystal Reports Page Server, see your BusinessObjects documentation.

Follow these steps:

1. Using BusinessObjects Enterprise, log in to the **Central Management Console**.
2. Navigate to the page displaying the servers.
3. Click **Crystal Reports 2013 Processing Server**.
4. On the **Properties** tab, change the setting for the **Database Records To Read When Previewing or Refreshing a Report** field to either unlimited records, or specify a specific record limit.
5. Click **Apply**.
6. Restart the Crystal Report Page Server.
   The report record limit changes and is used when running reports.

Change the Web Intelligence Session Time-Out

Users have Full Control access to the Web Intelligence application by default.

The Web Intelligence application has a session time-out of 20 minutes by default. Unsaved reports are lost when the session times out and the user must log in again to use the application.

Administrators can modify the connection session time-out value using the Central Management Console (CMC).

Follow these steps:

1. Select **Servers** from the **CMC Home** page.
   The **Servers** window opens.

2. Select **Web Intelligence Processing Server** in the **Server Name** column.

3. Type the appropriate time-out value (number of minutes) in the **Connection Time Out** field.

4. Click **Apply**.
   Your changes take effect after the server is restarted.

5. Click **OK**
   The session time-out value is set.

Default Settings in CMC

Most of the reporting configuration is performed silently during the CA Business Intelligence installation. Reporting configuration involves the following actions:

- Setting up security
- Deploying reports
- Deploying universes
- Deploying program objects
- Configuring Web Intelligence settings

The administrator can log in to the BusinessObjects CMC and modify the default settings at any time. Users are authorized access based on the CA SDM group to which they belong.

Note: For more information about the BusinessObjects CMC, see the CABI documentation (http://wiki.ca.com/CABI).

Integrate CA Business Intelligence With CA SDM

After you install CA Business Intelligence, update the Web Reporting options so CA SDM is properly integrated with CA Business Intelligence.

Follow these steps:

1. On the **Administration** tab, select **Options Manager, Web Report**.
   The Option List appears.

2. Set the correct values to the following **Web Report** options:

   - **bo_server_auth**
     Specifies which type of authentication you want to use for reporting. You can specify the following types of authentication:

- **secEnterprise --** (Default) Specify Enterprise Authentication as your authentication type when you prefer to create distinct accounts and groups in **BusinessObjects for use with CA Business Intelligence**, or when a user hierarchy has not been set up in a Windows NT user database, an LDAP server, or a Windows AD server.

  Note: Before you use the **secEnterprise option**, add your CA SDM report users (see page) to the **BusinessObjects Central Management Console** (CMC). In the CMC, enter the same user names and passwords that are configured in CA SDM.

- **secLDAP --** Specify LDAP Authentication as your authentication type if you have already set up an LDAP directory server and you want to use your LDAP user accounts and groups in **BusinessObjects for use with CA Business Intelligence**.
  When you map LDAP accounts to BusinessObjects, users can access CA Business Intelligence with their LDAP user name and password. This setup eliminates the need to recreate individual user and group accounts within BusinessObjects.

- **secWinAD --** Specify Windows AD Authentication as your authentication type if you are working in a Windows 2000 environment and you want to use your existing Active Directory user accounts and groups in BusinessObjects for use with CA Business Intelligence.

- **secExternal --** Specify **External Authentication** as your authentication type when you integrate the BusinessObjects authentication solution with a third-party authentication solution. For example, using JCIFS with Tomcat. This authentication type requires setting up Trusted Authentication in BusinessObjects to allow users to log in without providing their passwords. For complete details about administrative tasks you can complete for the Crystal Reports Page Server, see your BusinessObjects documentation.

- **bo_server_cms**
  Specifies the name of the Central Management Server (CMS) that maintains a database of information about your BusinessObjects that you use with CA Business Intelligence.
  For the **bo_hostname**, use the hostname of the computer where CA Business Intelligence is installed. The default bo_cms_port is 6400.

- **bo_server_location**
  Specifies the hostname of the computer where CA Business Intelligence is installed. Specify bo_hostname. CA SDM uses this URL for report URLs for requesting reports from the BusinessObjects server. The CMS location is specified by hostname and port. For more information, see the CA Business Intelligence installation documentation (https://wiki.ca.com/display/CABI41SP3/CABI+Installation+on+Windows).

3. Make changes to the options, if any of them have been specified incorrectly.

   a. Click **Save, Refresh**.

   b. The **Options Detail** page is updated with your selection.

   c. Click **Close Window**.

d. Stop and start the service named CA SDM Server.

After confirming the correct web reporting options, you can now set up web-based reports. For more information about setting up web-based reports, see the Web-Based Reports (see page 3201) topic.

How to Configure Trusted Authentication with CA SDM and BusinessObjects

Trusted Authentication lets you use a simple form of Single Sign On when integrating CA SDM and CA Business Intelligence.

Follow these steps:

1. Install and configure CA SDM.
2. Install and configure CA Business Intelligence.
3. Log in to the CMC as Administrator.
4. Access the **Central Management Console** (CMC) to set up Trusted Authentication.
5. Create CA SDM contacts and BusinessObject users.
6. Install the CA SDM web report options and set the **bo_server_auth** option to **Enterprise**. For more information about *bo_server_auth*, see the Web Report Options topic.
7. Cycle the BusinessObjects Apache Tomcat.
8. Cycle the CA SDM server in Windows Services.

Configure Trusted Authentication in CA Business Intelligence

You configure trusted authentication for CA Business Intelligence by first editing the web.xml file.

Follow these steps:

1. Log in to CMC as Administrator and go to the **Authentication management** area.
   The **Enterprise** page appears.
2. At the bottom of the page, select the **Trusted Authentication is enabled** option.
3. Click **New Shared Secret, Download Shared Secret** to download a shared secret. The shared secret is used to create a trusted authentication password.
4. Save the TrustedPrincipal.conf file.
5. Enter a time-out value for your trusted authentication requests.

Note: The time-out value determines how long the CMS waits for the IEnterpriseSession.logon() call from the client application.

6. Click **Update**.
   The trusted authentication is configured.

Configure Trusted Authentication in CA SDM

Configuring Trusted Authentication in CA SDM requires editing the TrustedPrincipal.conf file.

Follow these steps:

1. Open the NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd directory.
2. Replace TrustedPrincipal.conf with the one downloaded from the Central Management Console. For more information, see Configure Trusted Authentication in CA Business Intelligence.
3. (Applicable for advanced availability configuration only) Repeat the steps 1-2 for all configured application servers.
4. Recycle the CA Business Intelligence Tomcat server.
   The trusted authentication in CA SDM is configured.

Note: You must configure the trusted authentication in the CA SDM background server to launch reports from the background server URL.

Configure BusinessObjects LDAP Authentication

When configuring the LDAP authentication, use the fully qualified name (First Name, Last Name) for the LDAP Server Administration Credentials “cn”. Configuring the LDAP authentication allows you to map LDAP attributes to use the end-user logon name.

Important! The user Account Name for BusinessObjects must match the CA SDM contact User ID when configuring LDAP authentication.

Follow these steps:

1. Access the Authentication management area of the Central Management Console (CMC).
2. Double-click **LDAP**.
3. Enter the name and port number of your LDAP hosts in the **Add LDAP host** (hostname:port) field. For example, "myserver:123".
4. Click **Add** and then **OK**.
5. Select **Custom** for the server type from the **LDAP Server Type** list.

6. Follow the prompts in the CMS configuration wizard and complete the configuration.
   The BusinessObjects LDAP authentication is configured. For more information about configuring LDAP Authentication, see this (https://wiki.ca.com/display/CABI41SP3/Integrate+with+Open+LDAP+Directory+Server) topic.

Connect CA Business Intelligence Server to a Different CA SDM Server

This is required to generate reports from another instance of CA SDM installed on a different server.

Follow these steps:

1. Create an ODBC DSN for the CA SDM server (see page).
2. Connect the CA SDM universe to this CA SDM server (see page).

Create an ODBC DSN for the CA SDM Server

Use the ODBC Data Source Administrator to create 32 bit ODBC DSN and 64 bit ODBC DSN for the CA SDM server on CA Business Intelligence server.

Follow these steps:

1. Start the Windows ODBC Data Source Administrator (Data Sources (ODBC)).
2. On the **ODBC Data Source Administrator** form, select the **System DSN** tab, and select **Add**.
3. On the **Create New Data Source** form, select the **DataDirect OpenAccess** driver, and select **Finish**.
4. On the **DataDirect OpenAccess ODBC 32 Setup** form, assign an ODBC Name and select **Advanced**.
   The naming convention to use is casd_hostname. For example, if the hostname of the CA SDM server is MyServer, you would use casd_MyServer.
5. On the **OpenAccess Database Configuration** form, select **Add**.
6. On the **OpenAccess Database Setup** form, enter the following information:
   - **Name** -- Specify casd_hostname.
   - **IP Address** -- Specify the IP address of the CA SDM server.
   - **Port** -- Specify 19987.
   - **Type** -- Select **SQL**.
7. Click **OK**.
8. On the **Open Access Database Configuration** form, select **OK**.

9. On the **DataDirect OpenAccess ODBC 32 Setup** form, select **casd_hostname** from the **Database** drop-down list, and select **OK**.
   The 64 bit DSN is created.

10. Launch odbcad32.exe from C:\Windows\SysWOW64 directory and follow steps 2 - 9 to create 32 bit DSN.
    The 32 bit DSN is created.

Connect the CA SDM Universe to the Server

Use the Universe Design Tool in BusinessObjects Enterprise to establish a connection.

Follow these steps:

1. Log in to the server where the CA Business Intelligence Client Components are installed.

2. From the **Start** menu, browse to **CA, CA Business Intelligence 4.1 Client Tools, Universe Design Tool**.

3. Log in to the **Universe Design Tool** with the following credentials.

   - **System** -- Specify the hostname of the server where CA Business Intelligence was installed.
   - **User name** -- Specify the name of the CA Business Intelligence administrative user (typically Administrator).
   - **Password** -- Specify the password of the CA Business Intelligence administrative user.
   - **Authentication** -- Select **Enterprise**.

   The **Universe Design Tool** window appears.

4. Click **File, Import**.
   The **Import Universe** dialog appears.

5. Select the **CA Universes** folder from the drop-down list and then select the CA SDM universe and click **OK**.

   Note: If you are using Universe Design Tool for the first time, you may first need to select **Browse** to select the **CA Universes** folder.

6. Click **OK** to the **Universe successfully imported** message.
   The U**niverse** window appears.

7. Select **File, Parameters**.
   The **Universe Parameters** dialog appears.

8. On the **Definition** tab, click **Edit**.
   The **Login Parameters** dialog appears.

9. Select **Edit**.

10. Select the **ODBC DSN** you created (casd_hostname) from the **Data source name** drop-down list. Specify the CA SDM Privileged User and Password for **User name** and **Password**.

11. Click **Next, Test Connection**, and step through the **Universe Connection** dialogs that appear.

12. Click **OK** to finish.

13. Select **File, Export**
    The **Export Universe** dialog appears.

14. Select **CA Universes** from the **Domain** drop-down list.

15. Select **Everyone** from the **Groups** list.

16. Click **OK**.
    The universe is exported and the connection to the server is established.

> **Note:** If CA Business Intelligence server and Client Tools are installed on separate computers then create 32 bit DSN on the client computer. For more information, see the **Create an ODBC DSN for the CA SDM Server** topic.

Replicated Database for Offline Reporting

To manage potential performance issues that may affect the reporting components that are installed with CA SDM, create a replicated database for offline reporting purposes. For more information about creating a replicated database for offline reporting, see the sample documentation and scripts delivered in the NX_ROOT\samples\reporting directory.

Verify Reports

To ensure that the reports are generated without any problem, verify the CA Business Intelligence configuration.

Follow these steps:

1. Click the **Reports** tab.
   The **Web Report** page opens.

2. Click **BI Launchpad**.
   The Business Objects Business Intelligence Launch Pad window opens.

3. Click the **Documents** link.

4. Expand **Folders, Public Folders, CA Reports, CA Service Management, CA Service Desk**.

5. Select the **Asset** folder in the left pane.

6. Double-click the **Asset List** report.
   The report returns with zero or more Results Found. CA Business Intelligence is now configured for CA SDM.

Integrate CA Service Desk Manager with CA Process Automation Manually

CA Process Automation is a stand-alone CA product with features for automating and tracking hardware and software administration tasks in enterprise IT environments. CA Process Automation automates tasks and manages user interactions, such as approvals and notifications for compliance and accuracy within production environments.

When you integrate CA SDM and CA Process Automation, you can leverage the benefits of CA Process Automation workflow capabilities from key points within CA SDM. An effective integration between CA SDM and CA Process Automation requires you to understand both products.

CA Process Automation Components

CA Process Automation offers multiple capabilities and structures that facilitate a wide range of activities as part of CA Process Automation process management. For the integration with CA SDM, however, only the following CA Process Automation components are critical for CA Process Automation integration:

- **Process Definition --** Identifies a collective series of tasks, steps, and conditions that are structured in a specific order to be initiated, and completed by various individuals or parties. This component is the central building block of all CA Process Automation content.

- **Start Request Form --** An object containing descriptive information for end users. The Start Request Form presents a process definition to users while hiding the technical details of the process definition.

- **Keywords --** A list of pre-defined words or phrases to attach to Start Request Forms.

- **Automation Library --** An area within CA Process Automation that stores and shows Process Definitions and Start Request Forms.

- **Library Path or Reference Path --** A folder structure that organizes and describes Process Definitions and Start Request Forms within the automation library.

- **Process Instance --** An active entity that executes the rules that are defined in a process definition. The process instance progresses until the process definition state is complete.

- **Process Instance Log Messages --** A configurable, running record that details the progression of activities of the process instance. Log message categories are useful to the CA SDM integration with CA Process Automation.

Note: The scope of the definitions of CA Process Automation components is limited to the usage within CA SDM. For information about CA Process Automation components and capabilities, see the CA Process Automation documentation.

Complete the following steps only if you are not able to integrate CA Process Automation and CA SDM through the CA Service Management installer:

Verify the Integration Requirements

You can integrate CA Process Automation and CA SDM to coexist on a single server when the server architecture supports both products. When CA Process Automation or CA SDM components cannot integrate on the same server, consider installing each product on separate servers.

Important! If CA Process Automation is configured in FIPS mode, you must also configure EEM server and EEM SDK in FIPS mode. For more information about configuring the EEM SDK in FIPS mode, see the CA EEM documentation.

Before you configure CA Process Automation and CA SDM, confirm that both products are installed and are working independently.

Follow these steps:

1. Open a browser on the server that hosts CA SDM and verify that a CA Process Automation user can log in to CA Process Automation. Change the place holders to match the target CA Process Automation installation.

   ```
   http(s)://<server>:CA Portal/itpam
   ```

2. Enter the following URL. Change the place holders to match the target CA Process Automation installation.

   ```
   http(s)://<server>:CA Portal/itpam/JNLPRequestProcessor?processType=startUI
   ```

   The CA Process Automation product is accessible from the CA SDM host.

Install the CA Process Automation Workflow Options

When you install the CA Process Automation Workflow options, you specify connectivity between CA SDM and CA Process Automation. If you are using CA EEM for authentication, you also specify the CA EEM host name.

Follow these steps:

1. On the Administration Tab, select Options Manager, CA IT PAM Workflow.
   The Option List appears.

2. Right-click the name of each option and select Edit from the context menu. Install the following options:

   - **caextwf_eem_hostname**
     Specifies the name of the CA EEM server. For example, *<wf_hostname> (http://pam.host.com/)* identifies the authentication host. You install caextwf_eem_hostname only if you configured CA Process Automation to use CA EEM as an authentication server. CA SDM uses this value to transform a user name and password into a CA EEM token. Then, the user name and password do not pass in plain text over HTTP.

     Note: If the CA Process Automation installation is not using CA EEM, do not place a value in the caextwf_eem_hostname option, and do not install the caextwf_eem_hostname. Placing a false value or installing caextwf_eem_hostname when it is not necessary causes the integration to fail.

   - **caextwf_endpoint**
     Specifies the URL that points to the CA Process Automation web services by including the CA Process Automation host name, port, and the mandatory /itpam/soap path. For example, http://<wf_hostname>:<wf_tomcat_port>/itpam/soap identifies the endpoint. If your implementation uses CA EEM, installing the caextwf_eem_hostname option is required for the integration between CA Process Automation and CA SDM to operate properly.

   - **caextwf_log_categories**
     Specifies a comma-separated list of CA Process Automation process instance log category names to appear on the CA SDM Request, Change Order, and Issue Workflow Tasks tab. For example, *Operator,Response,MyOwnCategory* supplies three log categories.
     You install caextwf_log_categories based on business decisions from the CA SDM and CA Process Automation process design personnel. This option adjusts the default data that appears on the Workflow Tasks tab for requests, change orders, and issues.
     When you install the caextwf_log_categories option, all CA Process Automation process instance log messages from the Process category and the categories that you specify appear on the Workflow Tasks tab. When you do not install caextwf_log_categories, only the CA Process Automation process instance log messages from the Process category appear on the Workflow Tasks tab.

   - **caextwf_processdisplay_url**
     Specifies how to launch a graphical snapshot of a CA Process Automation process instance by supplying the host name and the mandatory /itpam/Web.jsp?page=runtimeeditor&ROID path. For example, http://<wf_hostname>:<wf_tomcat_port>/itpam/Web.jsp?page=runtimeeditor&ROID= launches a snapshot of a process instance. On the Workflow Tasks tab of a request, change order or issue, the user selects View Process to see the snapshot.
     Installing the caextwf_processdisplay_url option is required for the integration between CA Process Automation and CA SDM to operate appropriately.

- **caextwf_worklist_url**
  Specifies the process instance path by supplying the host name and the mandatory /itpam?page=tasklist path. For example, http://<wf_hostname>:<wf_tomcat_port> /itpam?page=tasklist enables CA SDM users to see a list of CA Process Automation process instances that require attention. The list appears in CA Process Automation when the CA SDM user selects a link associated with any listed task in the request, change order, or issue Workflow Tasks tab.
  Installing the caextwf_worklist_url option is required for the integration between CA Process Automation and CA SDM to operate properly.

- **caextwf_ws_password**
  Specifies the administrative password associated with the CA Process Automation user name from the caextwf_ws_user option. CA SDM uses the user name and password to access the CA Process Automation web service functions to perform integration activities such as selecting start request forms, process definition information, and process instance information.
  Installing the caextwf_ws_password option is required for the integration between CA Process Automation and CA SDM. The password and user name that you specify requires the appropriate access to CA Process Automation. However, it is not necessary the CA Process Automation user name and password to exist within the CA SDM contact records.

- **caextwf_ws_user**
  Specifies the CA Process Automation administrative user name associated with the CA Process Automation user name from the caextwf_ws_password option. CA SDM uses the user name and password to access the CA Process Automation web service functions. These services perform integration activities such as selecting start request forms, selecting process definition information, selecting process instance information, or launching process instances.
  Installing the caextwf_ws_user option is required for the integration between CA Process Automation and CA SDM to operate. The user name and password that you specify requires the appropriate access to CA Process Automation. However, it is not necessary the CA Process Automation user name and password to exist within the CA SDM contact records.

- **caextwf_retry_count**
  Specifies the number of times an event is triggered if CA Process Automation is unavailable. CA Process Automation Workflows can be attached to CA SDM tickets (for example,Change Orders) through CA SDM Events and Macros. The attached events are triggered by CA SDM at the specified retry interval duration. During retry, if the CA Process Automation is unavailable, the attached event is marked as Unknown and the process is not executed. CA SDM retry mechanism automatically re-triggers the attached Unknown events when CA Process Automation is unavailable. Default value is 3 and can be set in the range [1 – 20].

- **caextwf_retry_interval**
  Specifies time interval after which the event is again triggered in case CA Process Automation is unavailable.

3. Click Install.

4. Restart the CA SDM service.
   The CA SDM and CA Process Automation can communicate even though there is no process instance data. CA SDM and CA Process Automation are ready for you to create CA Process Automation process definitions and CA Process Automation start request forms.

Set Up SSL Communications with CA Process Automation

For security reasons, CA Process Automation implementers may have chosen to install or reconfigure CA Process Automation to require SSL communications. If CA Process Automation is configured to require SSL communications, integrated applications such as CA SDM require a certificate from the CA Process Automation keystore for communication.

Follow these steps:

1. Configure CA SDM options to use the CA Process Automation HTTPS address.
2. Export the CA Process Automation keystore certificate to a file and copy the file to CA SDM.
3. Load the certificate file into CA SDM using the CA SDM pdm_keystore_mgr utility.
4. If applicable to your CA SDM architecture, update the version control files to deliver the CA SDM keystore to all secondary servers.
5. Restart CA SDM.

Enable Communications When CA Process Automation is SSL Enabled

When CA Process Automation communicates with SSL, configure the CA SDM servers to communicate with CA Process Automation.

To enable communications when CA Process Automation is SSL enabled, do the following tasks:

1. Verify that you can use CA Process Automation in a browser, without launching CA SDM. Record the CA Process Automation URL and use it for reference when you configure the CA Process Automation Workflow options in Options Manager.
2. Log in to CA SDM and install or modify the CA Process Automation Workflow options in Options Manager. For each of the following options, use the syntax *https://server:8443 (https://server:8443/)* instead of http://server:8080 (http://server:8080/) for reaching the SSL enabled CA Process Automation application. If the CA Process Automation installation uses another port instead of the 8443 SSL port, specify the appropriate port number.
   - caextwf_endpoint
   - caextwf_processdisplay_url
   - caextwf_worklist_url

> **Note:** If the values do not match the actual CA Process Automation installation values, CA SDM cannot communicate with CA Process Automation. A runtime error occurs. Verify that the values match the actual CA Process Automation installation values, because the CA Process Automation installer might have selected a different port instead of port 8443.

3. On the CA Process Automation server, locate the KEYSTOREID and itpam.web.keystorealias entries in the following file:

   ```
   C:\Progra~1\ITPAM\server\c2o\.config\OasisConfig.properties
   ```

4. Copy the KEYSTOREID. Be prepared to paste the KEYSTOREID value as the password after you issue the keytool command.

5. On the CA Process Automation server, issue the following keytool command as one line on the command line:

   ```
   C:\Progra~1\ca\sc\jre\1.6.0_00\bin\keytool.exe -keystore C:
   \Progra~1\ITPAM\server\c2o\.config\c2okeystore -export -alias <keystorealias> -
   file itpam.cer
   ```

   The keytool utility prompts you for a password.

6. Paste or type the KEYSTOREID value as the password.
   The keytool utility uses the final parameter (-file itpam.cer) to create a file that is named *itpam.cer*. The *itapm.cer* file contains the necessary certificate information for communications with CA SDM.

7. Move the *itpam.cer* file to one of the following locations on the CA SDM server:

   - (Windows) %NX_ROOT%\bin
   - (UNIX) $NX_ROOT/bin

8. Import the CA Process Automation certificate information into CA SDM by entering the following command:

   ```
   (Windows) pdm_perl %NX_ROOT%\bin\pdm_keystore_mgr.pl -import %NX_ROOT%
   \bin\itpam.cer
   (UNIX) pdm_perl $NX_ROOT/bin/pdm_keystore_mgr.pl -import $NX_ROOT/bin itpam.cer
   ```

   The *pdm_keystore_mgr.pl (http://pdm_keystore_mgr.pl/)* script generates the keystore file in the following locations:

   - (Windows) %NX_ROOT%\pdmconf\nx.keystore
   - (UNIX) $NX_ROOT/pdmconf/nx.keystore

9. The *nx.keystore* must be delivered to the following CA SDM servers, depending on the CA SDM configuration:

- Conventional:Secondary server.
- Advanced Availability: Application and standby server.

Open the *server_secondary.ver* file from one of the following locations:

- (Windows) %NX_ROOT%\site\server_secondary.ver
- (UNIX) $NX_ROOT/site/server_secondary.ver

10. Modify the *server_secondary.ver* for version control by adding the following information:

```
[SSL_Keystore]
filename = "nx.keystore"
directory = "$NX_ROOT/pdmconf"
component_type = "file"
O_mode = "RW"
g_mode = "RW"
w_mode = "RW"
file_ctl
```

11. Restart CA SDM.
    The CA SDM server can communicate with the SSL enabled CA Process Automation application.

Configure the Integration

Both CA Process Automation and CA SDM, as stand-alone products, have individual requirements for authentication and authorization. To support a unified Service Oriented Architecture (SOA) strategy, you can configure both products to use CA EEM for authentication.

When you install CA Process Automation with CA EEM as the authentication server, the installer creates several policies and eight essential entities by default:

- Four application users: pamadmin, pamuser, pamproduser, and pamdesigner.
- Four application groups: PAMAdmins, PAMUsers, Designers, and Production Users.

CA SDM users who also use CA Process Automation can be divided between PAMAdmins and PAMUsers as follows:

- CA SDM analysts must be members of PAMUsers when their duties entail:
  - Approving, rejecting, or otherwise responding to CA Process Automation Interaction Request Forms.
  - Listing CA Process Automation process instances assigned to the user.
  - Viewing the graphical display by clicking the View Process button of CA Process Automation's process status screen. The CA Process Automation PAMUsers group requires an additional CA Process Automation policy to grant access the graphic.
- CA SDM analysts are members of PAMAdmins when their duties entail:

- Creating and checking in CA Process Automation process definitions and/or start request forms.
- Terminating process instances directly within CA Process Automation. Terminating process instances are an administrative exception to expected integration procedures.
- Delegating CA Process Automation process instance tasks.
- If the user is the user name defined in CA SDM Options Manager.

- CA SDM users require no access to CA Process Automation when their duties entail:
  - Creating requests, change orders, and issues that launch CA Process Automation instances.
  - Reviewing the Workflow tab which shows CA Process Automation process instance status and task information.
  - Changing the status of a request, change order, or issue which causes the termination of a CA Process Automation process (such as canceling a change order).
  - Selecting a CA Process Automation process definition on a CA SDM request area, change category, issue category.

Finalize the Integration

If you have CA SDM and CA Process Automation integration, set up the Single Sign-On (SSO).

Follow these steps:

1. Verify that the following requirements have been met:
   - CA SDM and CA Process Automation are configured to use the same CA EEM installation.
   - The user that logs in to CA SDM is also a user in CA Process Automation.
   - When CA EEM uses the internal database as a user store, the users must have either global permissions or belong to the same folder. Otherwise, if CA EEM references an external user store like an external directory or CA Siteminder, the users must be of the same store to access single sign-on.
2. Install CA EEM from CA Service Management installation (see page 293) or use any existing CA EEM install (for example, CA EEM for CA Process Automation).
3. On the CA SDM Administration tab, install the following options from under the Options Manager, Security folder:
   - eiam_hostname
   - use_eiam_authentication

> **Note:** You do not need to install the option caextwf_eem_hostname under Options Manager, CA Process Automation folder. But if you do install it, the value must be the same as eiam_hostname option.

4. Restart CA SDM.

5. To create a user in CA Process Automation, perform the following:

   a. Log in to CA EEM using the CA Process Automation application context using the EiamAdmin userid or any other administration user.

   b. Select the Manage Identities tab and click the icon next to the Users folder.

   c. On the New User page, the Name field at the top is the userid that must match the userid in the CA SDM contact table.

   d. Click the Add Application User Details button and complete the following:

      - Add any of the groups that are listed. Add at least one of these groups in order to be able to log in to CA Process Automation.

      - Complete the New User fields, such as First Name, Last Name, Display, and Password.

6. Create a user in the CA SDM contact table with the same userid. Verify that the Access Type Validation Type field for the user is set to CA EEM.
   You can log in to CA EEM and CA SDM with this user and the password specified in CA EEM.

CA Process Automation Integration with CA SDM at Run Time

When you enable the integration, CA SDM users experience the following:

- On a new Request, Change Order, or Issue, a CA Process Automation process instance initiates based on the ticket category or area. Summary information immediately appears on the Workflow Tasks tab.

- When a Request Area, Change Category, or Issue Category changes, an attached CA Process Automation process instance terminates and a new process instance initiates.

- When a CA SDM user attempts to close a Request, Change Order, or Issue where the CA Process Automation process instance is not yet complete, the user cannot close the ticket. Instead, the user must first cancel the ticket. The Cancel status terminates the CA Process Automation process instance before the ticket closes.

- When a user wants to understand the state of the process instance without navigating away from the ticket, the user can click the ticket Workflow Tasks tab. The Workflow Tasks tab shows the process instance start date, end date, current state, and a current audit trail of messages indicating the path of the process instance.

- When a user wants to see the current path of the process instance relative to the entire process, the user selects the View Process button on the Workflow Tasks tab. The View Process button launches a graphical snapshot of the entire process instance, and shows the current path.

- When a user wants to see CA Process Automation interaction request forms that are waiting for user action, the user can select any entry in the Workflow Tasks tab. The Workflow Tasks tab contains an audit trail of process instance messages that appear on the CA Process Automation task list.

Note: When a user selects the CA SDM View Process button or CA Process Automation process instance messages, the system prompts for a CA Process Automation user name and password for a single browser session. After the initial prompt, the system does not prompt the user again until the CA SDM browser closes.

How to Create a Process Definition

When you create the process definition, you populate CA Process Automation with content to appear in CA SDM. You use the CA Process Automation graphical process designer to create, test, and check in a process definition. From CA SDM, you can also create macros to initiate CA Process Automation processes. To create a process definition in CA Process Automation, perform the following:

Follow these steps:

1. Log in to the CA Process Automation client as an administrative user.

2. Use the CA Process Automation graphical process designer to create, test, and check in a process definition. When you work with the process definition, use the instructions in the CA Process Automation user documentation.

Note: If you fail to check in the process definition before attempting to use it, the workflow cannot operate properly in CA SDM.

The following process definition items are available in CA SDM:

- **Process Name**
  Appears on the Request Area, Change Category, and Issue Detail page. The process name also appears on the Workflow Tasks tab of a ticket. The process name describes the process definition to CA SDM to Analysts and other users who manage tickets.

- **Process Reference Path**
  Appears on the Request Area, Change Category, and Issue Detail pages. The Process Reference Path also appears on the ticket Workflow Tasks tab. The Process Reference

Path can be useful to describe the purpose of the process to end users. For example, " /Processes/Approval" is not helpful. Instead, a reference path like "/Office Supplies /Approvals/Over-200-CA SDM" describes the workflow to manage orders that exceed $200 US dollars.

- **Process Log Messages**
  Appears on the CA SDM ticket Workflow Tasks tab. By default, a record of activities stores with the process instance. Process log messages have the Process category. A process designer can create custom messages to appear on the Workflow Tasks tab of a CA SDM ticket.

Create a Start Request Form

When you create a Start Request Form, you associate it with the process definition and check it in. You include the appropriate keywords in the Start Request Form properties. If the appropriate keyword is missing from the Start Request Form properties, the Start Request Form and its associated process definition fail to appear in CA SDM.

Follow these steps:

1. Log in to the CA Process Automation client as an administrative user.
2. Open the CA Process Automation Library and navigate to the path Start Request Form.
   The Start Request Form appears in the right pane of CA Process Automation library.
3. Select the Start Request Form from the list.
   A shortcut menu appears.
4. Select Properties.
   The Library Object Properties page appears.
5. (Optional) Click the General tab and modify the description of the Start Request Form. Add a description that identifies the proper usage of the Start Request Form and the associated Process Definition to the CA SDM Administrator.
6. Click the Keywords tab.
   The Keywords tab is active.
7. Click the ab+ icon.
   A row adds to the empty list.
8. Click the row.
   A blinking cursor highlights the row and indicates the row is ready for typing.
   a. Enter one of the following values to associate a keyword to the appropriate ticket area or category.
      For example, to make a Start Request Form available for a CA SDM request area, enter the pcat keyword.
   b. Add a row to the list for each applicable keyword.
      For example, to make the Start Request Form appear on both request areas and change categories, add one row for the chgcat keyword and another row for the pcat keyword.

c. Click OK.
CA Process Automation saves the keywords and description and closes the Library Object Properties dialog.

d. Check in the Start Request Form.

Ticket	Use Keyword
request area	pcat
change category	chgcat
issue category	isscat

Note: If you fail to check in the Start Request Form, the form fails to appear in CA SDM.

The CA Process Automation Start Request Form information appears on the CA SDM Start Request Form List. The CA SDM administrator can associate the CA SDM Start Request Form with the Process Definition, on a Request Area, Change Category, or Issue Category Detail page.
The following Start Request Form items appear in CA SDM:

1.
- **Start Request Form Name**
Appears on the Request Areas, Change Categories, and Issue Categories list pages.

- **Start Request Form Reference Path**
Appears on the Request Areas, Change Categories, and Issue Categories list pages.

- **Start Request Form Description**
Appears on the Request Areas, Change Categories, and Issue Categories list pages. The text in this field describes how the Start Request Form is appropriate for selection on a particular Request Area, Change Category, or Issue Category.

Integrate CA Service Catalog with Common Components Manually

This section contains the following articles:

Integrate CA Service Catalog with CA EEM Manually

Important! Review the following section only if you want to manually integrate CA Service Catalog with CA EEM when the automatic integration between the two has failed.

Ensure that both the CA EEM server and CA Service Catalog server are up and running.

Follow these steps:

1. Log in to the setup utility and click Security on the left menu.
2. Perform *one* of the following actions, whichever applies:
   - If CA EEM is installed on one computer only, enter its host name.
   - If CA EEM is installed on multiple computers as a cluster *without* a Proxy, enter the host names of the CA EEM computers. Separate the names with commas.
     (*Proxy* here means load balancer.)
   - If CA EEM is installed on multiple computers as a cluster *with* a Proxy, enter the host name of the Proxy computer.
3. For the CA EEM application instance name, perform *one* of the following actions, whichever applies:
   - If you upgraded CA EEM during this CA Service Catalog upgrade or if you are using an existing version of CA EEM, specify the existing application instance name.
   - If you installed CA EEM for the first time during this CA Service Catalog upgrade, specify the application instance name of your choice.
4. Enter the CA EEM administrator (EiamAdmin) password.
5. Click Save.
   The utility creates the required CA Service Catalog objects in CA EEM. Examples include the *Service Catalog* application, policies, and users (including spadmin).

Integrate CA Service Catalog with CA Business Intelligence Manually

Important! Review the following section only if you want to manually integrate CA Service Catalog with CA Business Intelligence when the automatic integration between the two has failed. If you have any other earlier version of CA Business Intelligence, install CA Business Intelligence 4.1 SP3 and migrate the data from your earlier version (see page 285) for the reports to work.

CA Business Intelligence is a set of reporting and analytic software. You can use CA Business Intelligence to integrate, analyze, and then present through various reporting options, vital information that is required for effective enterprise IT management. CA Business Intelligence is a flexible, scalable, and reliable business intelligence reporting system that can be integrated into your information technology infrastructure.

CA Service Catalog supplies the data that you require to get started with CA Business Intelligence reports. After you have installed CA Service Catalog and CA Business Intelligence, you perform required setup tasks before running reports.

Follow these best practices when maintaining and using CA Business Intelligence:

- Install and maintain one universe per CA product.
- Do *not* modify the default universe. Instead, copy it and modify the copy. Otherwise, your changes can be erased when you apply service packs, patches, and other updates. Back up all your changes and then apply the patches to your customized universe.
- Reports:
  - Verify that the services in Central Configuration Manager (CCM) is running, when the reports stop running.
  - Do not overwrite predefined reports.
  - Always use a predefined report as a base to build a custom report and maintain consistent formatting in all reports.
  - Administrators *can modify all the reports and can create* new reports that are based on the existing universe. However, administrators must not add any reports to the existing folders.
  - Both administrators and end users *must not* change pre-defined reports. Any changes to those reports are applied to all other users using the same CA Business Intelligence instance. Instead, both administrators and end users must create their own custom folders, copy the reports there, rename them, and customize them.
  - Both administrators and end users must add new reports that they create to their custom folders.

Follow these steps:

- Step 1 - Verify that CA Business Intelligence Is Installed (see page 3295)
- Step 2 - Import the BIAR File (see page 3295)
- Step 3 - Set Up the User Database in CA Business Intelligence (see page 3295)
- Step 4 - Set the Administration Configuration Parameters (see page 3296)
- Step 5 - Configure Trusted Authentication (see page 3297)
- Step 6 - Run Pre-Defined Reports (see page 3298)

Note: If you plan to use Secure Socket Layer between CA Service Catalog and CA Business Intelligence, ensure that you:

- Configure CA Business Intelligence for Secure Socket Layer (SSL)
- Configure CA Business Intelligence to communicate with CA Service Catalog using SSL

Step 1 - Verify that CA Business Intelligence Is Installed

You obtain best system performance by installing CA Business Intelligence and CA Service Catalog components on separate computers.

For more information about installing CA Business Intelligence 4.1 SP3, see CA Business Intelligence 4.1 SP3 documentation (https://wiki.ca.com/display/CABI41SP3/CABI+Installation+on+Windows). To verify that CA Business Intelligence is installed and running, access CA Business Intelligence and start it.

Step 2 - Import the BIAR File

Importing the Business Intelligence Archive Resource (BIAR) file is a required task to set up CA Business Intelligence reports for CA Service Catalog.

For more information, see how to import the BIAR file (see page 3299).

Step 3 - Set Up the User Database in CA Business Intelligence

CA Service Catalog users can access *only* the CA Business Intelligence reports that their role authorizes them to.

Follow these steps:

1. Verify that a matching user name exists in CA Business Intelligence for each CA Service Catalog user.

   Note: The BIAR file automatically provides the CA Service Catalog default administrative user named spadmin and CASMAdmin.

   Optionally, import the users from your CA Service Catalog user database into your CA Business Intelligence user database. For example, in LDAP or Active Directory. Alternatively, create the users with matching user names directly in your CA Business Intelligence user database.

2. Assign those users to the CA Business Intelligence user groups that provide the access rights you want.
   Typically, you assign the users to groups that match their roles in CA Service Catalog. For example, you typically assign CA Service Catalog administrators to administrator groups in CA Business Intelligence.

   Important! All CA Service Catalog users who need access to CA Business Intelligence reports must exist in the CA Business Intelligence user database. Also, these users must belong to the CA Business Intelligence user group that provides the appropriate level of access rights.

   The CA Service Catalog Administrator groups are as follows:

- SLCM Catalog Administrators
- SLCM Administrators
- SLCM Service Managers
- SLCM Super Business Unit Administrators
- SLCM Service Delivery Administrators

The CA Service Catalog End User groups are as follows:

- SLCM End Users
- SLCM Catalog End Users
- SLCM Request Managers

Step 4 - Set the Administration Configuration Parameters

If you are running multiple instances of CA Business Intelligence, the configuration settings apply to all instances.

Follow these steps:

1. Click **Administration**, **Configuration** in the CA Service Catalog section.
2. Click the Modify icon to next to each property that you want to update:
   - **CMS Host Name**
     Specifies the computer name on which Central Management Server is installed.
   - **CMS Port Number (1 - 65535)**
     Specifies the port number on which the Central Management Server is running.
   - **Enable HTTPS**
     Specifies a web protocol, as follows:
     Select No (the default) to use HTTP to communicate with CA Business Intelligence.
     Select Yes to use HTTPS to communicate with the CA Business Intelligence.

     Important! If you select Yes, verify that CA Business Intelligence is also using HTTPS. For more information about how to configure CA Business Intelligence to use HTTPS, see the CA Business Intelligence documentation.
   - **Host Name**
     Specifies the computer name on which CA Business Intelligence web application server is hosted.
   - **Port Number** (1 - 65535)
     Specifies the port number on which CA Business Intelligence web application server is running.

3. Click the **Launch** button to test the connection between CA Service Catalog and Launch Pad.

4. Recycle Catalog Component.

The CA Business Intelligence configuration information is updated with the values that you specified.

Step 5 - Configure Trusted Authentication

Configure CA Service Catalog and CA Business Intelligence to use trusted authentication for the integration between the two products. Trusted authentication provides Single Sign-On. Single Sign-On enables CA Service Catalog users to access the Launch Pad application of CA Business Intelligence directly from the CA Service Catalog GUI.

CA Service Catalog uses standard CA Business Intelligence login if trusted authentication is not set up or if it is not working properly.

Note: The following login methods do *not* apply to CA Business Intelligence: CA EEM token, CA SiteMinder Integration, and NTLM authentication on Windows.

Follow these steps:

1. Log on to the CA Business Intelligence Central Management Console as a user with administrative rights.

2. Go to **Manage**, **Authentication** area of the Central Management Console.

3. Click the **Enterprise** tab.

4. Check **Trusted Authentication is Enabled** to enable trusted authentication.

5. Click **New shared secret** and you see that **Download Shared Secret** is enabled.

Note: The CA Business Intelligence client and the Central Management Console use the shared secret password to create a trusted authentication password. The value of this password and the frequency with which you update it meet your password security standards.

6. Click **Download Shared Secret** to generate TrustedPrincipal.conf file.

7. Perform the remaining steps on *every* Catalog Component computer.

8. Open the file that is named USM_HOME\reporting\CABI\TrustedPrincipal.conf using a text editor.

9. Scroll to the following line and specify the same shared secret password that you downloaded on the CA Business Intelligence Central Management Console.

```
SharedSecret=password
```

10. Save the TrustedPrincipal.conf file.

11. Restart the Catalog Component computer.

Important! Whenever you update the password on the CA Business Intelligence Central Management Console, make the same change to the password in the TrustedPrincipal.conf file on every Catalog Component computer.

Step 6 - Run Pre-Defined Reports

The **BI Launch Pad** button enables you to run the pre-defined reports quickly and easily from within CA Service Catalog.

Optionally view the pre-defined reports in localized format. To do so, set the language configuration in the **Preferences**, **Locales and Time Zone**, **Preferred Viewing Locale** section of CA Business Intelligence.

Note: Some fields remain in English even when you view reports in localized format. These fields include Request Status, Billing Status, Account Status, Account Type, and fields related primarily to payment and adjustment. In addition, in both English and localized reports, custom status values do appear in the reports; however, their descriptions do not.

Follow these steps:

1. Select **Home**, **DashBoards**, **Administration Quick Start**, **BI Launch Pad** in CA Service Catalog.

2. Click **Documents**, **Folders**, **Public Folders**, **CA Reports**, **CA Service Management, CA Service Catalog**.

3. Click **Admin Reports** or **User Reports**, as required.
   The Admin Reports folder and its reports are visible only to users who are members of the Administrator groups.
   The User Reports folder and its reports are visible only to users who are members of either the Administrator groups or the End User groups.

4. Double-click the report which you want to run.

5. Specify the parameters for your report.

6. Click Run Query.

7. View the report.

Note: In a multi-tenant (business unit) implementation, your reports display only the data of tenants to which you have access.

If you run a report for an integrated product (such as CA Service Desk Manager or CA Asset Portfolio Management), but that product has not been integrated with CA Service Catalog, then the report typically fails.

Import the BIAR File

This article contains the following topics:

The Business Intelligence Archive Resource (BIAR) file includes several required components and CA Service Catalog-specific content for use with CA Business Intelligence. The file includes CA Service Catalog universe, default objects, pre-defined reports, user groups, database schemas, locale strings, and data that helps you customize your CA Business Intelligence implementation, especially your reports.

To import the BIAR file, verify that a data source name (DSN) and ODBC connection exists for the DBMS used by the MDB. If necessary, create a Data Source Name and ODBC Connection for the MDB on SQL Server or Oracle. Then you use the biconfig utility to Import the BIAR file

Create a Data Source Name and ODBC Connection for the MDB on SQL Server

If you are using Microsoft SQL Server as your DBMS for the MDB, a data source name (DSN) and ODBC connection for the MDB on SQL Server are prerequisites for setting up your CA Business Intelligence implementation. If necessary, create them now.

Follow these steps:

1. From the Windows Control Panel, open ODBC.
2. Click Add on the System DSN tab.
3. Select SQL Server as the driver and click Finish.
4. Enter the following information and click Next:
   - Data source name (DSN)

     Note: Ensure that you create the DSN with the name "caslcm_cabi_dsn".

   - Description

- Name of the SQL Server server

5. Perform the following actions and click Next:
   a. Select SQL Server Authentication
   b. Select the option to Connect to SQL Server to obtain default settings for configuration options. Enter the user ID and password to connect to the database.
6. Perform the following actions and click Next:
   a. Change the default database to the SQL Server database.
   b. Select the option to use ANSI quoted identifiers.
   c. Select the option to use ANSI nulls, paddings, and warning.
7. (For localized environments *only*) Check the option to use regional settings for currency, numbers, dates, and times.
8. Click Finish.

You have created the DSN and ODBC connection for SQL Server.

Note: For more information about creating DSNs and ODBC connections, see your Windows or SQL Server documentation.

Create a Data Source Name and ODBC Connection for the MDB on Oracle

If you are using Oracle as your DBMS for the MDB, a data source name (DSN) and ODBC connection for the MDB on Oracle are prerequisites for setting up your CA Business Intelligence implementation. If necessary, create them now.

Follow these steps:

1. From the Windows Control Panel, open ODBC.
2. Click Add on the System DSN tab.
3. Select Oracle client /server for Oracle as the driver and click Finish.
4. Enter the following information and click OK:
   - Data source name (DSN)

     Note: Ensure that you create the DSN with the name "caslcm_cabi_dsn".

- Description
- DBMS user name
- One of the following values:
  - SID of the Oracle database, if you are using a standalone Oracle setup.
  - Local Net Service Name, if you are using a distributed Oracle setup.

You have created the (DSN) and ODBC connection for Oracle.

Use biconfig to Import the BIAR File

Importing the BIAR file is a required task to set up your CA Business Intelligence implementation. We recommend that you use the CA Business Intelligence biconfig batch utility to import the BIAR file.

Note: Delete the CA SLCM Connection from Central Management Console before you import the BIAR file.

Follow these steps:

1. Go to the CA Service Management Install path and locate the \filestore\BOXI\biconfig folder.
2. Copy the contents of the biconfig folder on to the CA Business Intelligence computer.
3. Create an XML file (with the contents of Example file for SQL server (see page 3303) or Oracle (see page 3304)) and update the appropriate file, according to your requirements.

   Set the following parameters in your BIAR file:

   - Networklayer: ODBC
   - RDBMS:
     - For Microsoft SQL Server (SQL Server): MS SQL Server 2008 or MS SQL Server 2012
     - For Oracle: Generic ODBC datasource
   - User name and password parameters for your database:
     - For SQL Server: Use *sa* for the user name.
     - For Oracle: Use *mdbadmin* for the user name.

     Note: These users have access to all required tables in the MDB.

- Path name of the SLCM_universe.biar file on the CA Business Intelligence computer
- Name of the DSN created previously in the datasource parameters. **Value:** caslcm_cabi_dsn
- Server parameter: Computer name of your Oracle or SQL Server server

4. Open a Windows command prompt and navigate to the biconfig folder on the CA Business Intelligence computer and enter the following command:

   ```
   biconfig -h "host" [-n "port"] -u "user" [-p "password"] -f "XML-config
   ```

   The quotation marks (" ") *are* required as shown in the command. However, the brackets [ ] are *not* required; the brackets signify optional parameters.
   The following parameters are required, unless noted otherwise.

   - **host**
     Specifies the CA Business Intelligence Central Management Server (CMS) host.
   - **port**
     (Optional) Specifies the CA Business Intelligence CMS port. The default is 6400.
   - **user**
     Specifies the CA Business Intelligence CMS user.
   - **password**
     Optional. Specifies the CA Business Intelligence CMS password.
   - **XML-config-file-name**
     Specifies the path name of the XML file you modified.
     If the file resides in the biconfig folder, you can specify the file name only. Otherwise, specify the complete path name.
   - **help**
     Optional. Displays the help for the biconfig utility.
     Enter *two* dashes to display the help.

   Note: For more information about using biconfig, see the biconfig-readme.txt file in the biconfig folder.

5. (Only for Oracle and if both your CA Service Catalog and CA Service Desk Manager are configured to use the same instance of CA Business Intelligence server, and the date format in odbc.prm file is changed to the CA SDM date format) Update the oracle.prm file at <CABI_Home>\SAP BusinessObjects Enterprise XI 4.0 \dataAccess\connectionServer\odbc\extensions\qt as follows:

6. a. Replace <Parameter Name="USER_INPUT_DATE_FORMAT">'dd-Mmm-yyyy'< /Parameter> with existing USER_INPUT_DATE_FORMAT tag.

Note: The CA SDM date format is **mm/dd/yyyy hh:mm:ss AM/PM**

b. Restart the Apache Tomcat for BI 4 and Server Intelligence Agent services in Central Configuration Manager.

7. Verify the import, as follows:

   a. Review the biconfig.log file in the biconfig folder.
   This file lists the status of the import. This file also includes error messages if the BIAR file is not imported successfully. A return code of zero (0) indicates a successful import.

   b. Log in to BI launch pad as a CA Business Intelligence administrator.

   c. Verify that you can view the CA Service Catalog Reports under Public Folders/CA Reports/CA Service Management/CA Service Catalog.

8. Specify a password for the spadmin user in CA Business Intelligence. This password is empty by default.

Note: If you must import the BIAR file again, delete the following elements from the CA Business Intelligence Central Management Console *before* you import the BIAR file again:

- CA SLCM folder
- CA SLCM Universe
- CA SLCM Groups
- SLCM Connection

Example XML File (SQL Server) to Import BIAR

```
<?xml version="1.0"?>
<biconfig version="1.0">
<!-- Import BIAR file -->
<step priority="1">
<add>
<biar-file name="Specify path of the SLCM_universe.biar file on the CA Business
Intelligence computer">
<networklayer>ODBC</networklayer>
<rdbms><Specify the MS SQL Server version></rdbms>
<username>sa</username>
<password><Specify the sa password></password>
<datasource>caslcm_cabi_dsn</datasource>
<server><Specify the Database Server name></server>
</biar-file>
</add>
</step>
<step priority="2">
<add-if-missing>
<user name="spadmin">
<password mode="normal"><Specify the password for the spadmin user in CA Business
```

```
Intelligence></password>
<description>SLCM Admin User</description>
<password-expiry>false</password-expiry>
<can-change-password>true</can-change-password>
<change-password-on-next-logon>false</change-password-on-next-logon>
</user>
</add-if-missing>
</step>
<step priority="3">
<add-if-missing><membership>
<group>SLCM Service Delivery Administrators</group>
<user>spadmin</user>
</membership>
</add-if-missing>
</step>
</biconfig>
```

Example XML File (Oracle) to Import BIAR

Important! If both your CA Service Catalog and CA Service Desk Manager are configured to use the same instance of CA Business Intelligence server, and the date format in odbc.prm file is changed to the CA SDM date format, specify your version of Oracle within the <rdbms> and </rdbms> tags.

```
<?xml version="1.0"?>
<biconfig version="1.0">
<!-- Import BIAR file -->
<step priority="1">
<add>
<biar-file name="Specify path of the SLCM_universe.biar file on the CA Business
Intelligence computer">
<networklayer>ODBC</networklayer>
<rdbms>Generic ODBC datasource</rdbms>
<username>mdbadmin</username>
<password><Specify the mdbadmin password></password>
<datasource><caslcm_cabi_dsn></datasource>
<server>abcdef-xp</server>
</biar-file>
</add>
</step>
<step priority="2">
<add-if-missing>
<user name="spadmin">
<password mode="normal"><Specify the password for the spadmin user in CA Business
Intelligence></password>
<description>SLCM Admin User</description>
<password-expiry>false</password-expiry>
<can-change-password>true</can-change-password>
<change-password-on-next-logon>false</change-password-on-next-logon>
</user>
</add-if-missing>
</step>
<step priority="3">
<add-if-missing>
<membership>
<group>SLCM Service Delivery Administrators</group>
<user>spadmin</user>
</membership>
</add-if-missing>
</step>
</biconfig>
```

Integrate CA Service Catalog with CA Process Automation Manually

Important! Review the following section only if you want to manually integrate CA Service Catalog with CA Process Automation when the automatic integration between the two has failed.

CA Process Automation uses graphical processes that system administrators create to execute operational processes automatically. CA Process Automation supports an integrated development and administrative environment to manage, create, and configure CA Process Automation components on your system. CA Process Automation also supports client applications that allow operators and other personnel to schedule and monitor automated processes. CA Process Automation includes efficient graphical tools for viewing, monitoring, and debugging process at run-time.

In CA Process Automation, operators define policies and rules for self-managed processes. These processes include configuration, monitoring, optimization, repair, and protection. By integrating the people, processes, and technology of an organization in an end-to-end, automated fashion, organizations can reduce operational expenses, increase staff productivity, and can deliver higher service level metrics. Examples of processes that CA Process Automation automates and manages include:

- Applications Monitoring and Restart
- Disaster Recovery
- Virtual Infrastructure Management
- ITIL compliance
- Security

For ITIL-based implementations, see Pre-Built CA Process Automation workflows (https://wiki.ca.com/display/CASM1401/Pre-Built+CA+Process+Automation+Workflows). Such implementations use *both* the basic predefined CA Process Automation that is supplied with CA Service Catalog and other ITIL-based CA Process Automation content.

To configure your implementation of CA Service Catalog, CA Process Automation, and any other integrated CA Technologies products primarily for an ITIL-based environment, review and follow all applicable instructions in thePre-Built CA Process Automation Workflows (see page 4905)Pre-Built CA Process Automation workflows (https://wiki.ca.com/display/CASM1401/Pre-Built+CA+Process+Automation+Workflows) . Use this section as a secondary reference tool for any information.

To configure your implementation of CA Service Catalog, CA Process Automation, and any other integrated CA Technologies products primarily for an environment that is not ITIL-based, review all applicable instructions in this section. Use the Pre-Built CA Process Automation workflows (https://wiki.ca.com/display/CASM1401/Pre-Built+CA+Process+Automation+Workflows) section as a secondary reference tool if any ITIL-related questions arise.

Do *not* combine, substitute, or interchange procedures from this section and the Pre-Built CA Process Automation workflows (https://wiki.ca.com/display/CASM1401/Pre-Built+CA+Process+Automation+Workflows)for performing a specific task. Doing so can produce unpredictable or inconsistent results.

Set Up the CA Process Automation - CA Service Catalog Integration

Important! Review the following section only if you want to manually integrate CA Process Automation with CA Service Catalog.

To Integrate CA Service Catalog with CA Process Automation, follow this process:

- Step 1 - Perform Setup Tasks (see page 3306)
- Step 2 - Set Up Rules, Actions, and Processes for Approval and Fulfillment (see page 3316)
- Step 3 - Assign Users to Required CA Process Automation User Groups (see page 3328)

Step 1 - Perform Setup Tasks

Perform these tasks after installing CA Service Catalog and CA Process Automation:

1. Become familiar with CA Process Automation so that you become a knowledgeable administrator and user of it. You must also be able to write basic CA Process Automation processes that include reusable operators. These operators enable communication between CA Process Automation and the products with which it integrates, including CA Service Catalog.

2. Verify that CA Process Automation is running. Install CA Process Automation either before or after you install CA Service Catalog.

   Important! Do *not* install the CA Process Automation domain orchestrator and CA Service Catalog components on the same computer.

3. Verify that you have:

   - Installed the DBMS client (Oracle client or SQL Server client) locally, unless the local computer is the DBMS server. For more information about how to install the DBMS client, see your DBMS documentation.

   - Implemented CA Service Catalog clustering, if you have installed two or more instances of CA Service Catalog. For more information about how to implement CA Service Catalog clustering, see the Implement Clustering (see page 604)section.

   - Met the following naming requirements:

     - The CA Service Catalog computer name must *not* begin with a number.

- If you are using a load balancer for CA Service Catalog or CA Process Automation, the computer name of the load balancer must *not* begin with a number.

If you do not meet these requirements, web service calls for the integration can result in errors, for example:

```
Caused by: com.sun.xml.messaging.saaj.util.JaxmURI$MalformedURIException: Host is not a well formed address!
```

4. If you plan to use Secure Socket Layer, perform the following tasks:
   - Configure CA Process Automation for Secure Socket Layer (SSL).
   - Configure CA Process Automation to communicate with CA Service Catalog using SSL**.**
5. Perform one of the following actions to specify your login method:
   - If you plan to log in using standard login credentials, skip the next step.
   - If you plan to log in using a CA EEM token instead of standard login credentials, set up certificate-based login (see page 3307).
6. Set and test the administration configuration parameters (see page 3311) for CA Process Automation.
7. Load and configure content in CA Service Catalog (see page 3313).
8. Configure content in CA Process Automation (see page 3314).

Set Up Certificate-Based Login in CA Service Catalog

To enhance security, you can set up CA Service Catalog to use certificate-based login to communicate with CA Process Automation. Otherwise, CA Service Catalog uses user name and password login to communicate with CA Process Automation.

The CA Process Automation integration with CA Service Catalog requires CA EEM certificates for certificate-based login. If you are upgrading CA Service Catalog and you already have a .p12 certificate for connecting to CA Process Automation, convert it to .pem format. Similarly, if you are installing CA Service Catalog for the first time, generate a new .pem file.

Follow these steps:

1. Configure CA Service Catalog and CA Process Automation to use SSL, if other CA products integrated with CA Service Catalog are configured with SSL. These tasks include creating and merging keystore files and adding self-signed certificates to the keystore.
2. Edit the USM_HOME\build.xml file, as follows:

```
<sysproperty key="javax.net.ssl.trustStore" value="${env.USM_HOME}/keystore/.
keystore" />
```

3. Verify that the file name and path name of the keystore file are correct. If necessary, update them.
   For example, if the keystore is located in USM_HOME and the keystore file name is . mykeystore, update this line as follows:

   ```
   <sysproperty key="javax.net.ssl.trustStore" value="${env.USM_HOME}/.mykeystore"
   />
   ```

4. Locate the following line:

   ```
   <sysproperty key="javax.net.ssl.trustPass" value="changeit" />
   ```

5. Verify that the keystore password is correct. If necessary, update it.
   For example, if the keystore password is mykeystorepw, update this line as follows:

   ```
   <sysproperty key="javax.net.ssl.trustPass" value="mykeystorepw" />
   ```

6. Verify that both CA Service Catalog and CA Process Automation are using the same CA EEM server. Typically, you completed this action when you set up the integration. However, see the eiam.backend property in USM_HOME\config.properties file in CA Service Catalog to verify the name of the CA EEM server.

7. Access the USM_HOME\scripts\eiam folder on any Catalog Component computer and edit the file that is named issue ITPAMCertificatePEM.xml, as follows:

   a. Replace __USMHOME_ (a placeholder value) with the actual value of USM_HOME, for example, C:\Program_files\CA\CA Service Catalog.

   b. Replace ITPAMContext (a placeholder value) with the actual value of the application context name that CA Process Automation uses to connect to CA EEM. For example, ITPAM.

   c. Comment or Uncomment the GroupMembership command line depending on the CA Process Automation version.

8. Locate the following Safex section and the group membership lines.
   For example:

   ```
   <Safex>
   <Attach label="ITPAM" />
   <IssueCertificate certtype="pem" certfile="C:/Progra~1/ca/servic~1
   /ITPAMCertfile.pem" keyfile="C:/Progra~1/ca/servic~1/ITPAMCertfile.key"/>
     <AddOrModify>
       <!--Add user and assign them to appropriate groups-->
       <User folder="/Users" name="CERT-ITPAM">
         <GroupMembership>ITPAMAdmins</GroupMembership>
         <GroupMembership>ITPAMUsers</GroupMembership>
     </User>
     </AddorModify>
   <Detach/>
   </Safex>
   ```

9. Update the values in the group membership lines, as follows:

```
<GroupMembership>PAMAdmins</GroupMembership>
<GroupMembership>PAMUsers</GroupMembership>
```

10. Save and close the file.

11. Verify that *filename* is the same in *filename*.key and *filename*.pem, for example, ITPAMCertfile.key and ITPAMCertfile.pem.

12. (Upgrades) Perform the following actions to convert your existing .p12 file (if you have one) to a .pem file:

    a. Open the Windows command prompt on the computer where CA EEM is installed. Change to the folder named *drive*:\Program Files\CA\SharedComponents\iTechnology.

    b. Run the following command:

```
igwCertUtil -version 4.6.0.0 -conv  -cert "<Certificate><certType>p12<
/certType><certURI>ITPAMCertfile.p12</certURI><certPW>ca</certPW><
/Certificate>" -target "<Certificate><certType>pem<
/certType><certURI>ITPAMCertfile.pem</certURI><keyURI>ITPAMCertfile.key<
/keyURI></Certificate>"
```

    This action converts the existing .p12 file to a .pem file.

13. (New Installations) Perform the following actions to create a .pem file:

    a. Open the CA Service Catalog command prompt by entering USM_HOME\usm.cmd at the Windows command prompt.

    b. Change to the USM_HOME\bin\safex folder, and run the following command at the CA Service Catalog command prompt:

```
safex.exe -u EiamAdmin -p <password> -h <eemserver> -f
USM_HOME\scripts\eiam\issueitpamcertificatepem.xml -
sdkconfig  USM_HOME\eiam.config
```

    This action creates the ITPAMCertfile.pem and ITPAMCertfile.key files. Both files are necessary for the .pem file authentication to work.

14. Log in to CA Service Catalog. Click Administration, Configuration, CA Process Automation and do the following actions:

    a. Enter the name of the .pem file in the PEM Certificate File Name column. The .pem file is stored in USM_HOME.

    b. Select Yes for the option that is named *Use Certificate for Authentication*.

    c. Set the other configuration parameters (see page 3311) for the properties.

15. Click Test to test the two-way web service connection between CA Service Catalog and CA Process Automation.

16. Load and Configure Content in CA Service Catalog (see page 3313).

17. Click the Launch button to start the CA Process Automation Server web URL with the updated properties.

18. Update the user password (see page 3314) for CA Service Catalog in the CA Process Automatior SLCM_GlobalDataset.

You have set up certificate-based login between CA Service Catalog and CA Process Automation.

Set Up Certificate-Based Login in CA Process Automation

To enhance security, you can set up CA Process Automation to use certificate-based login to communicate with CA Service Catalog. If you do not use this feature, CA Process Automation uses user name and password login to communicate with CA Service Catalog.

Important! This procedure applies *only* if you are using a CA Process Automation version that also supports certificate-based login for CA Service Catalog.

Follow these steps:

1. Access the USM_HOME folder of the CA Service Catalog computer and verify that the following certificate files exist:

   - USMcertfile.key
   - USMcertfile.pem
   - USMcertfile.p12

   The CA Service Catalog installation program creates these files automatically.

2. Decide the files to use with CA Process Automation:

   - If CA EEM is using FIPS mode, select USMcertfile.pem.
   - If CA EEM is using non-FIPS mode, select USMcertfile.p12.

   To verify whether CA EEM is using FIPS mode, log in to CA EEM. Click the About link on the top right corner of the page. An information dialog appears. Review the FIPS-related details on this dialog.

3. Log in as an administrator to CA Process Automation from the CA Service Catalog computer.

4. Perform the following actions:

   a. Click Configuration.

b. Click Manage User Resources at the left bottom portion of the page.
The User Resource folder is selected in the Repository tree, and the User Resource page appears on the right pane.

5. Perform the following actions for the file or files that you selected in Step 2. If you selected USMcertfile.key and USMcertfile.pem, perform these actions individually, once for each file.

   a. Click New.

   b. Click Browse in the Resource File field and navigate to the USM_HOME folder on the CA Service Catalog computer.

   c. Select the file and specify the resource name. You can specify an arbitrary name of your choice.

   d. Record the path names of the file or files. You require this information when you set the related administration configuration parameters.

6. Save your changes.

7. If you are using multiple CA Process Automation domain servers with CA Service Catalog, repeat these steps on each one.

You have set up CA Process Automation to use certificate-based login to communicate with CA Service Catalog.

Set Administration Configuration Parameters

If you are running multiple instances of CA Process Automation, the following settings apply to all instances.

Follow these steps:

1. Log in to CA Service Catalog.

2. Click **Administration**, **Configuration**.

3. Click **CA Process Automation** and complete the configuration options, as follows:

   - **Certificate File Path on CA Process Automation**
     Applies only when you are using certificate-based login in CA Process Automation (see page 3310) with USMcertfile.pem (for FIPS mode) or USMcertfile.p12 (for non-FIPS mode). If this condition exists, specify the path name of the appropriate file on the CA Process Automation server.

   - **Enable Automatic Retry**
     Applies in cases when a request is created in CA Service Catalog that is not processed in CA Process Automation due to connectivity issues between CA Service Catalog and CA Process Automation. The request is placed in queued state. Retry manually to process the request to CA Process Automation. Specify Yes for automatic retry or No for manual retry. When the Automatic Retry is selected as Yes, the CA Service Catalog connection is established. The ITPAM_QUEUE_FAILURE automatically gets deleted from the Home,

Messages, Alerts, List All Failed Actions list.
When the message disappears from the List All Failed Actions, verify that the request has changed to the appropriate status. For example, if the original status was Submitted (Queued) then the updated status must be Pending Approval.

- **Key File Path on CA Process Automation**
  Applies only when you are using certificate-based login in CA Process Automation (see page 3310) with the USMcertfile.key file.
  If this condition exists, specify the path name of the USMcertfile.key file on the CA Process Automation server.

- **Password for Certificate on CA Process Automation**
  Applies only when you are using certificate-based login in CA Process Automation (see page 3310) with the USMcertfile.p12 file.
  If you are using CA Process Automation 4.0 SP1 CP2, obtain the password from the USM_HOME\scripts\EIAM\issueCertificateP12.xml file. The password is a random-generated number that is specified in the IssueCertificate tag of the password attribute, as follows:

```
<IssueCertificate certfile="C:/Program Files/CA/Service Catalog/USMcertfile.p12" password="password"/>
```

- **Enable HTTPS**
  Indicates whether CA Service Catalog uses HTTPS when communicating with CA Process Automation. Specify Yes or No.

- **Host Name**
  Specifies the host name of CA Process Automation computer (the Domain Orchestrator).

  Note: After the integration has been configured and in use, do *not* change the host name of the CA Process Automation computer or the CA Service Catalog computer. The only exception occurs when the two host computers use the same MDB. For information about the MDB, see the MDB documentation included on the CA Service Catalog installation media.

- **PEM Certificate File Name**
  Applies only when you are using a CA EEM certificate for authentication. That is, when the setting named *Use Certificate for Authentication* is Yes. If that setting is Yes, then PEM Certificate File Name specifies the name that you specified earlier when set up certificate-based login for CA Process Automation.

- **Port Number**
  Specifies the port number on the CA Process Automation computer that listens for incoming calls from CA Service Catalog.

- **Retry Count**
  Specifies the number of retry attempts. This value indicates the number of times for CA Service Catalog to try again to perform a failed CA Process Automation action. The default retry count value is 3.
  If all retry attempts fail, CA Service Catalog logs a queue alert as ITPAM_FAILED, and ITPAM_QUEUE_FAILURE in Home, Messages, Alerts. You can manually retry the failed action by viewing the queue alerts in List All Failed Actions. Click the Retry button.

- **Retry Interval**
  Specifies the number of seconds between the retry attempts described for the previous item, Retry Count. The default retry interval is 15 seconds.

- **Use Certificate for Authentication**
  Indicates whether to use a CA EEM certificate for authentication. This certificate is used for communication from CA Service Catalog to CA Process Automation. Specify Yes or No.

- **User ID and User Password**
  Specifies the user ID and password for accessing the CA Process Automation computer. This user ID and password apply *only* when you are using standard login credentials. It does *not* apply when you are using a CA EEM certificate for authentication.

  Important! Verify that the user ID you specify has administrative access to *all* CA Process Automation processes. The user ID requires the right to execute a CA Process Automation process.

The new parameter settings are in effect. Verify that the request flow for a service that uses a CA Process Automation process works properly from approval to fulfillment.

Load and Configure Content in CA Service Catalog

The CA Process Automation *content* refers to the processes, SRFs, rules, actions, and related items that are supplied with CA Service Catalog. You load and configure this content in CA Service Catalog to activate it. Afterwards, you configure this content in CA Process Automation (see page 3314).

Follow these steps:

1. Log in to CA Service Catalog.
2. Click **Administration**, **Configuration**.
3. Click **CA Process Automation** in the Options section.
4. Click **Load**.
   The Load Configuration Dialog appears with two options.
5. Select one or both options (as applicable) and click **Load** in the Load Configuration Dialog.
   The loading process typically requires a few minutes. This process loads the CA Process Automation content for use with CA Service Catalog.
   If the loading process completes successfully, a confirmation message appears. A successful load imports the CA Process Automation content, including processes, and related CA Service Catalog rules, actions, and services.
   If an error message appears, verify that the CA Process Automation server is available and that the configuration parameters are valid.
6. Click **Configure**.
   The CA Service Catalog configuration properties SLCM_GlobalDataset and SDM_GlobalDataset are configured.

You have loaded and configured the content in CA Service Catalog.

Configure Content in CA Process Automation

The CA Process Automation content refers to the processes, SRFs, rules, actions, and so forth, supplied with CA Service Catalog.

Follow these steps:

1. Log in to your CA Process Automation client.
2. Navigate to the CA SLCM folder in the Library Browser, and open the data set named SLCM_GlobalDataset.
3. Open the Login Parameters tab In the Value Definition palette of the data set and perform the following actions:
   a. Verify that the values of the following options are correct for your implementation. Update these values as needed.
      - userID__ - Specifies an administrative user ID with the Service Delivery administrator role.
        As a best practice, create an administrative user in CA Service Catalog exclusively for this integration.
      - Password__ - Specifies the password for this administrative user.

      Important! This field is empty by default; therefore, enter a valid value.

   b. Record these values for use in a later step.
   c. Open the APP URLs tab in the global data set. Verify that the values of the following options are correct for your implementation. Update these values as needed.
      - SLCM_URL - Specifies the URL to launch CA Service Catalog, in the format http: *//hostname:portnumber*.
        If CA Service Catalog runs in a clustered environment, enter the host name and port number of the load balancer.
      - SLCM_CONTEXT - Specifies the URL of the CA Service Catalog context, in the format */usm*.
        For example, http:*//m:port/usm*

      Note: You can deploy CA Service Catalog in Tomcat web server, where the context name would be usm. If you deploy CA Service Catalog on other supported web servers, you can rename the context.

d. Record these values for use in a later step.

4. To save your changes to SLCM_GlobalDataset, perform the following actions:

5. Click Save.

6. Click the checkin icon to update and save your changes to SDM_GlobalDataset.

7. Perform the following steps, If, you have integrated CA Service Catalog with service desk:

   a. Select the CA SDM folder in the Library Browser, and open the data set named SDM_GlobalDataset.

   b. Open the Login Parameters tab In the Value Definition palette of the data set. Verify that the values for its parameters match the values you specified earlier for the Login Parameters tab of the SLCM_GlobalDataset. Update these values as needed.

   c. Open the SoapCallPaths tab In the Value Definition palette of the data set. Verify that the values for its parameters match the values you specified earlier for the APP URLs tab of the SLCM_GlobalDataset. Update these values as needed.

8. Save your changes to SDM_GlobalDataset.

You are now ready to set up rules, actions, and processes for approval and fulfillment.

Test the Web Service Connection to CA Process Automation

You can test the connection at any time when an issue is detected with processing CA Service Catalog requests. If the test connection fails, verify the view.log or error.log information for the possible reasons for failure.

Follow these steps:

1. Log in to CA Service Catalog.

2. Click **Administration**, **Configuration**.

3. Click **CA Process Automation** in the Options section.

4. Click **Test**.
   The two-way connection is tested between CA Service Catalog and CA Process Automation, using the CheckSLCMConnectivity SRF and the new values specified. If the connection fails, verify the configuration values provided.

Add Multiple CA Process Automation Instances in CA Service Catalog

There can be many rules that are written between departments in a business unit depending on the various services offered. When a rule is created, an action is allocated to the rule for the CA Process Automation instances to process. Multiple CA Process Automation instances can be added in CA Service Catalog for different services and different users. Add multiple CA Process Automation instances in CA Service Catalog to each domain for approval and fulfillment phases based on the category id and domain id. Adding multiples CA Process Automation instances support you to share work between multiple departments.

Follow these steps:

1. Log in to CA Service Catalog.
2. Click **Administration**, **Configuration**.
3. Click **CA Process Automation** in the Options list.
4. Click **Add**.
   The Explorer User Prompt appears:
5. Enter a configuration name for the new CA Process Automation instance.

   Note: You can only enter alphanumeric characters to add a CA Process Automation instance. All the properties that are associated with the default CA Process Automation instance are imported into the new CA Process Automation instance. Configure the property values.

6. Click OK.
7. (Optional) Click the Modify icon and update the values of each property.

   Note: Each instance that you add accepts the same configuration parameters as the original instance. Typically, for best performance, configure a maximum of ten CA Process Automation instances.

You have added a CA Process Automation instance to CA Service Catalog.

You can also delete a CA Process Automation instance. For example, if the instance it is corrupted, or if you want to replace the existing instance with a different instance. All requests must be in a canceled or completed state before deleting a CA Process Automation instance.

Important! The default CA Process Automation instance cannot be deleted.

Step 2 - Set Up Rules, Actions, and Processes for Approval and Fulfillment

This article contains the following topics:

To use CA Process Automation for approval and fulfillment of CA Service Catalog requests, you set up rules and actions in CA Service Catalog. You also set up CA Process Automation processes for the actions that you select.

1. Verify that your service is set for workflow-driven approval.

2. Review the important information about CA Service Catalog events, rules, and actions in the Manage Events-Rules-Actions (see page 3040) section. Events are always enabled. For events, certain rules are enabled by default, and other rules are disabled by default. If enabled, rules are triggered and executed when the event occurs. You specify whether to keep or change the default settings for which rules are enabled or disabled. For rules, certain actions are enabled by default, and other actions are disabled by default. If enabled, actions are triggered and executed when the conditions specified by the rule occur.

3. The rules and actions that you use depend on the CA Process Automation content that you load for use with CA Service Catalog. CA Process Automation actions apply only to the rules for the event named Request/Subscription Item Change. By default, for the event *Request /Subscription Item Change*, for the rule *When Status is Canceled*, an action is enabled that terminates CA Process Automation instances when a request is canceled. For best product performance, keep this default setting.

4. Review and decide the rules, actions, and CA Process Automation process that you want to use for *approval*. For more information, see CA Process Automation-Driven Approval (see page 3318).

5. Review and decide the rules, actions, and CA Process Automation processes that you want to use for *fulfillment*. For more information, see CA Process Automation-Driven Fulfillment (see page 3319).

6. In addition, you can create or customize rules or processes that are used in approval and fulfillment. Some customization is permitted for built-in rules, but you can optionally create and customize new rules.
   Similarly, you can optionally create or customize CA Process Automation processes. For more information, see your CA Process Automation documentation.

Processes and Start Request Forms

Each CA Process Automation action that you use with a CA Service Catalog rule invokes a start request form (SRF). The SRF starts a CA Process Automation process that aligns to one or more business process or processes. For more information about processes and SRFs, see your CA Process Automation documentation.

CA Process Automation-Driven Approval

CA Service Catalog supplies a pre-defined rule that fires once for each service when a request is submitted for approval.

In each rule, you specify a CA Process Automation action to initiate an approval CA Process Automation start request form . Each start request form or an SRF initiates a CA Process Automation process that manages approval of requests.

Approval Rule, Condition, and CA Process Automation Action

The approval-related rule is associated with the Request/Subscription Item Change event. This event is launched when any service option element in any service in a request changes.

Because approvals are done at the service level, assign a rule to "act on" the status changes for every service in a request. You specify the conditions in the rule to help ensure that the rule actions are performed only for the first service option element in the first row of the first service option group in each service in the request. Thus, the rule launches only once for each service, regardless of the number of service options and service option elements in the service.

The rule that is associated with the approval process is as follows:

When Status is Submitted and Approval Process is driven by Workflow is launched when these conditions are satisfied:

- 100 <= old status < 200 - The old status is in the not submitted range.
- 200 <= new status < 400 - The new status is in the submitted range.
- approval_process = 2 - The approval process for the service is workflow-driven approval. Workflow drives a service approval.
- sd_row = 1 - This service option element is the first service option element in the service.
- rate_item_col = 0 - This service option element is the first service option element in its row of service option elements.

Note: This rule is launched regardless of the category of any of the service option elements in a service.

Define a CA Process Automation action for approval and associate it with this rule. This action uses the following values:

- Type - CA Process Automation
- Start Request Form (SRF) - click the Search icon and select your approval SRF from the list.
- Configuration Name - All the CA Process Automation multiple instances are listed. Select the CA Process Automation and create the process instance.

- Parameters - When you select an SRF, the required input parameters are automatically listed. Either enter one or more custom values or select one or more values from the list.

The action launches the SRF, passing the information necessary to assign an approval task to the approvers defined in your CA Process Automation approval process. Typically, you use the CA Process Automation process that the SRF calls to set the status of the requested item to Pending Approval (400).

CA Process Automation-Driven Fulfillment

CA Service Catalog supplies rules, conditions, and actions that you can associate with CA Process Automation start request forms (SRFs). These SRFs initiate CA Process Automation processes that handle various fulfillment processes. While approval is handled at the service level, fulfillment is handled at the service option level. The characteristics of the first service option element in a service option determine the fulfillment process to use. The distributed rule conditions are based on the service option element Category field with separate rules for Hardware, Software, None, and all other Category values.

A set of rules is associated with a complex fulfillment process and a simple fulfillment process. Another set of rules opens a CA Service Desk Manager request. The fulfillment process is then left to the CA Service Desk Manager workflow processes.

You can alter the distributed components to fit your business processes more accurately.

Note: Enabling all the rules that are related to all three options is not recommended, because the three fulfillment options overlap.

- **Complex Fulfillment Overview**
  The complex fulfillment process takes into account the current service option element status value to determine the next step in the fulfillment process. The major fulfillment phases related to:
  - Checking availability of the requested item when initially requested or when the item status is Received.
  - Optionally opening a CA Service Desk Manager Change Order (for Hardware or Software). Or notifying appropriate fulfillment personnel when the item is found in available inventory.
  - Notifying the Procurement personnel of the requested item when it is not found in available inventory. The Procurement personnel marks the item as Received when it arrives.
- **Simple Fulfillment Overview**
  The simple fulfillment process notifies the appropriate fulfillment personnel that the item must be fulfilled with no special regard for fulfillment phases.

CA Process Automation Fulfillment Rules, Conditions, and Actions

The fulfillment-related rules are associated with the Request/Subscription Item Change event. This event is launched when any service option element in any service in a request changes.

Use the rule condition to help ensure that the rule actions are performed only at the appropriate time.

The fulfillment process takes different paths that are based on the category and status of the first service option element in the service option. The categories are Software (0), Hardware (1), None (-1), and any custom categories that you define.

The list of categories and their associated numeric values are defined in the following line:

```
USM_HOME\view\webapps\usm\locale\icusen\billing\category.xml
```

The list of statuses and their associated numeric values are defined in the following line:

```
USM_HOME\view\webapps\usm\locale\icusen\request\requestshared.xml
```

CA Process Automation Simple Fulfillment

Simple fulfillment consists of notifying the appropriate department that the requested item must be fulfilled. The assigned fulfillment users change the status of the requested item as appropriate until the status is changed to Fulfilled or Fulfillment Cancelled.

CA Process Automation Simple Fulfillment Rule and Actions

The rule that is associated with the simple fulfillment process used for CA Process Automation is *When Status is Pending Fulfillment*.

Important! If you enable this rule, verify that *all other* fulfillment rules are disabled. Otherwise requests pending action can be duplicated.

- **When Status is Pending Fulfillment Rule**
  This rule is launched when a request item status change and these conditions are satisfied:
  - 800 <= old status <= 999 - The old status is in the approved range.
  - new status = 1000 - The new status is Pending Fulfillment (1000)
  - rate_item_col = 0 - This service option element is the first service option element in its row of service option elements.

  This rule condition ensures that the rule is used only when a request first enters the fulfillment phase.
  Define CA Process Automation Action
  Define a CA Process Automation action for simple fulfillment and associate it with this rule.
  This action uses the following values:
  - Type - CA Process Automation
  - Start Request Form (SRF) - click the Search icon and select your simple fulfillment SRF from the list.

- Configuration Name - All the CA Process Automation multiple instances are listed. Select the CA Process Automation to create the process instance.

- Parameters - When you select an SRF, the required input parameters are automatically listed. Either enter one or more custom values or select one or more values from the list.

When this action starts the Fulfillment, it passes the information necessary to assign a fulfillment needed task to the appropriate fulfillment user or group. Typically, you also use the CA Process Automation process that the SRF calls to set the status of the requested item to Pending Fulfillment (1000).

CA Process Automation Complex Fulfillment

The first step of complex fulfillment is for the appropriate department to check the availability of the requested item. For example, for hardware and software this department can be the IT Services department.

For hardware and software items, if the requested item is found in available inventory, then you can optionally perform one of the following actions:

- Notify the IT Services department to fulfill the request.

- Integrate with another product, such as CA Service Desk Manager. You can now open CA Service Desk Manager change order.

For items that are neither hardware nor software, if the requested item is found in available inventory, then the appropriate department is notified to fulfill the request.

For all items, if the requested item is not found in available inventory, then the Procurement department is notified that the requested item must be purchased. After the status of the requested item is set to Received, it is assumed that the item is then available in the inventory. The appropriate department must check the inventory.

If the appropriate department is notified that fulfillment is needed, the user assigned the fulfillment task sets the request item status to Fulfilled. When all request item statuses are set to Fulfilled, the system changes their statuses to Completed, as appropriate. This action allows billing from Service Accounting Component.

If you have integrated with another product, then you can configure an associated CA Process Automation process in that product to manage the rest of the fulfillment process. For example, if you configure the CA Process Automation process to create a CA Service Desk Manager change order, then, after the change order is closed, the associated CA Process Automation process in CA Service Desk Manager sets the request item status to Fulfilled.

If for some reason, the requested item cannot be fulfilled, then the status is set to Fulfillment Cancelled. The system changes the status to Cancelled when all of the request item statuses are set to Fulfilled or Fulfillment Cancelled. This status change marks the end of the fulfillment phase.

CA Process Automation Complex Fulfillment Rules and Actions

The following rules are associated with the complex fulfillment process:

Check Availability Rules for CA Process Automation

The Check Availability rules for use with CA Process Automation are as follows:

- **When Category is Hardware and Status is Pending Fulfillment** is launched when these conditions are satisfied:
  - 800 <= old status < = 999 - The old status is in the approved range.
  - new status = 1000 - The new status is pending fulfillment (1000)
  - category = 1 - The service option element category is Hardware (1)
  - rate_item_col = 0 - This service option element is the first service option element in its row of service option elements.
- **When Category is Software and Status is Pending Fulfillment** is launched when these conditions are satisfied:
  - 800 <= old status < = 999 - The old status is in the approved range.
  - new status = 1000 - The new status is pending fulfillment (1000)
  - category = 0 - The service option element category is Software (0)
  - rate_item_col = 0 - This service option element is the first service option element in its row of service option elements.
- **When Category is neither Hardware nor Software and Status is Pending Fulfillment** is launched when these conditions are satisfied:
  - 800 <= old status < = 999 - The old status is in the approved range.
  - new status = 1000 - The new status is pending fulfillment (1000)
  - category > 1 - The service option element category is not Hardware (1) or Software (0) or None (-1)
  - rate_item_col = 0 - This service option element is the first service option element in its row of service option elements.

Define CA Process Automation Action

For each Check Availability rule, define a CA Process Automation action and associate it with the rule.

Each action uses the following values:

- Type - CA Process Automation
- Start Request Form (SRF) - click the Search icon and select your Check Availability SRF from the list
- Configuration Name - All the CA Process Automation multiple instances are listed. Select the CA Process Automation to create the process instance

- Parameters - When you select an SRF, the required input parameters are automatically listed. Either enter one or more custom values or select one or more values from the list.

When this action starts the Check Availability SRF, it passes the information necessary to assign a check availability task to the appropriate fulfillment user or group. Typically, you use the CA Process Automation process that the SRF calls to set the status of the requested item to Check Availability (1001).

Fulfillment Rules and Actions for CA Process Automation

The fulfillment rules are as follows:

- **When Category is Hardware and Status is Filled From Inventory** is launched when these conditions are satisfied:
  - old status <> 1002 - The old status is not Filled From Inventory (1002)
  - new status = 1002 - The new status is Filled From Inventory (1002)
  - category = 1 - The service option element category is Hardware (1)
  - rate_item_col = 0 - This service option element is the first service option element in its row of service option elements

Define CA Process Automation Action

If you use the When Category is Hardware and Status is Filled From Inventory rule, define a CA Process Automation action and associate it with the rule. Define this action to pass the information to doone or more tasks, for example:

- Assign a fulfillment needed task to the appropriate fulfillment user.
- Integrate with another product; for example, open a CA Service Desk Manager change order.

Each action uses the following values:

- Type - CA Process Automation
- Start Request Form (SRF) - click the Search icon and select your Fulfillment SRF from the list
- Configuration Name - All the CA Process Automation multiple instances are listed. Select the CA Process Automation to create the process instance.
- Parameters - When you select an SRF, the required input parameters are automatically listed. Either enter one or more custom values or select one or more values from the list.

Typically, you use the CA Process Automation process the SRF calls to set the status of the requested item to Notified IT Services (1015).

- **When Category is Software and Status is Filled From Inventory** is launched when these conditions are satisfied
  - old status <> 1002 - The old status is not Filled From Inventory (1002)

- new status = 1002 - The new status is Filled From Inventory (1002)
- category = 0 - The service option element category is Software (0)
- rate_item_col = 0 - This service option element is the first service option element in its row of service option elements

Define CA Process Automation Action

If you use the When Category is Software and Status is Filled From Inventory rule, define a CA Process Automation action and associate it with the rule. Define this action to pass the information to doone or more tasks, for example:

- Assign a fulfillment needed task to the appropriate fulfillment user.
- Integrate with another product; for example, open a CA Service Desk Manager change order, associating any assigned assets.

Each action uses the following values:

- Type - CA Process Automation
- Start Request Form (SRF) - click the Search icon and select your Fulfillment SRF from the list
- Configuration Name - All the CA Process Automation multiple instances are listed. Select the CA Process Automation to create the process instance.
- Parameters - When you select an SRF, the required input parameters are automatically listed. Either enter one or more custom values or select one or more values from the list.

Typically, you use the CA Process Automation process called by the SRF to set the status of the requested item to Notified IT Services (1015).

- **When Category is neither Hardware nor Software and Status is Filled From Inventory** is launched when these conditions are satisfied:
  - old status <> 1002 - The old status is not filled from inventory (1002)
  - new status = 1002 - The new status is filled from inventory (1002)
  - category > 1 - The service option element category is not None (-1), Software (0) or Hardware (1)
  - rate_item_col = 0 - This service option element is the first service option element in its row of service option elements

Define CA Process Automation Action

If you use the When Category is neither Hardware or Software and Status is Filled From Inventory rule, If you use the When Category is Software and Status is Filled From Inventory rule, define a CA Process Automation action and associate it with the rule. Define this action to pass the information to doone or more tasks, for example:

- Assign a fulfillment needed task to the appropriate fulfillment user.
- Integrate with another product; for example, open a CA Service Desk Manager change order, associating any assigned assets.

Each action uses the following values:

- Type - CA Process Automation
- Start Request Form (SRF) - click the Search icon and select your Fulfillment SRF from the list
- Configuration Name - All the CA Process Automation multiple instances are listed. Select the CA Process Automation to create the process instance.
- Parameters - When you select an SRF, the required input parameters are automatically listed. Either enter one or more custom values or select one or more values from the list.

Typically, you use the CA Process Automation process called by the SRF to set the status of the requested item to Notified IT Services (1015).

- **When Category is None and Status is Pending Fulfillment** is launched when these conditions are satisfied:
  - 800 <= old status <=999 - The old status is in the approved range
  - new status = 1000 - The new status is Pending Fulfillment (1000)
  - category = -1 - The service option element category is None (-1)
  - rate_item_col = 0 - This service option element is the first service option element in its row of service option elements

Define CA Process Automation Action

If you use the When Category is None and Status is Pending Fulfillment rule, Define a CA Process Automation action for simple fulfillment and associate it with this rule.

This action uses the following values:

- Type - CA Process Automation
- Start Request Form (SRF) - click the Search icon and select your simple fulfillment SRF from the list
- Configuration Name - All the CA Process Automation multiple instances are listed. Select the CA Process Automation to create the process instance.
- Parameters - When you select an SRF, the required input parameters are automatically listed. Either enter one or more custom values or select one or more values from the list.

When this action starts the Fulfillment (SRF), it passes the information necessary to assign a fulfillment needed task to the appropriate fulfillment user or group. Typically, you also use the CA Process Automation process called by the SRF to set the status of the requested item to Pending Fulfillment (1000).

Procurement Rules for CA Process Automation

The procurement rules for use with CA Process Automation are as follows:

- **When Category is Hardware and Status is Not Filled From Inventory** rule is launched when these conditions are satisfied:
  - old status <> 1003 - The old status is Not Filled From Inventory (1003)
  - new status = 1003 - The new status is Not Filled From Inventory (1003)
  - category = 1 - The service option element category is Hardware (1)
  - rate_item_col = 0 - This service option element is the first service option element in its row of service option elements
- **When Category is Software and Status is Not Filled From Inventory** rule is launched when these conditions are satisfied:
  - old status <> 1003 - The old status is not Not Filled From Inventory (1003)
  - new status = 1003 - The new status is Not Filled From Inventory (1003)
  - category = 0 - The service option element category is Software (0)
  - rate_item_col = 0 - This service option element is the first service option element in its row of service option elements
- **When Category is neither Hardware nor Software and Status is Not Filled From Inventory** rule is launched when these conditions are satisfied
  - old status <> 1003 - The old status is Not Filled From Inventory (1003)
  - new status = 1003 - The new status is Not Filled From Inventory (1003)
  - category > 1 - The service option element category is not None (-1), Software (0) or Hardware (1)
  - rate_item_col = 0 - This service option element is the first service option element in its row of service option elements

Define CA Process Automation Action

For each procurement rule, define a CA Process Automation action and associate it with the rule.

Each action uses the following values:

- Type - CA Process Automation
- Start Request Form (SRF) - click the Search icon and select your procurement SRF from the list
- Configuration Name - All the CA Process Automation multiple instances are listed. Select the CA Process Automation to create the process instance

- Parameters - When you select an SRF, the required input parameters are automatically listed. Either enter one or more custom values or select one or more values from the list.

When this action starts the Check Availability SRF, it passes the information necessary to assign a procurement task to the appropriate procurement user or group. Typically, you use the CA Process Automation process called by the SRF to set the status of the requested item to Pending Procurement (1012).

Received or Order Cancelled Rules

The Received or Order Cancelled rules for use with CA Process Automation are as follows:

- **When Category is Hardware and Status is Received or Order Canceled** rule is launched when these conditions are satisfied:
- old status <> 1007 - The old status is not Received (1007)
- old status <> 1008 - The old status is not Order Cancelled (1008)
- new status = 1007 OR new status = 1008 - The new status is Received (1007) or Order Cancelled (1008)
- category = 0 - The service option element category is Software (0)
- rate_item_col = 0 - This service option element is the first service option element in its row of service option elements.
- **When Category is Software and Status is Received or Order Canceled** rule is launched when these conditions are satisfied
  - old status <> 1007 - The old status is not Received (1007)
  - old status <> 1008 - The old status is not Order Cancelled (1008)
  - new status = 1007 OR new status = 1008 - The new status is Received (1007) or Order Cancelled (1008)
  - category = 0 - The service option element category is Hardware (1)
  - rate_item_col = 0 - This service option element is the first service option element in its row of service option elements
- **When Category is neither Hardware nor Software and Status is Received or Order Canceled** rule is launched when these conditions are satisfied
  - old status <> 1007 - The old status is not Received (1007)
  - old status <> 1008 - The old status is not Order Cancelled (1008)
  - new status = 1007 OR new status = 1008 - The new status is Received (1007) or Order Cancelled (1008)
  - category <> 0 and category <> 1 - The service option element category is neither Hardware (1) nor Software (0)

- rate_item_col = 0 - This service option element is the first service option element in its row of service option elements

Define CA Process Automation Action

For each Received or Order Cancelled rule, define a CA Process Automation action and associate it with the rule.

Each action uses the following values:

- Type - CA Process Automation
- Start Request Form (SRF) - Click the Search icon and select your Check Availability SRF from the list
- Configuration Name - All the CA Process Automation multiple instances are listed. Select the CA Process Automation to create the process instance
- Parameters - When you select an SRF, the required input parameters are automatically listed. Either enter one or more custom values or select one or more values from the list.

When this action starts the Check Availability SRF, it passes the information necessary to assign a check availability task to the appropriate fulfillment user or group. Typically, you use the CA Process Automation process the SRF calls to set the status of the requested item to Check Availability (1001).

Step 3 - Assign Users to Required CA Process Automation User Groups

You can launch the CA Process Automation client from the CA Service Catalog request tracking page. To do so, assign users to the appropriate CA Process Automation groups in CA EEM. Launch the client in context to an active CA Process Automation process.

When you install CA Process Automation, it creates the following user groups in CA EEM:

- PAMADMIN - the administrators user group
  By default, this group contains one member, named pamadmin, but you can optionally add others.
  Users in this group have complete administrative access to CA Process Automation.
- PAMUser - the user group for non-administrative users
  By default, this group contains one member, named pamuser, but you can optionally add others.

Assign the users to one of these groups. Verify that the users can launch the CA Process Automation client from the CA Service Catalog request tracking page.

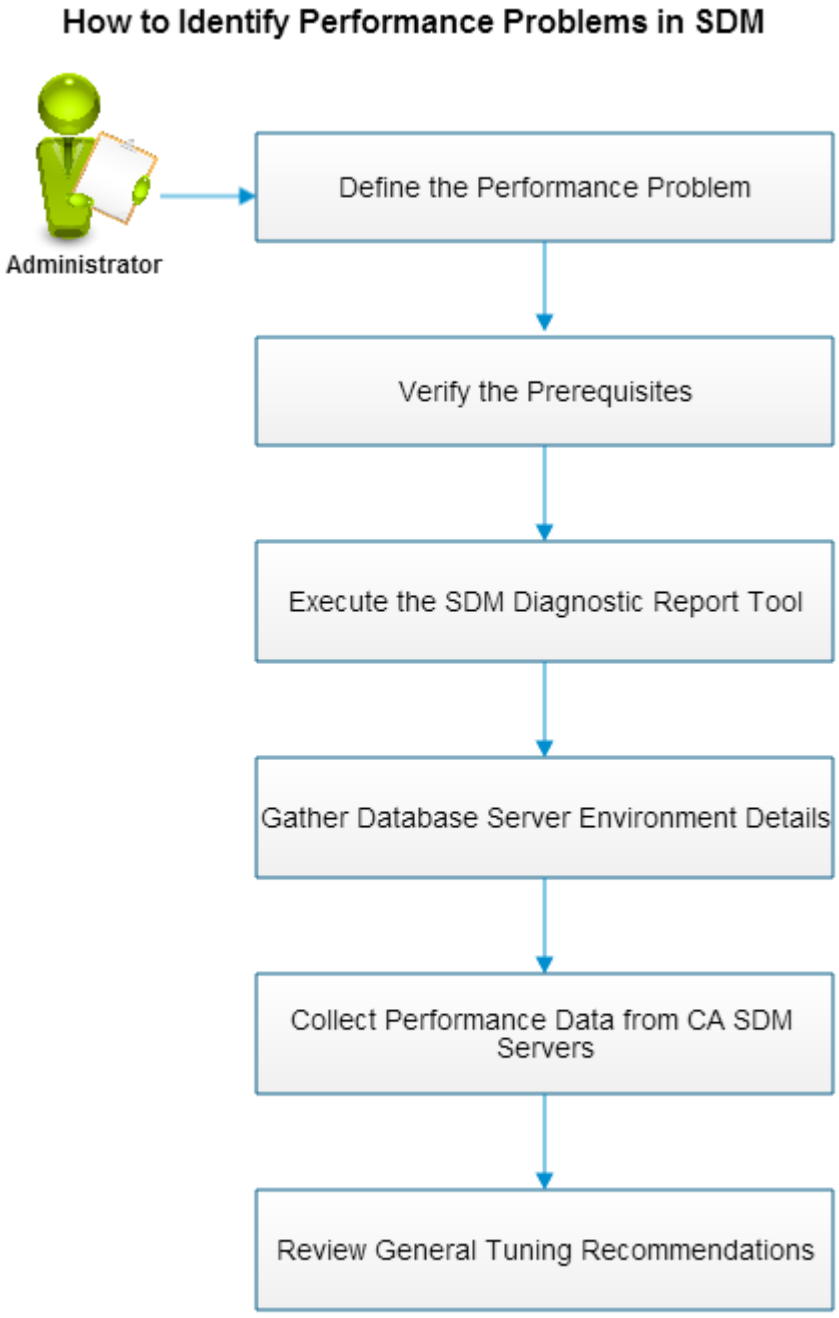
Troubleshooting CA Service Desk Manager

This section contains the following articles:

How to Identify Performance Problems in CA SDM

As a system administrator, you gather information about your installation environment, resource usage, configuration details, and other available system resources. For example, understand the computer configuration to determine the Operating System type, version, and available system resources. This data helps you to identify and diagnose a performance or memory-related issue in CA SDM. The CA Diagnostic Report tool and the Interval Logging utility help you collect diagnostic information about your CA SDM environment.

The following diagram describes how to gather diagnostic information and identify performance problems in CA SDM:



Follow these steps:

1. Define the Performance Problem (see page 3331).
2. Verify the Prerequisites (see page 3331)
   - Install PS Tools (see page 3332)

3. Execute the SDM Diagnostic Report Tool (see page 3332).
   - Collect Information from the CA Diagnostic Report Tool (see page 3333).
   - Verify Windows Report (see page 3334)
   - Verify UNIX Report (see page 3335)
   - Verify Collected Diagnostic Report (see page 3336)
4. Gather database server environment details (see page 3337).
5. Collect Performance Data from CA SDM Servers (see page).
   - Collect Usage Data using Interval Logging (see page 3338).
6. Review general tuning recommendations (see page 3341).

Define the Performance Problem

To define performance problems, begin by collecting the system information. Then consider the following example questions for relevance:

- What did users experience to disrupt their tasks?
- When did users first discover the problem?
- Has your environment changed recently, such as hardware upgrades?
- What functionality of the product experiences issues?
- How many users does the issue impact, and what type of users?
- What types of users are not impacted?
- What is the geographic location of the users that see the problem?
- What is the Access Level of the impacted users?
- Do you host CA SDM on a VMware ESX server or other virtualized environment?
- What other software are you running on the ESX server or host machine?
- What are the specifications of this environment?
- How many CPUs do you have on each computer?
- How much memory did you configure for each computer?

Verify the Prerequisites

1. For Windows operating system, install pslist.exe tools (see page 3332) and add its directory path variable on each CA SDM server.

2. Install and configure the CA SDM servers before running the diagnostic tool.

> **Note:** We recommend that you contact CA Support Online before you use the diagnostic tool.

Install PS Tools for Windows

> **Note:** For a Windows installation, install the pslist.exe tool and add its directory path variable to the system path variable.

Follow these steps:

1. Download PS Tools Suite from Microsoft.
2. Extract pstools.zip to any directory of your choice and add the directory to the Windows %PATH% environment variable.
3. Execute pslist.exe once manually from the command prompt as the Local System user and accept the license agreement. To execute pslist.exe as the Local System user, run the following command:

   ```
   psexec.exe -s -i pslist.exe
   ```

> **Note:** You can start the CA SDM Windows service under a different user account other than the Local System account. For that service, execute pslist.exe under that account and accept the license agreement. To add pslist.exe after installing and configuring CA SDM, accept the PsList license agreement and restart the CA SDM services.

Execute the SDM Diagnostic Report Tool

The CA Diagnostic tool creates a .CAZ file on the Windows OS and .tar.gz on UNIX in the $NX_ROOT\diag\rpt directory. You upload the file that the CA Diagnostic tool creates with your issue at http://support.ca.com.

Follow these steps:

1. Execute supp_diag.cmd on Windows, or execute supp_diag.sh on UNIX.
   The diagnostic tool can take five to 10 minutes to complete.

2. If the data collection process does not complete, navigate to the $NX_ROOT\diag\<host_name>_supp_diag.log log file. To determine the errors that occurred, examine the log file.

   Note: If you want to cancel the background batch job, use CTRL-C to cancel the batch file. Some processes still run in the background, such as MSINFO32.exe. If you have any questions about using this diagnostic tool, contact the CA Support Online.

3. The script directory structure displays the location of the script files, diagnostic zip files, and log files:

   - The $NX_ROOT\diag\bin directory contains script files.
   - The $NX_ROOT\diag\rpt directory contains the diagnostics zip file (in .caz format on Windows systems and in .tar.gz format on UNIX systems).
   - The $NX_ROOT\diag\misc_logs directory contains the log files that can be automatically included in the zip file.

4. To unzip the gathered files, complete the steps that are appropriate for the operating system:

   - **Windows**
   - Open a command prompt.
   - Cd to $NX_ROOT\diag\rpt or any directory where the .CAZ file is located.
   - Execute the following command:

     ```
     $NX_ROOT\diag\bin\cazipxp -u <package_name>.CAZ
     ```

   - **UNIX**
   - Open a command prompt.
   - Cd to $NX_ROOT/diag/rpt or any directory where the .tar or .tar.gz file is located.
   - Uncompress and untar the file:

     ```
     gunzip -d <package_name>.tar.gz

     tar -xvf <package_name>.tar
     ```

Collect Information from CA Diagnostic Report Tool

The CA SDM installation media includes the Diagnostic Report Tool to help collecting information for diagnosing performance problems. You can use the diagnostic tool to collect information relevant to the operating system. You can use the diagnostic tool to determine the commands for collecting data from CA SDM.

Configure the CA SDM server before running the diagnostic tool.

Follow these steps:

- **Windows**
- Set $NX_ROOT as your CA SDM installation root directory.
  The default for $NX_ROOT is the C:\Program Files\CA\Service Desk\ on Windows. You can change the default when you want to change the default directory during the installation process.
- Verify that the system path variable includes $NX_ROOT\bin.
- **UNIX/Linux**
- Set $NX_ROOT as your CA SDM installation root directory.
  The default for $NX_ROOT is -- /opt/CAisd/ on a Unix or Linux operating system. You can change the default when you want to change the default directory during the installation.
- Verify that your $PATH includes $NX_ROOT/bin.

Verify Windows Report

The following list describes the Windows report files that are created and included in the CAZ\tar file package.

- **Ca.olf**
  The Ca.olf report file specifies the CA licensing information from ca_lic directory.
- **Lic98.log**
  The Lic98.log report file specifies the log file that is related to CA licensing from ca_lic directory.
- **Lic98version.log**
  The Lic98version.log report file specifies the log file that is related to CA licensing from ca_lic directory.
- **Licdebug.log**
  The Licdebug.log report file specifies the file that is related to CA licensing from ca_lic directory.
- **Drwatsoninfo.txt**
  The Drwatsoninfo.text report file specifies the Dr. Watson configuration of the computer.
- **<host name>_env.txt**
  The <host name>_env.txt report file specifies the environment variables that are set on the computer.
- **<host name>_slstat.txt**
  The <host name>_sistat.txt report file specifies the output of slstat command.
- **<host name>_pdm_status.txt**
  The <host name>_pdm_status.txt file specifies the output of slstat command.
- **<host name>_dir_listing.txt**
  The <host name>_dir_listing.txt report file specifies the Service Desk install directory listing.

- **<host name>_pslist.txt**
  The <host name>_splist.txt report file specifies the process listing when the PsList Microsoft tool is installed.

- **<host name>_MSINFO32.NFO**
  The <host name>_MSINFO32.NFO report file specifies the MSINFO output gathering system information.

- **<host name>_SYSTEMINFO.TXT**
  The <host name>_SYSTEMINFO.TXT report file specifies the system information.

- **<host name>_appevents.csv**
  The <host name>_appevents.csv report file specifies the application event logs created in the past seven days.

- **<host name>_sysevents.csv**
  The <host name>_sysevents.csv report file specifies the application event logs created in the past seven days.

- **<host name>_hostinfo.txt**
  The <host name>_hostinfo.txt report file specifies the computer information.

- **<host name>_prodinstallinfo.txt**
  The <host name>_prodinstallinfo.txt report file specifies installation information for CA products.

- **<host name>_caprod_registry.txt**
  The <host name>_caprod_registry.txt report file specifies the Registry information of installed CA products.

- **<host name>_softfeatures.txt**
  The <host name>_softfeatures.txt report file specifies the list of software features that are installed for Service Desk.

- **<host name>_ipconfig.txt**
  The <host name>_ipconfig.txt report file specifies the IP configuration information.

- **<host name>_supp_diag.log**
  The <host name>_supp_diag.log report file specifies the log created for running the supp_diag tool.

Verify UNIX Report

The following list describes the UNIX report files that are created and included in the CAZ\tar file.

- **Ca.olf**
  The Ca.olf report file specifies the CA licensing information from ca_lic directory.

- **Lic98.log**
  The Lic98.log report file specifies the log file that is related to the CA licensing from ca_lic directory.

- **<host name>_env.txt**
  The <host name>_env.txt report file specifies the environment variables that are set on the computer.

- **<host name>_slstat.txt**
  The <host name>_slstat.txt report file specifies the output of slstat command.

- **<host name>_pdm_status.txt**
  The <host name>_pdm_status.txt report file specifies the output of the pdm status command.

- **<host name>_dir_listing.txt**
  The <host name>_dir_listing.txt report file specifies the Service Desk install directory listing.

- **<host name>_pslist.txt**
  The <host name>_pslist.txt report file specifies the process listing when the pslist Microsoft tool is installed.

- **<host name>_uname.txt**
  The <host name>_uname.txt report file specifies the output of the uname operating system command.

- **<host name>_diskinfo.txt**
  The <host name>_diskinfo.txt report file specifies the output of df operating system command.

- **<host name>_freemem.txt**
  The <host name>_freemem.txt report file specifies the output of memory information.

- **<host name>_supp_diag.log**
  The <host name>_supp_diag.log report file specifies the log created for running the supp_diag tool.

- **<host name>_prtconf.txt**
  The <host name>_prtconf.txt report file specifies the output of the prtconf operating system command on Solaris and the AIX computers.

- **<host name>_solrev.txt**
  The <host name>_solrev.txt report file specifies the OS version and patches Information on Solaris computers.

- **<host name>_netconf.txt**
  The <host name>_netconf.txt report file specifies the IP configuration Information on AIX computers.

Verify Collected Diagnostic Report

The default CA SDM documentation file\directory list includes the following reports in the CAZ\tar file. Add files or directories that you include in the CAZ\tar file by placing it in the $NX_ROOT\diag\misc_logs directory.

- $NX_ROOT/GENLEVEL or $NX_ROOT/.GENLEVEL

- $NX_ROOT/<COMPUTERNAME>.his

- $NX_ROOT/NX.env
- $NX_ROOT/NX.env.last
- $NX_ROOT/log\
- $NX_ROOT/pdmconf\
- $NX_ROOT/pdmconf\version
- $NX_ROOT/bopcfg\www*.cfg
- $NX_ROOT/site\mods\
- $NX_ROOT/site\ddict.sch
- $NX_ROOT/site\eh\
- $NX_ROOT/bopcfg\www\CATALINA_BASE\logs\
- $NX_ROOT/bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\web.xml
- $NX_ROOT/bopcfg\www\CATALINA_BASE\webapps*.xml

Gather Database Server Environment Details

You can gather details about your database server to help identify performance problems in CA SDM.

Follow these steps:

1. Determine the location of your database server, such as local or remote.
2. Determine the DBMS version, Operating System version, and patch level.
3. Complete the appropriate steps for your database type:
   - Execute the following queries for SQL Server and note the results:

     ```
     select @@version

     SELECT SERVERPROPERTY('productversion'), SERVERPROPERTY ('productlevel')
     ```

   - Execute the following query for Oracle:

     ```
     select * from v$version where banner like 'Oracle%';
     ```

4. Confirm the version of the database client that you installed on the application server.
5. If available, gather information about Environmental Data, such as the Operating System and other databases.

6. Gather network topology and topology information or other products that you integrate with CA SDM.
   For example, locate information about the products from available PDF files or diagrams.

Collect Performance Data from the CA SDM Servers

You can collect resource usage data on each SDM server in a multiple server configuration to determine the problems. The collected data sets are used to analyze and troubleshoot any performance or memory-related issues in the CA SDM servers. The interval logging utility allows you to start or stop the diagnostic data collection using the CA SDM web interface. Share the collected data set with CA Support Online. CA Support can help identify and resolve the CA SDM server problems.

Interval logging utility runs on pdm_intrvlog_nxd daemon that collects log data from a server. The daemon automatically starts when a Service Desk server start.

- To stop the interval logging daemon manually, remove the entry of interval logging utility from pdm_startup.
- To start the interval logging daemon manually, double-click the pdm_intrvlog_nxd.bat file in the $NX_ROOT/bin folder.

Collect Usage Data using Interval Logging

To collect the resource usage data on the CA SDM servers, configure the server for interval logging. You can select the type of data you want to collect from each server. You can change the logging options for the servers at any time.

For example, if you select only the CPU usage option, the utility collects only CPU usage data on the server.

Follow these steps:

1. Log in to CA SDM.
2. Select Systems, Interval Logging under the Administration tab.
   The Interval Logging Configurations List opens.
3. Click Create New to add an interval log configuration.
4. Complete the following fields:
   - **Server Name**
     The Server Name field specifies the server for which you want to collect the log data. Clicking Search displays the list of servers you can configure for the interval logging.
   - **Recurrence Interval**
     The Recurrence Interval field specifies the time interval during which the log data is collected for the server. For example, if the recurrence interval is set to 3 minutes, the log is collected for every 3 minutes.
     - **Default: 3 minutes**

- **Minimum: 2 minutes**

- **Enabled**
  The Enabled field indicates whether the interval logging is enabled or disabled for the server. If enabled, interval log is collected for the server.

  Note: To stop the interval logging before the scheduled end date, change the Enabled status to NO.

- **Record Status**
  The Record Status field indicates whether the interval log configuration is active or inactive.

- **Scheduled Start Date**
  The Scheduled Start Date field specifies the start date and time for collecting the log data. If a start date is not provided, interval logging starts immediately or whenever you activate and enable the configuration.

- **Scheduled End Date**
  The Scheduled End Data field specifies the end date and time for collecting the log data. If you do not enter an end date, interval logging runs until you inactivate or disable the configuration.

5. Select the appropriate log option that you want to collect from the server.
   For example, select CPU Usage if you want to capture the log for CPU usage data.

   - **CPU Usage**
     The CPU Usage log option collects CPU usage statistics for the server. This log option executes "pslist - x" on Windows and “ps” on UNIX. Depending on your configuration type, you can collect the diagnostic data on the following servers:

     - Conventional: Primary server.
     - Advanced Availability: All servers.

   - **Memory Usage**
     The Memory Usage log option collects memory usage data for the server. This log option executes the "pslist - m" command on Windows and the “ps” command on UNIX. Depending on your configuration type, you can collect the diagnostic data on the following servers:

     - Conventional: Primary server.
     - Advanced Availability: All servers.

   - **Network Status**
     The Network Status log option collects information on all active connections. This log option collects network statistics by executing the "netstat /b" command or the "netstat /a" command. Depending on your configuration type, you can collect the diagnostic data on the following servers:

- Conventional: Primary server.
- Advanced Availability: All servers.

- **Task List**
  The Task List log option collects application and services information for all tasks running on the server. Depending on your configuration type, you can collect the diagnostic data on the following servers:
  - Conventional: Primary server.
  - Advanced Availability: All servers.
- **Web Session Counts**
  The Web Session Counts log option collects CA SDM sessions and user statistics for the web engine processes. This log option executes the "pdm_webstat" command. You can collect the data for any CA SDM servers.
- **Server Status**
  The Server Status log option collects information about all the CA SDM daemons or processes on the server. This log option executes the "pdm_status" command. You can collect the data for any CA SDM servers.
- **DB Report**
  The DB Report log option collects information of database record types by executing the db_report command. You can collect the data for any CA SDM servers.
- **Virtual DB Info**
  The Virtual DB Info log option collects information that is related to the queued database requests. This log option executes the "pdm_vdbinfo" command. You can collect the data for any CA SDM servers.
- **List Server Connections**
  The List Server Connections log option collects information on active connections for the server by executing the pdm_listconn command. You can collect the data for any CA SDM servers.
- **List Slump Processes**
  The List Slump Processes log option collects information about slump connections and processes. This log option executes the "slstat" command. You can collect the data for any CA SDM servers.

6. Click Save.
   The server is configured for the interval logging.
7. (Optional) Repeat Steps 1-5 to create more interval log configurations.
8. Go to the $NX_ROOT\log directory and view the generated log files. The output files that are generated depend on the Interval Logging options you select, where files include:
   - cpu_usage_hostname
   - db_report_hostname

- memory_usage_hostname
- netstat_hostname
- pdm_listconn_hostname
- pdm_vdbinfo_hostname
- server_status_hostname
- session_counts_hostname
- tasklist_hostname

Important! The maximum limit of the output file size defaults to 30 KB. You can modify the file size by changing the @NX_LOGFILE_LIMIT value in NX_env file. If the generated output file exceeds the maximum file size limit, a new file is created. The new file name is appended with the suffix of 1. Files that are generated later have the suffix of the number incrementally.

You can share the collected log data with CA Support to help identify performance problems in your SDM installation.

Review General Tuning Recommendations

As a best practice, we recommend you to monitor the key performance indicators and the resource consumption regularly. Also, ensure that routine maintenance is applied to identify small problems before they become serious.

If you suspect an issue or users complain about slow performance, open a CA Support Online issue. Include information about the problem. For example, send the Interval Logging data, CA SDM Diagnostic Tool Report, and CA SDM standard logs. Send the information to CA Support from each CA SDM server.

The following list describes common signs of performance problems:

- The long messages in the CA SDM standard logs (stdlog.x files)
- Search for the messages in the stdlogs that state "The following query took #### milliseconds...".
- Queuing on database agents in pdm_vdbinfo output
- Search for *Queued Requests(#)* in the pdm_vdbinfo output. You can execute this command at the OS prompt manually. The Interval Logging script also executes this command.
- A large number of connected users to each web engine. For example, more than 200 users.

Note: To display the number of concurrent users per web engine, execute pdm_webstat. You can execute this command manually from the OS command prompt. The Interval Logging script also executes this command.

- User complaints
- When CA SDM is up and running, it is recommended to check the process memory. For optimal performance, we recommend the following method:

  1. Set a notification when the process memory exceeds 1.25 GB and begin a check on the processes that are running.
  2. Set a warning notification when the process memory exceeds 1.5 GB and take corrective actions to check the memory usage.

How to Monitor LDAP Using Trace Logging

This article contains the following topics:

To turn on trace logging to monitor LDAP use within CA SDM, use the pdm_logstat utility.

The pdm_logstat command has the following syntax:

```
pdm_logstat -f ldap_virtdb.c 1000
```

The following stdlog messages help you understand the status of the connection process.

Determine if ldap_virtdb Process Has Started

The first line to look for when analyzing stdlogs for LDAP messages is the startup of the ldap_virtdb process. The LDAP awareness for CA SDM begins only when this process starts.

Note: Even if LDAP integration options are not installed or set up, this process still runs.

```
06/03 17:00:18.27 cpasd1   bopLDAP       1964 SIGNIFICANT  ldap_virtdb.c
680 STARTUP of LDAP_virtdb
```

Determine if All Required Options are Installed

If any of the required LDAP options have not been defined, the stdlog shows the missing options. The following example shows the output:

```
06/03 17:00:18.72 cpasd1   bopLDAP  1964 SEVERE_ERROR ldap_virtdb.c  1023 LDAP Server
port id missing
06/03 17:00:18.78 cpasd1   bopLDAP  1964 SEVERE_ERROR ldap_virtdb.c  1023 LDAP Server
distinguished name missing
06/03 17:00:18.78 cpasd1   bopLDAP  1964 SEVERE_ERROR ldap_virtdb.c  1023 LDAP Server
distinguished name password missing
```

Determine if the LDAP Connection is Successful

You can identify whether the LDAP connection is successful by looking at the entries in the stdlog. The entries indicate that a connection is successfully established with the LDAP server. The following example shows the output:

```
06/05 12:35:10.41 cpasd1   bopLDAP  1912 SIGNIFICANT  ldap_virtdb.c  958 LDAP_SRVR
connecting to host(Francisco.us.danconia.net) port(389)
06/05 12:35:11.01 frisco   bopLDAP  1912 SIGNIFICANT  ldap_virtdb.c 1002 LDAP_SRVR
binding with username(simon)
```

Determine if the LDAP Connection is not Available

If you lose the LDAP server connection, the *LDAP Entries*, *Merge LDAP*, or any other LDAP functionality is disconnected and returns no results. In such circumstances, the stdlog displays messages as the following:

```
06/03 17:00:32.25 cpasd1   bopLDAP  1964 SIGNIFICANT  ldap_virtdb.c    219 LDAP
server not available; 'register_producer' not processed
06/05 10:52:57.63 cpasd1   bopLDAP  1896 SIGNIFICANT  ldap_virtdb.c    219 LDAP
server not available; 'select_full' not processed
06/05 10:52:57.66 cpasd1   web:local 1868 ERROR   sel_data_cache.  611 Error in ldap
Select_Cache method got_initial_count: LDAP server not available; 'select_full' not
processed
06/05 10:52:57.66 cpasd1   bopLDAP  1896 SIGNIFICANT  ldap_virtdb.c    219 LDAP
server not available; 'select_cancel' not processed
```

Determine Actual Filter Used

CA SDM fetches records from the LDAP Directory as per the search base, user search criteria, and the Options Manager filter definition. To determine the actual filter that the search request generates, look for the following message:

```
06/24 14:18:28.32 mcxxx04- bopLDAP    3844 TRACE   ldap_virtdb.c    853 Starting
select full: base=DC=kirklandsd,DC=ca,DC=com; filter=(&(objectCategory=person)(|
(sn=Jones)(pzLastName=Jones))); attributes=(uid,sAMAccountName,pzUserName,
distinguishedName)
```

Determine Attributes Fetched

CA SDM fetches records from the LDAP Directory according to the search base and the Options Manager filter definition. The SEARCH_BASE and attribute mapping as defined in ldap.maj and ldap_group.maj is checked for accuracy by the following message:

```
06/24 14:18:28.39 mcxxx04- bopLDAP       3844 TRACE     ldap_virtdb.c    766 Starting
select short: base=CN=John D. Jones,CN=Users,DC=kirklandsd,DC=ca,DC=com; filter=(&
(objectCategory=person)); attributes=(modifyTimestamp,sn,pzLastName,givenName,
pzFirstName,initials,pzMiddleName,uid,sAMAccountName,pzUserName,telephoneNumber,
pzWorkPhoneNumber,mobile,pzMobilePhoneNumber,department,pzDepartment,
facsimileTelephoneNumber,pzFaxPhoneNumber,pager,mail,pzEmailAddress,streetAddress,
pzAddress,l,pzCity,st,pzState,postalCode,pzPostalCode,c,pzCountry,o,memberOf)
```

Determine Which LDAP Data is Available and Not Available

```
06/24 14:18:28.41 mclda04- bopLDAP       3844 TRACE   ldap_virtdb.c   1396 Value not
available for 'modifyTimestamp'
06/24 14:18:28.41 mclda04- bopLDAP       3844 TRACE   ldap_virtdb.c   1396 Value not
available for 'telephoneNumber,pzWorkPhoneNumber'
```

When CA SDM maps successfully to the LDAP Object ID, the attributes are retrieved for each entry. These attributes are defined in $NX_ROOT/bopcfg/majic/ldap.maj. If the mapping is unsuccessful, a message is logged to indicate that an attribute is not defined.

Tomcat Logging

CA SDM uses a separate log4j.properties file for its web components such as Servlets and PDM_RPC. Support Automation, CMDB Visualizer, and REST also have a separate log4j.properties file. Starting or stopping the Tomcat logging does not require you to recycle the Tomcat daemons.

The following list describes how the log4j.properties files of CA SDM components differ:

- CA SDM monitors the log4j.properties in the NX_ROOT\site\cfg and in the NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF for changes.
- Support Automation monitors the log4j.properties in the NX_ROOT\bopcfg\www\CATALINA_BASE_SA\webapps\SupportAutomation\WEB-INF.
- CMDB Visualizer monitors the cmdbvisualizerlogging.properties in the NX_ROOT\bopcfg\www\CATALINA_BASE_VIZ\webapps\CMDBVisualizer\WEB-INF\classes.
- REST monitors the rest.log4j.properties in the NX_ROOT\site\cfg.

Use the pdm_log4j_config utility only for changing variables in the log4j.properties, cmdbvisualizerlogging.properties, and rest.log4j.properties files. You cannot use the pdm_log4j_config utility to modify the polling interval.

CA SDM checks the log4j properties files for any changes periodically. Configure the time interval by modifying the NX_LOG4J_REFRESH_INTERVAL variable in the NX.env file.

Servlet Defaults

The following servlets log INFO level messages to the jsrvr.log file by default:

- PDMContextListener – Log entry that is generated during the startup and shutdown of services.
- PDMweb -- Log entry that is generated from operations on the user interface.
- UploadServlet -- Log entry that is generated when you attach files to a ticket.
- pdmExport -- Log entry that is generated when you click Export on list forms.
- pdm_report -- Log entry that is generated when you click the Report menu on list forms.
- page_cache -- Log entry that is generated from operations on the user interface.
- BOServlet -- A log entry that is generated when you configure CA Business Intelligence and click the Reports tab.

REST Logging

REST uses the pdm_rest_util.jar and rest-core.jar packages, which contain log4j logging support. These components do *not* write any messages to the standard logs (stdlog.*), but through the log4j component. By default, these packages log INFO, ERROR, and WARN messages. Because the Java packages use the same log4j configuration properties file, each logs messages to the same output file. You view the *rest.log4j.properties* file in the $NX_ROOT\site\cfg\ directory.

To increase the log level to trace or debug, update the following section in the *rest.log4j.properties* file:

```
log4j.rootCategory=debug, jrestlog
```

Locate the output file, as defined in the configuration properties file in the following directory:

```
$NX_ROOT\log\jrest.log
```

Enable CXF Logging

CA SDM disables CXF logging by default because it can affect performance on a production environment. If your environment requires logging for debugging purposes, the administrator can modify the beans.xml file to enable CXF logging.

Follow these steps:

1. Locate the beans.xml file in the following directory:

   ```
   NX_ROOT\bopcfg\www\CATALINA_BASE_REST\webapps\caisd-rest\WEB-INF
   ```

2. Locate the following section of the XML file:

```
<cxf:bus>
    <cxf:features>
    </cxf:features>
</cxf:bus>
```

3. Add <cxf:logging/> to the section, as shown in the following example:

```
<cxf:bus>
    <cxf:features>
       <cxf:logging/>
    </cxf:features>
</cxf:bus>
```

4. Save the XML file.

Troubleshooting LDAP Configuration with CA SDM

This article contains the following topics:

The primary consideration when troubleshooting communications with an LDAP server is that seldom are any two LDAP implementations identical. The CA SDM utilities can verify that LDAP integration is working correctly.

Note:

CA SDM is preconfigured for integration with Microsoft Active Directory, eTrust, and iPlanet only. Integrating with other LDAP servers often requires changes and accommodations on both sides.

To monitor LDAP using the pdm_logstat utility, see How to Monitor LDAP Using Trace Logging (see page 3342).

Show Status of Daemons or Processes

The ldap_virtdb process manages interactions between CA SDM and the LDAP virtual database.

To show the status of all CA SDM daemons (UNIX) or processes

1. Execute pdm_status at the command line with no parameters:

```
pdm_status
```

The pdm_status command shows the status of all CA SDM daemons (UNIX) or processes (Windows). The following output is an example:

```
DAEMON                          STATUS      HOST      PID   SLUMP CONNECT TIME
-------------------------------------------------------------------------------
Agent antfarm                   Running     antfarm   455   Tue Feb 17 17:55:12
Ddict_rd             (ddictrd) Completed   antfarm
Data Dictionary   (ddictbuild) Completed   antfarm
...
User Validation      (boplgin) Running     antfarm   456   Tue Feb 17 17:55:21
```

2. Examine the command output for the status of the ldap_virtdb process.

slstat Command

Run the following command without parameters for verifying whether the bopLDAP is connected:

```
slstat
```

To see the status of bopLDAP, examine the command output.

NX.env File

To verify that the basic LDAP options are correctly installed, review the $NX_ROOT/NX.env file.

Depending on the LDAP options that are installed, the NX.env file consists of the following lines:

```
@NX_LDAP_DN=qauser
@NX_LDAP_ENABLE=Yes
@NX_LDAP_ENABLE_AUTO=Yes
@NX_LDAP_HOST=myserver
@NX_LDAP_PORT=389
@NX_LDAP_PWD=OBUNQXo7CmgbThZlCiMKIwJlA3UXdVNAOjUpHjstfDt2LBIDPgwtWA==
@NX_LDAP_SEARCH_BASE=dc=mycontroller, dc=xyz, dc=com
@NX_LDAP_SERVICE_TYPE=Active Directory
@NX_LDAP_SYNC_ON_NULL=Yes
@NX_LDAP_USER_OBJECT_CLASS=person
```

Important The Sun Java System Directory Server and Novell directory servers does not support paged searching. Hence, LDAP search, import, and sync are limited to the value of NX_LDAP_MAX_FETCH records per invocation. The default value is 100. To specify the maximum number of LDAP records, add the NX_LDAP_MAX_FETCH to your NX.env file. You can set NX_LDAP_MAX_FETCH to any value less than the value of LDAP_SIZELIMIT_EXCEEDED or LDAP_ADMINLIMIT_EXCEEDED on your LDAP server.

How to Connect CA SDM to the Office365 Servers Using SSL

Complete the following steps if you are unable to connect to Office365 servers:

1. Log in to outlook.office365.com using the credentials for the account that you wish to use with maileater.
   You are redirected to the login.microsoftonline.com page.

2. Save the root certificate from the login.microsoftonline.com page as a base 64 encoded.cer file, and copy it to the CA SDM server. Complete the following steps to save certificate:

   a. As an Administrator, click on the lock in the address bar of the page from where you want to save the certificate.

   b. From the Certification Path tab, select the root certificate and click View Certificate.

   c. From the Details tab, click Copy to File, and choose Base 64 Encoded x.509 (.CER) as the format.

3. Log in to CA SDM and use the same settings in the Mailbox details screen (ensure that you add the full email address and file path to the certificate that you saved).

4. Connect CA SDM to the Office365 servers and verify.

Troubleshooting CA Service Catalog

This section contains the following articles:

Maintain Log Files

CA Service Catalog includes log files, each of which is helpful for researching a specific component or a function. To maintain log files, follow these steps:

1. Review the names and locations of all log files (see page 3349).

2. Review the descriptions of the most frequently used log files (see page 3350).

3. Become familiar with the process of setting log levels (see page 3351).

4. Review the process of configuring rollover settings for selected log files (see page 3353).

5. To keep older rolled over log files from consuming excessive disk space, delete them manually at regular intervals.
   Verify that you comply with the file retention policy of your organization. By default, certain

log files are automatically rolled over and are automatically deleted periodically. Both processes occur according to your specifications when you configure rollover settings for selected log files (see page 3353). However, *no other* rolled over log files are automatically deleted; therefore, delete them manually.

Names and Locations of All Log Files

The following log files are located in the USM_HOME\logs folder:

- view.log
- view.log.1, view.log.2, view.log.3, and so forth
  You can configure rollover settings for these log files (see page 3353).

The following log files are located in the USM_HOME\logs\accounting folder:

- accounting.log
- AccountingService.log
- tomcat_fulfillment.log
- wf_admin.log
- wf_process.log
- wf_security.log
- wl.log
- wl.log.1, wl.log.2, wl.log.3, and so forth
  You can configure rollover settings for these log files (see page 3353).
- wsactorSoapRequest.xml
- wsactorSoapResponse.xml

The following log files are located in the USM_HOME\logs\install folder:

- acnt_seed_data.log
- createFiscalPeriod.log
- createRootOffering.log
- DeployServices.log
- importCommonReports.log
- importPlanningContent.log
- importPortalContent.log

- imq_cfg1.log
- imq_cfg2.log
- imq_cfg3.log
- InstallProducts.log
- ixerr.log
- ixutil.log
- seeddata.log
- sqlUtil.log
- usm_eiam_check.log
- usm_eiam_viewG.log
- usm_eiam_viewL.log
- usmInstall.log
- view_seed_data.log
- wf_seed_data.log
- workflow_install.log

The following log file is located in the USM_HOME\logs\LDAPImporter folder:

- LDAPImporter.log

The following log file is located in the USM_HOME\logs\view folder:

- postEvent.log
- tomcat_view.log
- ViewService.log

The following log files are located in the USM_HOME\logs\repagent folder:

- repagent.log
- RepositoryAgentService.log

Most Frequently Used Log Files

If a file is marked with an asterisk (*), you can set the logging levels (see page 3351) for the file.

- **accounting.log***
  Stores log messages that Service Accounting Component generates.
  This file is located in the USM_HOME\logs\accounting folder.

- **AccountingService.log**
  Stores log messages that CA Service Accounting Windows service generates.
  This file is located in the USM_HOME\logs\accounting folder.

- **ixutil.log***
  Stores log messages that the IXUtil import/export command-line utility generates.
  This file is located in the USM_HOME\logs folder.

- **repagent.log***
  Stores log messages that the CA repository agent generates.
  This file is located in the USM_HOME\logs\repagent folder.

- **RepositoryAgentService.log**
  Stores log messages that the Windows service of the repository agent generates.
  This file is located in the USM_HOME\logs\repagent folder.

- **seeddata.log***
  Stores log messages that the database containing the initial data that is supplied with CA Service Catalog generates. This initial data is required to get CA Service Catalog running immediately after installation.
  This file is located in the USM_HOME\logs folder.

- **view.log*, view.log.1*, view.log.2*, view.log.3*, and so forth**
  Store log messages that the Catalog Component component generates. The logs also contain rolled over log files (see page 3353) from previous days.
  These files are located in the USM_HOME\logs folder.

- **ViewService.log**
  Stores log messages that the Windows service of Catalog Component generates.
  This file is located in the USM_HOME\logs\view folder.

- **usmInstall.log**
  Stores log messages that the CA Service Catalog installation program generates.
  This file is located in the USM_HOME\logs\install folder.

- **tomcat_view.log***
  Stores log messages that Apache Tomcat hosting Catalog Component and the Service Accounting Component services generates.
  This file is located in the USM_HOME\logs\view folder.

Set Log Levels

Configuring the log level helps you maintain the log files and troubleshoot any problems that occur in your system.

Follow these steps:

1. Determine the log file whose output you want to control.

2. Determine the log4j.xml file (see page 3352) that controls the output of the log file whose log level you want to set.

3. Edit that log4j file and set the new logging level (see page 3352).

4. Review the contents of the affected log file after approximately 60 seconds. If necessary, reset the log level and review the contents again until you are satisfied with the level of detail.

Note: For more information about the logging features that CA Service Catalog uses, see the information about log4j at http://jakarta.apache.org

Log Files Controlled by Each Log4j.xml File

CA Service Catalog includes several log4j.xml files that control the output of the most frequently used log files. Each log4j.xml file controls the log file of CA Service Catalog services, as summarized in the following table:

Service Logged	Location of Log4j File	Log Files Controlled	Log file Location
Catalog Component	USM_HOME\view \conf	seeddata.logview. logtomcat_view.log	USM_HOME\logs\installUSM_HOME\logsUSM_HOME\logs\view
CA Service Fulfillment	USM_HOME\fulfillment\conf	tomcat_fulfillment.log	USM_HOME\logs\fulfillment
Service Accounting Component	USM_HOME\accounting\conf	accounting.log	USM_HOME\logs\accounting
Repository Agent	USM_HOME\repagent\config	repagent.log	USM_HOME\repagent\log
IXUtil import\export utility	USM_HOME\scripts	ixutil.log	USM_HOME\logs\install

Logging messages that are generated by a CA Service Catalog component, such as the Event Manager, are written to the log file of the calling service. Example: If the Catalog Component service calls the Event Manager, the log for the call is written in the view.log file. Calls from the Service Accounting Component service to the Event Manager are written to the accounting.log file.

Set the Log Level of a Service

You can set the log level to a higher level to investigate a problem. After you are finished investigating, you can reduce the log level for efficiency reasons.

Follow these steps:

1. Open the log4j.xml file (see page 3352) of the CA Service Catalog service whose logging level you want to set.

2. Find the following section:

```
<root>
    <priority value="log-level" />
    <appender-ref ref="accounting" />
    <!-- appender-ref ref="console" /-->
</root>
```

3. Specify one of the following values for the *log-level*:

   - **Fatal**
     Logs only errors that shut down a CA Service Catalog component. This log level typically provides the least detail. This log level requires the least amount of disk space for rolled-over log files and hence the least maintenance.

   - **Error**
     Logs all of the messages from the previous level and failed actions. For example, a user submitted a request, but the system did not present the request for approval.

   - **Warn**
     Logs all of the messages from the previous levels and warning messages. For example, a user creates a service with a name that is not unique.

   - **Informational**
     Logs all of the messages from the previous levels and messages that are informational only. For example, the total number of open database connections.

   - **Debug**
     Logs all of the messages from the previous levels and more detailed messages to help troubleshoot a problem. For example, debug messages can include every step of a multiple-step process.

   - **Trace**
     Logs every action and displays the final XML. This log level typically provides the most detail. This log level requires the most amount of disk space for rolled-over log files and the hence most maintenance.

4. Save and close the log4j.xml file.

5. Recycle the CA Service Catalog service whose logging level you updated.

Important! To make any *other* changes to any log4j file, consult CA Technologies.

Configure Rollover Settings for Selected Log Files

To maintain maximum efficiency, CA Service Catalog automatically rolls over selected frequently used log files, according to default settings. You can configure both the rollover size and the number of rolled over log files retained. Doing so helps you customize the log files to match the needs of your organization more closely.

Follow these steps:

1. Open the log4j.xml file (see page 3352) that controls the output for the log file that you want tc update. Use an editor of your choice.

2. Find the following section:

```
<appender name="view" class="org.apache.log4j.RollingFileAppender>
      <param name="File" value="${usm.home}/logs/view.log" />
      <param name="MaxFileSize" value="size" />
      <Param name="MaxBackupIndex" value="backup-index" />
      ...
</appender>
```

3. Specify the following settings:

   - ***size***
     Specifies the rollover size, in MB. For example, specify 5 to make the log file roll over when its size reaches 5 MB.
     Default: 10

   - ***backup-index***
     Specifies the number of recently rolled over log files that you want to keep on the disk. For example, 50.
     Default: 100

4. Save and close the log4j.xml file.

5. Verify that the log file output matches your needs. If necessary, reconfigure the log4j file or files to match your needs more closely.
   You have configured the rollover settings for selected log files.

Track Log Statements in Memory

This article contains the following topics:

The log appender or the in-memory appender allows writing messages to the memory until an error message occurs. Once the error message occurs, it is logged to the log file. The in-memory appender performs the following functions:

- Tracks all the log statements in the memory until an error occurs.
- Dumps the log statements in the error.log file from the memory.
- Discards the log statements or messages if no error occurs.

Note: The error.log is the default file name and you can rename it to a name of your choice.

The in-memory appender is implemented to log events under com.ca.usm package only. Using the in-memory appender improves the performance as the log statements are filtered at the appender level.

Step 1 - Complete the Prerequisites

You are required to have adequate knowledge of the Apache log4j.

Step 2 - Customize the Configuration File

Customize the appender section of the log4j.xml file by modifying the parameters in the log4j file.

Follow these steps:

1. Open the log4j.xml file from Installed_Loc/view/conf/ and modify the parameters for in-memory appender.
   You can customize the following in-memory appender parameters in appender section:

   - **File**
     Defines the path of the file where the in-memory logs are logged in case of an error.
     Default: <param name="File" value="${usm.home}/logs/error.log" />

   - **MaxFileSize**
     Defines the maximum size of the log file. Once the log file reaches the maximum size, the backup of the current log file is taken.
     Default: <param name="MaxFileSize" value="10MB" />

   - **MaxBackupIndex**
     Defines the maximum number of backup files to be restored on the system.
     Default: <param name="MaxBackupIndex" value="10" />

   - **MaxMemoryLogs**
     Defines the maximum count of logs in the memory. The appender then either recycles the logs in memory or moves them to temporary files on the disk.
     The following actions are performed on the temporary files:

     - If there is no error, the temporary files are discarded.

     - If there is an error, the logs in the temporary files are logged to the log file.
       The optimal value is tested to be 50000.

     Default: <param name="MaxMemoryLogs" value="50000" />

   - **MaxMemoryTime**
     Defines the maximum time in milliseconds for the logs that remain in memory. If the logs remain in memory for MaxMemoryTime, they are discarded.
     The optimal value is tested to be 600000 milliseconds.
     Default: <param name="MaxMemoryTime" value="600000" />

- **ConversionPattern**
  Defines the log statements that are logged based on the pattern provided. For more information about the ConversionPattern, see the Apache log4j documentation.
  The *{UNIQUEID}* helps to identify the complete request from the beginning until the end of the request.

```
<layout class="org.apache.log4j.PatternLayout">
 <param name="ConversionPattern" value="%d{yyyy/MM/dd HH.mm.ss.SSS} %-5p [%X
{UNIQUEID}] [%t] [%c{1}] %m%n" />
 </layout>
```

> **Important!** Do not update the logger name parameter of the logger section in the log4j.xml configuration file.

2. Save the file.
   You have customized the configuration file.

Step 3 - Update the Threshold Parameter in Default Console Appender

To update the log levels of the default console appender, update the threshold parameter to the required log level.

Follow these steps:

1. Open the log4j.xml file from Installed_Loc/view/conf/ and modify the threshold parameter of the default console appender. The following code sample shows the in-memory appender parameters:

```
<appender name="view" class="org.apache.log4j.RollingFileAppender">
    <param name="File" value="${usm.home}/logs/view.log" />
    <param name="MaxFileSize" value="20MB" />
    <param name="MaxBackupIndex" value="100" />
<param name="Threshold" value="INFO" />
    <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern" value="%d{yyyy/MM/dd HH.mm.ss.SSS} %-5p [%
t] [%c{1}] %m%n" />
    </layout>
  </appender>
```

2. Update the threshold value to INFO, where INFO is the required log level. For more information about the log levels, see the section Set the Log Level of a Service (see page 3352).

3. Save the file.
   You have updated the threshold parameter in the default console appender.

Step 4 - (Optional) Disable the In-Memory Appender

To disable the in-memory appender. comment the following logger section in the log4j.xml configuration file on each computer where CA Service Catalog is installed.

```
<logger name="com.ca.usm">
```

```
  <level value="ALL" />
  <appender-ref ref="memory" />
</logger>
```

Install or Upgrade Issues

This section contains the following issues:

- Product Installation or Upgrade Fails Because of Duplicate Records (see page 3357)

Product Installation or Upgrade Fails Because of Duplicate Records

Symptom:

During the installation or upgrade of CA Service Catalog, CA MDB is automatically installed or upgraded.

Example: CA MDB 1.0.4 is automatically upgraded to CA MDB 1.5 during the CA Service Catalog installation or upgrade. However, suppose CA MDB 1.0.4 is shared with other CA products. Then, the CA MDB upgrade can fail if duplicate records exist where the CA MDB tables require unique constraints. Examples include the following tables: ca_resource_class, ca_resource_family, ca_discovered_software, and cr_stat.

Solution:

Back up these tables, evaluate them, and clean up any duplicate records in them. Then try again to install or upgrade CA Service Catalog.

CA Service Catalog Request Management Issues

This section contains the following issues:

- Pending My Action page Is Not Refreshed Until User Logs Off (see page 3357)
- Request Approval or Fulfillment Pending Action Is Not Assigned (see page 3358)
- Requests Are Assigned to Multiple Users and Groups (see page 3358)
- Requests Do Not Move to the Next Status (see page 3358)

Pending My Action page Is Not Refreshed Until User Logs Off

Symptom:

After you add or remove a user from a group in CA EEM, the Pending My Action page is not refreshed.

Solution:

Log off and log in again to refresh the Pending My Action page.

Request Approval or Fulfillment Pending Action Is Not Assigned

Symptom:

An approval or fulfillment task for a request is assigned to a user or group. However, the request does not appear in the pending action list for the user.

Solution:

Use a user ID or group name not longer than 50 characters.

Requests Are Assigned to Multiple Users and Groups

Symptom:

CA Service Catalog assigns requests pending action to multiple users and groups.

Solution:

CA Service Catalog assigns requests pending action to *both* an Application group and a Global group that is defined in CA EEM when both the following conditions exist:

- Both groups have the same name in CA EEM.
- Both groups are configured to approve requests.

Consider renaming one of the groups or configuring one of them *not* to approve requests.

Requests Do Not Move to the Next Status

Symptom:

Requests do not move to the next status of the request life cycle as expected. Example: From Submitted to Pending Approval.

Solution:

To move requests to the next status of the request life cycle as expected, verify the related date settings.

Follow these steps:

1. Identify the status change where requests are getting stuck.
2. Verify that the related CA Process Automation processes are activated.
3. Verify the following:
    - Verify that you have enabled the rule actions for updating the request status of interest.

- Perform the following steps if you are using CA Process Automation to manage the request status change of interest:
  - Verify that the host name, port number, and other connection parameters for CA Process Automation are configured correctly.
  - Verify that the Global Data Set parameter points to the correct Catalog Component computer.
- Verify whether the assignees for the request are members of CA EEM groups whose names include special characters.
  If the assignees are members of such groups, the request statuses can fail to update. If necessary, rename the applicable groups in CA EEM so that their names do *not* include special characters.

4. Restart the CA Service Catalog Windows services. They are CA Service Catalog and CA Service Accounting.

Browser Issues

This section contains the following issues:

Pages Do Not Appear to Be Refreshing Properly

Symptom:

When I access CA Service Catalog, the pages do not appear as expected in my web browser.

Solution:

Set your browser cache settings to retrieve an updated page from the server on every visit to the page.

Note: For more information, see the documentation for your web browser.

Pop-up Window for Report Data Object Does Not Display Input Fields

Symptom:

I am trying to test a report data object with a query that uses a variable. The dialog for the test does not display the field for entering values for the variable. The problem occurs with all supported web browsers that I use to access CA Service Catalog.

Solution:

Try the following actions:

- Review the view.log file for errors.
- Verify that CA Service Catalog services are running on the computer that you are trying to log in to.
- Clear the browser cache.
- Verify that the trusted sites for the browser include CA Service Catalog.
- Verify that active scripting is enabled for the browser. The following example applies if you are using Internet Explorer:
    1. Select Tools, Internet Options, Security.
    2. On the internet zone, click Custom Level and select Active Scripting.
- Try adjusting other browser security settings.
- Try adjusting the network firewall settings.

If necessary, consult your network administrator for assistance with the previous two items.

Unable to View Invoice in CSV Format from Invoice History UI in HTTPS

Symptom:

I am using Internet Explorer to access CA Service Catalog. I cannot view invoices in CSV format from Invoice History in an HTTPS environment. The invoices do not display correctly.

Solution:

Follow these steps:

1. Open the Internet Explorer browser.
2. Select Tools, Internet Options, Advanced tab.
3. Scroll down to the Security setting.
4. Select the check box named Do not save encrypted pages to disk.
5. Click Apply.
6. Verify that the invoices display correctly.

Integration Issues

This section contains the following issues:

Errors for integration with CA APM

Symptom:

I am unable to integrate CA Service Catalog with CA Asset Portfolio Management.

Solution:

If CA Service Catalog is installed first and CA Asset Portfolio Management is installed later, you must recycle the CA Service Catalog Windows service and then proceed with the integration.

Symptom:

I get an error when trying to assign CA Asset Portfolio Management assets to a CA Service Catalog request item or to view associated assets. The error text is similar to the following: “Warning: A connection to the database could not be established.”

Solution:

The user does not have a role in CA Service Catalog. If the user is meant to be able to assign assets, then the user must use a role in CA Asset Portfolio Management that allows update access to the Asset Fulfillment security object. If the user is only meant to be able to view assigned assets, the user must use a role in CA Asset Portfolio Management which allows view access to the Asset Fulfillment security object, but not update access.

Symptom:

When trying to access CA Asset Portfolio Management, I receive a pop-up message saying "please wait" and CA Asset Portfolio Management opens very slowly or not at all. This error occurs when I use the Microsoft Internet Explorer browser. This error commonly occurs when I attempt to assign a CA Asset Portfolio Management model to a service option.

Solution:

Change your Internet Explorer settings to avoid the pop-up and the delay.

To change Internet Explorer settings:

1. Open the Internet Explorer browser.

2. In the browser bar, select Tools, Internet Options.
   The Internet Options dialog appears.

3. Click the Security tab.
   The security options appear.

4. Click the Local Intranet zone to select it, and click Custom Level.
   The security settings dialog for this zone appears.

5. Scroll to the Miscellaneous group and locate the option named Access data sources across domains.
6. Click Enable or click Prompt; do not click Disable.
7. Click OK to close the local intranet security settings dialog.
8. Click OK to close the Internet Options dialog.

Symptom:

I get an error when trying to assign CA Asset Portfolio Management models to a CA Service Catalog service option.

Solution:

One reason for this error is that the user does not have a role in CA Service Catalog. The user must use a role in CA Asset Portfolio Management that allows access to the Model security object.

Integration Fails

Symptom:

The integration fails between CA Service Catalog and other products. The other products can be CA Service Desk Manager, CA Business Intelligence, and CA Asset Portfolio Management.

Solution:

Verify that every computer with CA Service Catalog or an integrating product is set to the exact date and time. The date and time must also be adjusted for the time zone. This requirement applies to even the CA Service Catalog DBMS Server and integrating products DBMS Servers.

Example: Consider one of the computers is set to November 11, 6:27 p.m. Eastern USA. Now, all computers must be set to November 11, 6:27 p.m. Eastern USA or its equivalent, regardless of the computer's physical or geographic location. Some examples of equivalent dates and times for November 11, 6:27 p.m. Eastern USA are as follows:

- November 11, 3:27 p.m. Pacific USA
- November 11, 5:27 p.m. Central USA
- November 11, 9:27 p.m. Eastern Brazil
- November 11, 11:27 p.m. GMT
- November 12, 5:07 a.m. India Standard
- November 12, 7:27 a.m. China Standard

Methods for synchronizing the time and time zone on all computers include, but are not limited to, the following methods:

- Setting the time and time zone manually on each computer. For more information, see your operating system documentation.
- Configuring the Windows Time service to use an external time source or an authoritative time server. For more information, see the Microsoft web site.

Miscellaneous Issues

This section contains the following issues:

Cannot Add or Update a User Because of Duplicate User ID

Symptom:

When I try to add a new user or update an existing user ID, I receive the following error message:

```
Error - User with this user id already exists. Choose a different user id.
```

Solution:

A duplicate user profile exists. This problem can occur even if that user has been deleted. A deleted user is marked as inactive but the user is retained in the database.

Before assigning the user ID to a different user, remove the user ID from the inactive user.

Follow these steps:

1. Click Administration, Users.
2. Click the View Advanced icon option of the Search Users options.
3. Select User ID from the list of fields and select Contains from the list of operators.
4. Enter the user ID in the value field and click the Add link.
5. Select Inactive from the list of fields and select Equals from the list of operators.

6. Enter 1 for “true” in the value field and click the Add link.

7. Click Search.
   The list of users that match the selection criteria appears.

8. Edit the user: Change, or clear the User ID field, and click OK.

Cannot Connect to a Trusted Computer

Symptom:

I have integrated CA Service Catalog with CA Service Desk Manager. The two products use Secure Socket Layer (SSL) to connect to each other using a trusted relationship. However, when I test the connection, it fails. I also receive error messages that state there are no trusted relationship exists.

Solution:

- Verify that you have configured CA Service Catalog to use SSL.

- Verify especially that you have added self-signed certificates to the keystore, if applicable.
  When you use *self-signed* certificates for any computer that connects directly to CA Service Catalog, add these certificates to the keystore. **Example:** Suppose you want to use clustering with load balancing for CA Service Catalog. In that case, if you are using a self-signed certificate for the load balancing computer, add it to the keystore.
  Moreover, verify the computer to be trusted. Example: Suppose you want to integrate CA Service Catalog with CA Service Desk Manager through a load balancing computer. In that case, CA Service Catalog connects directly to the load balancer (not CA Service Desk Manager). Therefore, the computer to be trusted is the load balancer and not the CA Service Desk Manager computer.

Cannot Delete an Account

Symptom:

When I try to delete an account, a message appears indicating that I cannot delete this account.

Solution:

You cannot delete an account with an active subscription. Before you delete an account, prepare to delete it.

Follow these steps:

1. Cancel the subscriptions that are associated with the account.

2. Close the account by setting the status of the account to Closed.

3. Verify that all the billing runs affecting the account are completed.

Cannot Email a Request

Symptom:

I have CA EEM configured to use an external directory containing many groups. When emailing a request, I get the following error:

```
Cannot send email, please contact your administrator.
```

Solution:

To process the number of groups that are defined in your external directory, increase the value of CA EEM Max Search Size.

Follow these steps:

1. Click the embedded **CA EEM** link in the **Administration Quick Start** menu.
2. Log in using the EiamAdmin user name and password.
3. Click **Configure**, **Session**, **Configuration** menu option.
4. Change the **Max Search Size** to a value larger than the number of groups in your external directory.
5. Click Save.

Cannot Log In to CA Service Catalog

Symptom:

I cannot log in to a CA Service Catalog computer.

Solution:

- Verify that your user name and password are valid.
- Verify that the CA Service Catalog services are running on the computer that you are trying to log in to.
- Verify that the CA Service Catalog computer name does not contain an underscore, if you are using Internet Explorer to access CA Service Catalog. If an underscore appears in the computer name, perform one of the following steps:
  - Remove the underscore in the CA Service Catalog computer name. Update all references to the computer name throughout your environment. You can now use Internet Explorer to access CA Service Catalog.
    For more information about this Internet Explorer issue, see the related knowledge base article on the Microsoft web site.
  - Use Mozilla Firefox or Safari instead of Internet Explorer and then access CA Service Catalog.

Compilation Errors After Customization

Symptom:

After I customize files, multiple compilation-related error messages appear in the logs of Catalog Component computers.

```
...
yyyy/mm/dd computer-name-or-address ERROR [TP-Processor21] [DomProcessor] Error
Generating Document
javax.xml.transform.TransformerConfigurationException: Could not compile stylesheet
...
```

Solution:

- Review the instructions for customizing XSL, XML, JavaScript, and image files (see page 2018). Verify that you have followed all instructions.
- Verify that the filestore is set up correctly. Especially verify that *all* Catalog Component computers share the filestore.

Data Not Uploaded If CA Repository Agent Service Is Configured with Active Directory

Symptom:

Data sets are not uploaded if CA Service Catalog is configured for use with Active Directory. Exceptions appear in the RepositoryAgentService.log file.

Solution:

Install a secondary view server and do *not* configure this view server for use with Active Directory. Configure the CA Repository Agent services and files on this secondary view server. Use this secondary view server to upload the data in CA Service Catalog.

IXUTIL Out-of-Memory Error Occurs

Symptom:

When I use the IXUTIL utility to import or export CA Service Catalog data, the attempt fails. I receive an error message, such as a "generic" SAXException error.

Solution:

Open the ixutil.bat file. Increase the size of the JVM parameter in the ixutil.bat file to 1024 or higher.

Note: The ixutil.bat file is located in the USM_HOME\scripts folder.

Sorting of Services by Selection Type

Symptom:

When I view services in the catalog, they are not sorted by Selection Type as I expect them to be. Even the Featured Services are not sorted by Selection Type.

Solution:

When you create a service, you specify a Selection Type. The sorting of services according to Selection Type is controlled internally. The sort order is *not* based on the name of the Selection Type. Instead, the sort order is based on the *numeric value* of the Selection Type, as follows:

Numeric Value	Selection Type
0	No Selection
1	Single Selection
3	Multiple Selection

Windows Service Does Not Start

Symptom:

One or both Windows services for CA Service Catalog fail to start.

Solution:

The services are set by default to start automatically after a reboot or shutdown. If necessary, start the services manually.

Troubleshooting CA Asset Portfolio Management

This section contains the following articles:

Installation Does Not Start or Displays Server Not Found Error

Valid on all supported operating environments.

Symptom:

When starting the Unicenter APM installation, the installation does not start or you receive a Server Not Found error.

Solution:

Restart the UtilDev Web Server Pro Windows service.

Tenancy Management Page Cannot Be Displayed Browser Error Appears

Symptom:

The following browser error message appears when I click Administration, Tenancy Management:

```
Page cannot be displayed.
```

Solution:

Verify that the CA CASM service is started.

Tenancy Management Page Does Not Appear

Symptom:

When I click the Administration tab, I do not see a Tenancy Management option.

Solution:

Your Unicenter APM administrator has not assigned you to a role in which Tenancy Administration Access is enabled. If you need access to Tenancy Management, contact your Unicenter APM administrator.

Web Servers Named with Underscore Characters

Valid on all supported operating environments.

Symptom:

Using underscore characters in web server host names can cause problems. You see the problems when logging in to the product or when you use Embedded Entitlements Manager for user configuration.

Solution:

If you use a virtual or ghosted system, configure a new host name by creating another image without the underscore. For a production system, add a new host name to your internal Domain Name System (DNS). Adding a host name lets you access the product with a different URL.

Log In Fails with a User Name Containing Extended Characters

Symptom:

When using Embedded Entitlements Manager with Single DB Login authentication, I cannot log in to the Unicenter APM web interface.

Solution:

Select a User Name that does not contain extended characters (that is, Japanese or German characters).

WCF Services Fail when IIS 7 is Installed on Windows 2008

Valid on Windows 2008 operating environments.

Symptom:

When I have Microsoft Internet Information Services (IIS) 7 installed on Windows 2008, the WCF Services do not work. Unicenter APM uses a WCF Service to implement the web services function.

Solution:

This problem happens for one of the following reasons:

- The service file types are mapped incorrectly.
- The Windows components, including IIS 7, were installed in an incorrect order.

To correct the problem, verify and change (if necessary) the IIS settings. Microsoft provides information and solutions for the problem.

To resolve the problem, complete the following steps:

1. In a web browser, open the Microsoft website (http://www.microsoft.com) and search for "IIS Hosted Service Fails".
2. Follow the instructions in the article.

Missing Operating System Message Appears in Message Queue

Symptom:

I receive one of the following error messages in the message queue during the Reconciliation Engine processing of normalization rules:

- The following discovered operating systems are missing from the Public Operating System list:
  Missing Operating System: *operating system name*

- The following discovered operating systems are missing from the Operating System list and must be added to the Public Operating System list or the list for tenant: *tenant name*
  Missing Operating System: *operating system name*

Note: The Reconciliation Engine writes messages to the message queue in the database. To see these error messages in the message queue, set the Engine Debug Level in the Hardware Reconciliation Engine Configuration Settings to Fatal (or a higher level of detail). For more information about the message queue and the configuration settings, see Hardware Reconciliation (see page 2404).

Solution:

The normalization rules apply to all tenants and public data and can be used across tenants. If an operating system value assigned through the normalization list does not exist for a tenant, the Reconciliation Engine produces an error message.

Note: For more information about normalization rules, see Data Normalization (see page 2407).

If one or two operating systems are missing, resolve the problem by adding the operating systems manually to normalization rules.

If numerous operating systems are missing, complete the following steps to resolve the problem:

1. Log in to Unicenter APM and click Administration, Reconciliation Management.

2. On the left, click Reconciliation Message Search.
   The message queue displays reconciliation log messages in the Search Results.

3. Search to find the missing operating system normalization rule error messages.
   The message queue displays all missing operating system normalization rule error messages.

4. Verify that the system administrator email address in the product is correct and click Export to CSV.
   The operating systems that are missing are exported to a CSV file. The system administrator receives an email message with a link to the CSV file.

5. Edit the content of the CSV file to prepare the file for the ITAM Data Importer. For example, you can remove duplicate operating systems or extraneous words from the file.

> **Note:** For more information about using the ITAM Data Importer, see Import Data (see page 1622) section.

6. Log in to the CA APM.

7. Click Administration, ITAM Data Importer, and select the tenant or public data that is missing the operating systems.

8. Import the CSV file.
   The missing operating systems are imported into the Management Database and are available for use during Reconciliation Engine normalization processing.

Incorrect Database Configuration Results in Failure of Discovered Data Import from CA SAM

Symtom:

In the Software Asset Management Configuration page, you incorrectly select the database as Oracle. But you configured CA SAM on SQL database.

When you import data using the Data Importer, discovered data is not saved to the CA APM database as the database is wrongly specified. However, when you later specify the correct database and import the data, the data that was earlier discovered is not imported to CA APM.

Solution:

On the CA SAM database, run the following command using any compatible database client application:

```
delete * from dx_processes where dx_processes.file_name LIKE '%CA_SAM_Device_Export%'
```

Import Data to CA APM Installed on Oracle Database

You may encounter issues when you import data to CA APM that is installed on Oracle database. This article explains the various scenarios and the recommended tasks you must perform to import data successfully.

Terminologies you Must Know

Onboarding

Onboarding refers to the activity of importing data to the database for the first time. This is a one-time activity and does not repeat.

Ongoing

Ongoing refers to the activity of importing data to the database on a frequent basis. The frequency of data import may be daily, weekly, monthly, scheduled, or on-demand.

Pre-requisites

- If you are upgrading from UAPM 11.3.4 to CA APM 14.1, complete the CA APM installation and data migration using the CA APM Migration utility.
- If you are upgrading from ITAM 12.6, 12.8, or 12.9 to CA APM 14.1, then complete the CA APM 14.1 installation.

Recommendations for Data Import

The recommendation steps for the various scenarios only apply to the following environments:

- Oracle Database 11g, 12c
- Standalone installation of CA APM or CA APM integrated with CA SDM, CA Service Catalog, or CA ITCM.

Scenario 1: Onboarding Data More than 100 Thousand Records

To onboard data of more than 100 thousand records on a pristine CA APM Oracle Database, complete the following steps:

1. Stop the following Windows services:
   - CA APM Event ServiceCA APM
   - HW Reconciliation Engine
   - CA APM Registration Service
2. Verify that the CA APM Data Importer Engine Service is running.
3. Start the data import process.
4. After the data import is complete, start CA APM Registration Service.
5. After the registration is complete, start the following services:
   - CA APM HW Reconciliation Engine
   - CA APM Event Service

Scenario 2: Ongoing Data More than 25 Thousand Records

- Existing data on the database - 100 thousand Assets and/or 150 thousand Service Desk Configuration Items.
- Ongoing data load - More than 25 thousand records.

Follow these steps:

1. Stop the following Windows services:
   - CA APM Event Service
   - CA APM HW Reconciliation Engine
   - CA APM Registration Service
2. Verify that the CA APM Data Importer Engine Service is running.
3. Start the data import process.
4. After the data import is complete, start the following Windows services:
   - CA APM Registration Service
   - CA APM HW Reconciliation Engine
   - CA APM Event Service

Scenario 3: Ongoing Data Less than 25 Thousand Records

- Existing data on the database – Less than 25 thousand Assets/Configuration Item data records (record count of the table ca_owned_resource).
- Ongoing data load - Less than 25 thousand records.

No special steps are recommended. All the Windows services may continue to run.

Troubleshooting CA Service Desk Manager Connector

This topic contains the following information:

Verify that the CA SDM Connector Installed Successfully

Symptom:

I want to verify that the CA SDM Connector is installed successfully.

Solution:

Follow these steps:

1. Check if there are any errors in the Catalyst_SDMConnector_InstallDebug.log file or CatalystInstallDebug.log file.

   Note: These files are located in the %TEMP% directory.

2. If either of the log files has errors, open a support issue.
3. If there are no errors in either of the log file, complete the following steps:
   a. Open the CA Catalyst Registry Server UI using the following URL:

      ```
      https://<registryserver:port>/registry/carbon/admin/login.jsp
      ```

   b. Log in to the CA Catalyst Registry UI and browse to the following directory:

      ```
      \topology\physical\<SDM Connector NODE>
      ```

   c. Check if connector-modules.xml and startup.properties files are present in the directory.

   d. If either connector-modules.xml or startup.properties file is missing from the directory, then the CA SDM Connector installation has failed.

- Uninstall and reinstall the CA SDM Connector.

4. Verify that the CA SDM Connector installer has completed the steps to configure the CA Catalyst server. Complete the following steps to verify:

   a. Verify reconciledViews.xml content.

   b. Verify plannerpolicy.xml content.

   c. Verify plancontrol.xml content.

   d. Verify correlation.properties content.

Verify that the CA SDM Connector Started Properly

Symptom:

I want to verify that the CA SDM Connector started properly.

Solution:

Follow these steps:

1. Open the CA Catalyst Admin UI using the following URL:

   ```
   http://<<rose>-Server:port>/adminui
   ```

2. Log in to the CA Catalyst Admin UI.

3. Click CA SDM Container node from the left panel.
   The CA SDM Container node is expanded to display the CA SDM Connector and status of the CA SDM Connector.
   If the status of the CA SDM Connector is RUNNING, then the CA SDM Connector has started properly.

   Note: If you have just started the CA SDM Connector, wait for the CA SDM Connector nodes to move to the Running state before you perform any operation.

CA SDM Connector Fails to Start

Symptom:

The CA SDM Connector fails to start.

Solution:

The CA SDM Connector failed to start because of one of the following reasons:

- CA SDM Server is Down (see page)
- Login Failure (see page 3376)

CA SDM Server is Down

Symptom:

If the CA SDM server is down and you try to start the CA SDM Connector, the CA SDM Connector attempts to connect to the server a few times and shuts down. The following line appears in the ServiceDeskManagerConnector.log file located in the CATALYST_HOME/container/data/logs/ directory:

```
Unable to connect to Service Desk Manager.
```

Solution:

Complete the following steps to start the CA SDM Connector:

1. Ensure that the CA SDM Server is up and running.
2. Restart CA SDM Connector Container.

Login Failure

Symptom:

If the password of the logged-in user has changed in CA SDM, the CA SDM Connector fails to log in to CA SDM. The following line appears in the ServiceDeskManagerConnector.log file located in the CATALYST_HOME/container/data/logs/ directory:

```
Login failure
```

Solution:

Complete the following steps to start the CA SDM Connector:

1. Open the following directory from the command prompt:

   ```
   CATALYST_HOME\tools\encrypt
   ```

   Note: Ensure that java.exe is in the PATH.

2. Run encrypter.bat <New Password> command and copy the encrypted string output from the command.
3. Browse to the following directory from the https://registryserver:port/registry/carbon/admin/login.jsp (https://registryserverport) URL:

```
\topology\physical\<SDM Connector
Server>\modules\configuration\ServiceDeskManagerConnector.xml
```

4. Click Edit as Text.
5. Replace the value of the password with the encrypted string output that is copied from encrypter utility.
6. Click Save Content.
7. Restart the CA SDM Connector Container.

CA SDM Connector Container Fails to Connect to CA Catalyst Registry or CA Catalyst Server Container

Symptom:

The CA SDM Connector Container failed to connect to the CA Catalyst Registry or the CA Catalyst Server Container.

Solution:

The connection has failed because of one of the following reasons:

- CA Catalyst Registry or CA Catalyst Server Container Service is Down (see page 3377)
- CA Catalyst Registry Database Server or CA Catalyst Server Container Database Server is Down (see page 3377)
- Firewall Restrictions (see page 3378)

CA Catalyst Registry or CA Catalyst Server Container Service is Down

Symptom:

The CA Catalyst Registry or the CA Catalyst Server Container service is down.

Solution:

Complete the following steps to start the connection:

1. Start the CA Catalyst Registry or the CA Catalyst Server Container.
2. Restart the CA SDM Connector Container.

CA Catalyst Registry Database Server or CA Catalyst Server Container Database Server is Down

Symptom:

The database server used by the CA Catalyst Registry or the CA Catalyst Server Container is down.

Solution:

Complete the following steps to start the connection:

1. Start the database server.
2. Start the CA Catalyst Registry or the CA Catalyst Server Container.
3. Restart the CA SDM Connector Container.

Firewall Restrictions

Symptom:

If the CA SDM Connector and the CA Catalyst Registry are on different computers, then firewall restricts the connection.

Solution:

Ensure that the firewall is not blocking any port that is used for communication between the CA Catalyst Registry and the CA SDM Connector container.

Verify the Data Published By the CA SDM Connector

Symptom:

I want to verify the data published by the CA SDM Connector.

Solution:

Follow these steps:

1. Launch the following URL:

   ```
   http://<<rose>-server:port>/ca-rest/home
   ```

2. Log in with the credentials of the CA Catalyst server.
3. Click Browse by CI Type.
   A new page with the data source button is displayed.
4. Select ServiceDesk-CMDB and look for any CI or relationship information.

CIs are Not Displayed in CMDB

Symptom:

I do not see the CIs in the CMDB, even after running the Catalyst job or the Management profile with the enabled integration.

Solution:

Follow these steps:

- If the CIs appear in the Catalyst, then verify that you applied the correct registry configuration steps and recycled the CA Catalyst container service in the CA Catalyst server. When the CA Catalyst Server and the CA SDM Connector are online, perform the full synchronization using the Priming Utility. For more information, see the *CA Catalyst documentation*.
- If the CIs do not appear in the Catalyst, then ensure that the CA Catalyst server, the CA Configuration Automation Connector, and the CA SDM Connector are up and running. Then rerun the CA Configuration Automation Catalyst Job.

Catalyst UI Login Failure

Symptom:

I am unable to log in to the Catalyst UIs such as the Admin UI or USM Web View even though my credentials are correct. However, I am able to log in to the Registry UI with the same credentials.

Solution:

Follow these steps:

1. Ensure that CA Embedded Entitlements Manager is up and running.

   Note: The Registry UI does not use CA Embedded Entitlements Manager for its user validation.

2. Restart the CA Catalyst container service in the CA Catalyst server.
3. Restart CA Catalyst Admin UI service in the CA Catalyst server.

Failed to Launch In-Context to a CI in CA Configuration Automation

Symptom:

I am unable to launch in-context to a CI in CA Configuration Automation while viewing the CI in CA SDM.

Solution:

If the in-context button (CCA$) does not appear for the CIs, ensure that the MDR for CA Configuration Automation was configured. For more information, see Create an MDR Definition in CA SDM (see page 3373).

Relationships are not Displayed in CMDB

Symptom:

I am unable to view the relationships in CMDB.

Solution:

Check the CA Catalyst Profile in CA Configuration Automation to find out the relationship types that were chosen for the export. If you enable TWA, then the relationships appear in TWA after the CI transactions are loaded to CMDB from TWA.

CIs are Not Displayed in the ServiceDesk-CMDB Data Repository

Symptom:

I am unable to view the CIs in the ServiceDesk-CMDB data repository. However, I can view the CIs listed for the default CA Catalyst data repository in the USM Web View.

Solution:

You are unable to view the CIs in the ServiceDesk-CMDB data repository because you have enabled TWA while installing the CA SDM Connector. Complete the following steps to disable the TWA:

1. Browse to the following directory from the https://<registryserver:port>/registry/carbon /admin/login.jsp URL:

   ```
   \topology\physical\<SDM Connector
   Server>\modules\configuration\ServiceDeskManagerConnector.xml
   ```

2. Click Edit as Text.
3. Replace the value for enable_twa property to **false**.
4. Click Save Content.
5. Restart the CA Catalyst Connector container service on the CA SDM server.

> **Note:** If you do not want to disable TWA, follow the CMDB process of verifying and loading the CIs to CMDB using GRloader utility, provided by CMDB.

Limit the Data Exported to CMDB

Symptom:

I want to limit the data exported to CMDB.

Solution:

Follow these steps:

1. Use the CA Catalyst Profiles in CA Configuration Automation to determine which attributes are exported. The attributes include Network Discovery Gateway CIs, Hardware or Storage or Network Details components, and Relationship types. The default profile exports all the NDG CIs, each of the Hardware or Software or Network Details components, and all relationship types.

2. Use the Catalyst Jobs or Management Profiles to determine which servers or services, and blueprints are exported.

Troubleshooting CA CMDB and CA Configuration Automation Integration

This topic contains the following information:

Verify that the CA Configuration Automation Connector Installed Successfully

Symptom:

I want to verify that the CA Configuration Automation Connector started properly.

Solution:

Follow these steps:

1. Check if there are any errors in the Catalyst_CCAConnector_InstallDebug.log file or CatalystInstallDebug.log file.

   Note: These files are located in the %TEMP% directory.

2. If either of the log files has errors, open a support issue.
3. If there are no errors in either of the log file, complete the following steps:
   a. Open the CA Catalyst Server Registry UI using the following URL:

      `https://<registryserver:port>/registry/carbon/admin/login.jsp`

   b. Log in to the CA Catalyst Registry UI and browse to the following directory:

      `\topology\physical\<<ACM>_Connector NODE>`

   c. Check if connector-modules.xml and startup.properties files are present in the directory.
   d. If either connector-modules.xml or startup.properties file is missing from the directory, then the CA Configuration Automation Connector installation has failed.
      - Uninstall and reinstall the CA Configuration Automation Connector.

Verify that the CA Configuration Automation Connector Started Properly

Symptom:

I want to verify that the CA Configuration Automation Connector started properly.

Solution:

Follow these steps:

1. Open the CA Catalyst Admin UI using the following URL:

   `http://<CA_Catalyst_Server>:<port>/adminui`

2. Log in to the CA Catalyst Admin UI.
3. Click CA Configuration Automation Container node from the left panel.
   The CA Configuration Automation Container node is expanded to display the CA Configuration Automation Connector and status of the CA Configuration Automation Connector.

- If the status of the CA Configuration Automation Connector is RUNNING, then the CA Configuration Automation Connector has started properly.

Note: If you have just started the CA Configuration Automation Connector, wait for the CA Configuration Automation Connector nodes to move to the Running state before you perform any operation.

cca.log File Displays Exception Traces

Symptom:

The cca.log file shows errors with exception traces.

Solution:

Review and identify a resolution for the exceptions that appear in the cca.log file. The following possible exceptions may appear in the cca.log file:

- CA Configuration Automation Server Connection Exception (see page)
- Database Exception (see page 3384)
- JVM Port Binding Exception (see page 3385)

CA Configuration Automation Server Connection Exception

Complete the following steps to remove the CA Configuration Automation Server Connection Exception found in the cca.log file:

1. Check if the CA Configuration Automation server is online and can be pinged from the CA Configuration Automation Connector Server.
2. Check if there is any firewall that is blocking access to the necessary CA Configuration Automation server port from the CA Configuration Automation Connector server.

Important! If you have restarted the CA Configuration Automation server while starting the CA Configuration Automation Connector, restart the CA Catalyst container service on the CA Configuration Automation Connector server.

3. If the password of the CA Configuration Automation user has changed since the installation of the CA Configuration Automation Connector, update the password parameter in the CCAConnector.xml file from the CA Catalyst server Registry UI. Complete the following steps:
    a. Go to the following directory:

```
<ROSE>_HOME\ tools\encrypt
```

Note: Ensure that java.exe in present in the path.

b. Run encrypter.bat <New Password> command and copy the encrypted string output from the command.

c. Open the following URL:

```
https://<registryserver:port>/registry/carbon/admin/login.jsp
```

d. Browse to the following directory:

```
\topology\physical\<Configuration_Automation_Connector_Server>\modules\co
nfiguration\CCAConnector.xml
```

e. Click Edit as Text.

f. Replace the value for db.password with the value copied from the encryptor utility.

g. Click Save Content.

h. Restart the CA Catalyst Container service and verify it again.

Database Exception

Complete the following steps to remove the Database Exception found in the cca.log file:

1. Check if the database server is online and can be pinged from the CA Configuration Automation Connector server.

2. Check if there is any firewall that is blocking access to the necessary database ports from the CA Configuration Automation Connector server.

3. If the DB password has changed since the installation of the CA Configuration Automation Connector, update the db.password parameter in the CCAConnector.xml file from the CA Catalyst server Registry UI. Complete the following steps:

   a. Go to the following directory:

   ```
   CATALYST_HOME\ tools\encrypt
   ```

   Note: Ensure that java.exe in present in the path.

   b. Run encrypter.bat <New Password> command and copy the encrypted string output from the command.

c. Open the following URL:

```
https://<registryserver:port>/registry/carbon/admin/login.jsp
```

d. Browse to the following directory:

```
\topology\physical\<CA_Configuration_Automation_Connector_Server>\modules
\configuration\CCAConnector.xml
```

e. Click Edit as Text.

f. Replace the value for db.password with the value copied from the encryptor utility.

g. Click Save Content.

h. Restart the CA Catalyst Container service and verify it again.

JVM Port Binding Exception

Complete the following steps to remove the JVM Port Binding Exception found in the cca.log file:

1. Check if any process is using the port that is used for the notification_listen_port parameter during the CA Configuration Automation Connector installation.

2. If a port conflict exists after the installation, update the parameter in the CCAConnector.xml file from the CA Catalyst server Registry UI. Complete the following steps:

   a. Open the following URL:

   ```
   https://<registryserver:port>/registry/carbon/admin/login.jsp
   ```

   b. Browse to the following directory:

   ```
   \topology\physical\<CA_Configuration_Automation_Connector_Server>\modules
   \configuration\CCAConnector.xml
   ```

   c. Click Edit as Text.

   d. Replace the value of the notification_listen_port with the value that does not conflict with other ports on the CA Configuration Automation server.

   e. Click Save Content.

   f. Restart the CA Catalyst Container service and verify it again.

Verify that the CA Configuration Automation Connector Sent Data to the CA Catalyst Server Successfully

Symptom:

I want to verify that the CA Configuration Automation Connector sent data to the CA Catalyst Server successfully.

Solution:

Follow these steps:

1. Open the Catalyst USM web view using the following URL:

   ```
   http://catalystserver:8080/ca-rest/browse/type?mdr=all
   ```

2. Select CMDB-View from Data Source and check if the CIs are listed on the page.

3. If the CIs are not listed in the CMDB-View, complete the following steps:

   a. Ensure that the Catalyst Container Service of the CA Configuration Automation Connector is restarted when you started the CA Configuration Automation server.

   b. Check if the time settings on the CA Catalyst server and the CA Configuration Automation Connector server nodes are same to avoid connectivity issues.

   c. If you used the Catalyst Job to push the data from CA Configuration Automation Connector, verify completion of the Catalyst Job. This verification is applicable for the Management Profile based integration. If the Catalyst Job is complete, the log view on the CA Configuration Automation server displays the Job started and Job finished messages.

   d. Match the Check Sum Table (see page) with the projections of the CA Configuration Automation Connector.

Match the Check Sum Table

Match the Check Sum table with the projections of the CA Configuration Automation Connector. The CA Catalyst Persistence Store maintains the projections of the CA Configuration Automation Connector for every CI sent to the CA Catalyst server.

Follow these steps:

1. Run queries to find the failed CIs.

   Note: You must adapt the queries with the corresponding database names, passwords, and so on. The Database may also need to configure cross computer DB access for CA Configuration Automation and CA Catalyst databases.

   - Use the following query in SQL to identify the failed CIs:

     ```
     select ci_id = CASE CHARINDEX( '|', ci_typ)
     WHEN '0' THEN ci_id
     ELSE (ci_id + substring( ci_typ, CHARINDEX( '|', ci_typ) + 1, len(ci_typ)))
     END collate sql_latin1_general_cp1_ci_as from acm_catlst_ci_cksum
     ```

```
EXCEPT
select c_mdrelementid from [catalystdb].[dbo].t_ci_detail where c_mdrproduct
= 'CA:00033'
```

- Use the following query in ORACLE to identify the failed CIs:

```
CREATE PUBLIC DATABASE LINK catalystdb CONNECT TO catalystadmin IDENTIFIED
BY <Password> USING '//<DBServer>/<DB SID>';
select CASE instr( ci_typ, '|')
HEN 0 THEN cast( ci_id as NVARCHAR2(36) )
ELSE concat( cast( ci_id as NVARCHAR2(36) ) , substr( ci_typ, instr( ci_typ,
'|') + 1, length(ci_typ)))
END as c_mdrelementid
from acm_catlst_ci_cksum
minus
select c_mdrelementid from t_ci_detail@catalystdb where c_mdrproduct = 'CA:
00033'
```

2. Check the invalidCIs.log file from the CATALYST_HOME\container\data\log directory.

> **Note:** For each CI ID output that is received from the query, there exists a corresponding dump for the CI in the invalidCIs.log file.

- If either the invalidCIs.log file is empty or the CI ID is not present in the file, then the CI synchronization from CA Configuration Automation Connector to the CA Catalyst server is still in progress.

> **Note:** The synchronization and reconciliation activities on the CA Catalyst server are not instantaneous and results in the CIs to take time to get across to CMDB.

Failed to Select the Items to Synchronize Between CA Configuration Automation and CMDB

Symptom:
I am unable to choose the items to synchronize between CA Configuration Automation and CMDB. In the old CA Configuration Automation or CMDB CA Business Intelligence-boxed integration I could choose the CI types.
Solution:
A combination of the attribute profile and Catalyst Job or management profile helps you filter data. This filtering mechanism has no similarity with the previous CA Business Intelligence integration where the filter was using CI types.

Integrating

This section contains the following articles:

Integrating CA Service Desk Manager

This section contains the following articles:

Integrate with Other Products

You can integrate CA SDM with some of the CA Technologies products. For more information see the Green book (https://support.ca.com/phpdocs/7/common/greenbooks/CA_Service_Desk_Integrations_Vol_1_ENU.pdf).

Integrate with CA Portal

This article contains the following topics:

You can access CA SDM components through CA Management Portal and CA Portal.

Note: CA Management Portal and CA Portal are not shipped with CA SDM, and must be purchased and licensed separately. CA SDM provides only the most basic information for accessing CA SDM through Portal Administration. For detailed information, see the *CA Portal* and *CA Management Portal Server Administration Online Help*.

Verify CA SDM Web Interface Accessibility

After CA SDM is installed on a system, ensure that you can access the web interface through the tomcat server. For Portal Integration to work, the CA SDM Web Interface must be accessible through tomcat.

Note: For CA SDM LINUX server installation, set the LD_LIBRARY_PATH to $NX_ROOT/sdk /lib.

Install and Start CA Portal

For more information about CA Portal, see the *CA Portal Getting Started Guide* that applies to your installation.

Note: You can install CA Portal on the system where CA SDM is installed, or on a separate system.

Include Portlets

You can use the product to include CA SDM portlets in the portal.

Follow these steps to include portlets:

1. Log in to CA SDM and click Search from the Options Manager on the Administration tab.
   The Options List window appears.
2. Click Portal_Safe_List.
   The Portal_Safe_list Detail window appears.
3. Enter the *servername:portnumber* where the portal was installed in the Options Value Field.
4. Click Install.
5. Restart the CA SDM daemon.
6. Log in to CA Portal as an administrator.

7. Create a user which is valid CA SDM User. For more information about how to create a user, see the CA Portal documentation.

   Note: The password that is used to create this user in the portal could be different from the password that the same user uses to log in to CA SDM. This is because, CA SDM authenticates the users for this integration using a combination of the username, a valid CAPortalsession, and the CA Portal install value. The CA Portal install value is used only if it exists in the PORTAL_SAFE_LIST option.

8. Select Knowledge from the main CA Portal menu bar.
   The Knowledge page appears.

9. Select Library from the left pane Knowledge bar.
   The Library tree appears in the left pane.

10. Create a folder in the Library and then select it. Select Publish File from the Knowledge bar.
    The Publish File form opens.

11. Type the following CA SDM portlet URL in the Content text box on the General Information tab:

    ```
    http://hostname:portnumber/CAisd/PortalServlet?USERNAME=$USER.
    username$&PORTALSESSION=$SESSION$&PORTALINSTALL=portalhostname:portalportnumber
    ```

    Note: Substitute the *hostname:portnumber* parameter with the name and port of the web server on which CA SDM resides. Substitute the *portalhostname: portalportnumber* parameter with the name and port of the web server on which Portal resides.

12. Enter CA SDM in the Title text box.

13. Click Advanced.
    The Advanced properties page of the Publish File form displays.

14. Enter *portal/variable-url* in the Content (mime) Type field and click Publish.
    The published contents appear in the selected Library folder.

15. Configure the Workplace to display this portlet.

16. Log out and log in as the newly created user. You are automatically logged in to CA SDM in the portlet you have created.

Note: If CA SDM is running in a portlet, the preference Avoid Popups is not available in the Preference page. A popup window is used regardless of the setting of the preference.

Connect to the CA Portal Server

To connect to the CA Portal server, open a web browser, and enter the following URL:

```
http://<servername>:<port#>/servlet/portal
```

- **<servername>**
  Specifies the server name (or IP address) of the portal server.

- **<port#>**
  Specifies the port number that the CA Portal server monitors. You specified the port number during the CA Portal server installation. The default port is 8080.

Configure CA SDM to Use SSL with CA Portal

Note: For production purposes, we recommend that you obtain a certificate from a trusted certificate authority.

Before configuring CA SDM to use SSL, verify if the CA Portal and CA SDM integration works without SSL. If the integration works without SSL, you can include portlets.

Setup SSL Using a Self-Signed Certificate

To set up the CA SDM Portal Integration using a self-signed certificate

1. At the command line, enter:

   ```
   %JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA
   ```

   Answer the prompts appropriately and enter "changeit" as the password for both password prompts.
   The certificate is now set up.

2. Edit the server.xml file that is located in:

   ```
   $NX_ROOT/bopcfg/www/CATALINA_BASE/conf
   ```

4. Uncomment the following section and save:

   ```
   <!--
   <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
      port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
   acceptCount="100" debug="0" scheme="https" secure="true"useURIValidationHack="
   false" disableUploadTimeout="true">
   ```

```
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
clientAuth="false" protocol="TLS" /></Connector>
-->
```

5. Add keystoreFile attribute to server.xml. (When you run the command in step 1, a .keystore file is created in the home directory of the user. Add the reference to the keystoreFile attribute and Save the file. Your server.xml appears as follows.

```
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
acceptCount="100" debug="0" scheme="https" secure="true"  useURIValidationHack="
false" disableUploadTimeout="true">
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
clientAuth="false" protocol="TLS" keystoreFile="location/.keystore" />
 </Connector>
```

6. Restart CA SDM.

7. To verify the SSL functionality, point your browser to *https://hostname:8443*. The browser displays a Security Alert dialog. Click Yes.

> **Note:** SSL uses port 8443.

8. Replace the CA SDM portlet to use HTTPS and port 8443.

```
https://hostname:8443/CAisd/PortalServlet?
USERNAME=$USER.username$&PORTALSESSION=$SESSION$&PORTALINSTALL=portalhostname:
portalportnumber
```

Connect to CA SDM when CA Portal Uses SSL

You can import the CA Portal Server Certificate so that a trusted connection can be made between CA SDM and CA Portal. The connection can be made only when CA Portal is configured to use SSL.

To connect to CA SDM when Portal Uses SSL

1. Verify that CA Portal is configured and works with SSL.

> **Note:** For information about the verification process, see your CA Portal documentation.

2. Export the certificate from the computer on which CA Portal is installed by following these steps:

    a. Locate the server.xml file at the following location:

```
PORTAL_Install_Dir\jakarta-tomcat-4.1.29\conf.
```

b. Note the keystore location and password (pwd), as illustrated in the following lines in server.xml. The default password is *changeit* (all lower case). If you used a custom password while creating the certificate during the portal setup, you have to use the custom password. For information, see your CA Portal documentation. In the following steps and examples, *changeit* is the default password used:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
   port="8443" minProcessors="5" maxProcessors="150"
      enableLookups="true"
      acceptCount="100" debug="0" scheme="https" secure="true"
      useURIValidationHack="false" disableUploadTimeout="true">
 <Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
      keystoreFile="c:\Program Files\CA\SC\Unicenter Management
Portal\UMPkeystore"
      keystorePass="changeit"
      clientAuth="false" protocol="TLS" />
    </Connector>
```

c. Navigate to the JRE bin directory (PORTAL_Install_Dir\ jre\bin) on the portal server computer. This directory includes the keytool utility that you use for exporting the PORTAL Server certificate to a file.

d. Access the keytool utility, using the following command:

```
keytool -export -alias tomcat -file umpserver.cer -keystore "c:\Program
Files\CA\SC\Unicenter Management Portal\UMPkeystore"
```

Enter the keystore password: changeit
Certificate is stored in the file <umpserver.cer>

Note: When prompted for the password, use the password that is obtained from step 2b. In the previous example, *changeit* is the password noted in step 2b. The keystore location is also obtained from step 2b.

3. Import the certificate that is obtained from the server to the computer containing the CA SDM installation by using the keytool utility, Complete the following:

a. On the CA SDM computer, navigate to the JRE\bin directory directory, typically at the following location:

```
C:\Program Files\CA\SC\JRE\bin.
```

b. Import the certificate into the Certification authority that is used by the CA SDM Java Virtual Machine.
The following example illustrates an import. In this example, the location of the Certificate authority is as follows:

```
C:\Program Files\CA\SC\JRE\1.4.2_06\lib\security\cacerts
```

When prompted for a *pwd*, enter “changeit”. When prompted for *Trust this certificate*, enter Yes.

```
Keytool.exe -import -alias tomcat -trustcacerts -file umpserver.cer -
keystore "C:\Program Files\CA\SC\JRE\1.4.2_06\lib\security\cacerts"
Enter keystore password:  changeit
Owner: CN=ump001.ca.com, OU=unicenter, O=ca, L=islandia, ST=ny, C=us
Issuer: CN=ump001.ca.com, OU=unicenter, O=ca, L=islandia, ST=ny, C=us
Serial number: 43ecb469
Valid from: Fri Feb 10 10:42:33 EST 2006 until: Thu May 11 11:42:33 EDT
2006
Certificate fingerprints:
         MD5:  A1:AF:AE:92:39:2E:53:D5:1C:6D:FE:44:68:61:DD:5C
         SHA1: 66:3A:BC:77:32:81:60:89:70:B9:EF:FB:74:3D:93:74:CD:8E:E2:
D2
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Note: When prompted for the password, use the password that is obtained from step 2b. In the previous example, *changeit* is the password noted in step 2b.

4. Edit the file portal-xml-api.xml under $NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\xml\portal-xml-api.xml by completing the following steps:

   a. Replace http in following the line:

   ```
   <!DOCTYPE PORTAL SYSTEM "http://127.0.0.1:8080/servlet/media/xml/api
   /request.dtd">
   ```

   With https:

   ```
   <!DOCTYPE PORTAL SYSTEM "https://127.0.0.1:8080/servlet/media/xml/api
   /request.dtd">
   ```

   b. Save the file.

   c. If Portal_Safe_List has been installed, ensure that you change the port number to 8443 and the computer name to include the domain name. For example, computername.ca.com:8443.

Note: Include the domain name in the computer name as the portal certificate contains the domain name. For more information, see your CA Portal documentation.

5. Recycle the CA SDM server.

6. From CA Portal, connect to the CA SDM Portlet using the following URL:

```
http://hostname:portnumber/CAisd/PortalServlet?USERNAME=$USER.
username$&PORTALSESSION=$SESSION$&PORTALINSTALL=servername:8443
```

> **Note:** Substitute *servername* in the URL with the name of the web server on which CA Portal resides. The server name in this URL must include the domain name, for example, servername.ca.com:8443. Substitute the hostname:portnumber with the name and port of the web server on which CA SDM resides.

Integrate with Mainframe Product

The CA SDM data (.dat file) associated with a mainframe product integration is in a list that associates a .dat to the mainframe product name.

> **Note:** The CA SDM server is configured, by default, to use ITIL methodology.

To load CA SDM side data to enable a particular integration, use *pdm_userload -f integXXX.dat*.

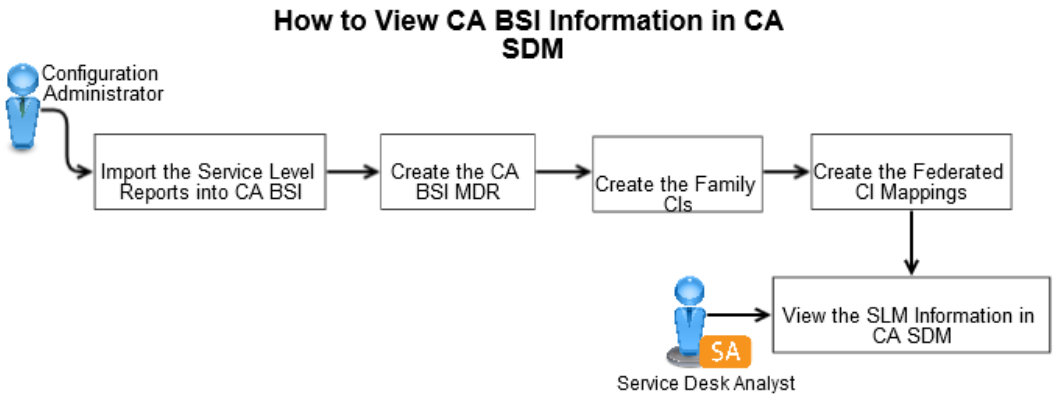
The data files are delivered to $NX_ROOT\data\integrations\.

For more information about enabling the calling side (mainframe product side) of the integration, see the *CA Common Services for z/OS - CA Service Desk Integration Guide*.

Integrate CA Service Desk Manager with CA Business Service Insight

An organization wants to improve the management of changes to IT services and decides to integrate CA BSI and CA SDM. The integration lets CA BSI export Service Level Management (SLM) information into CA SDM. The Configuration Administrator imports the reports into CA BSI and configures CA SDM so that a Service Desk Analyst can view the SLM information. Service Desk Analysts work with this information to improve IT service delivery.

The following diagram explains how a Configuration Administrator enables CA BSI to export SLM data to CA SDM so that a Service Desk Analyst can view the information:



1. Import the Service Level Reports into CA BSI (see page).
2. Create the CA BSI MDR (see page 3397).
3. Create the Family CIs (see page 3397).
4. Create the Federated CI Mappings (see page 3398).
5. View the SLM Information in CA SDM (see page 3398).

Import the Service Level Reports into CA BSI

CA BSI provides the *Service Level Compliance* report by default. The BSI Service tab appears on CI detail pages in CA SDM and displays Exceeds and Violations counts. You import the *Modified Service Level by Metrics vs Target* and *Modified Service Level by Contract vs Target* reports into CA BSI.

Follow these steps:

1. Copy the $NX_ROOT/samples/BSI/bsireports.sql file to the CA BSI database server.
   This Oracle script contains the report definitions that are required for the integration between CA BSI and CA SDM.
2. Connect to the CA BSI Oracle instance with a user that has the SYSDBA role. Or, connect as the database owner.

   Important! This user *must* have update rights to the database. Confirm if you have these privileges with your Oracle Database Administrator.
3. Execute the bsireports.sql script and verify that no errors occur.
   The reports are available for the CA SDM integration.

Create the CA BSI MDR

The Configuration Administrator creates an MDR for CA BSI in CA SDM. This MDR provides information about the CA BSI server, such as the host name and privileged user ID.

Follow these steps:

1. On the Administration tab, click CMDB, MDR Management, MDR List.
2. Click Create New.
3. Complete the following example information:
   - Enter **BSI** as the Class name.
   - Enter labels for the button and MDR names.
     For example, you enter **BSI**.
   - Enter the host name of the CA BSI server.
   - Enter **sadmin** as the Userid to BSI server and enter **CA** (must be an organization name that is configured in BSI server) as the Shared Secret.

     Note: This information depends on your user name and organization. Confirm this information with your CA BSI Administrator.
   - Delete all the contents of the URL to Launch in Context field.
4. Click Save and close the window.

Create the Family CIs

Create the Enterprise Service and Contract Family CIs in CA SDM. These CIs correspond to CA BSI data that you want to view in CA SDM. In this example, you create Service 1 and Contract 7.

Follow these steps:

1. On the Administration tab, click CMDB, CI List.
2. Click Create New.
3. Complete the following information:
   - Enter **Service 1** as the name.
   - Enter **Business Service** as the Class.
4. Click Continue.
5. Click Save and close the window.

6. Create another CI with the following information:
   - Enter **Contract 7** as the name.
   - Enter **License Agreement** as the Class.
7. Click Continue.
8. Click Save and close the window.

Create the Federated CI Mappings

Create the Federated CI Mappings to complete the integration between CA BSI and CA SDM. This mapping provides information about a CI. In this example, you map Service 1 and Contract 7 to the BSI MDR. The Integration component does not verify if the CI Name in CMDB matches with Federated Asset ID. However, this component only verifies the family name of a CI and its MDR class name BSI.

Follow these steps:

1. On the Administration tab, click CMDB, MDR Management, Federated CI Mapping.
2. Click Create New.
3. Complete the following fields:
   - Enter the CI Name and Federated Asset ID.

     Note: Federated Asset ID must be the name of an existing service in BSI, while the CI Name can be anything.

   - Enter the MDR Name.
4. Click Save and close the window.
5. Repeat steps 2 through 4 for the contract CI.

   Note: Federated Asset ID must be the name of an existing contract in BSI, while the CI Name can be anything.

View the SLM Information in CA SDM

The Service Desk Analyst views the SLM information to manage changes to IT services within your organization. For example, you want to analyze the violations that appear for Service 1.

Follow these steps:

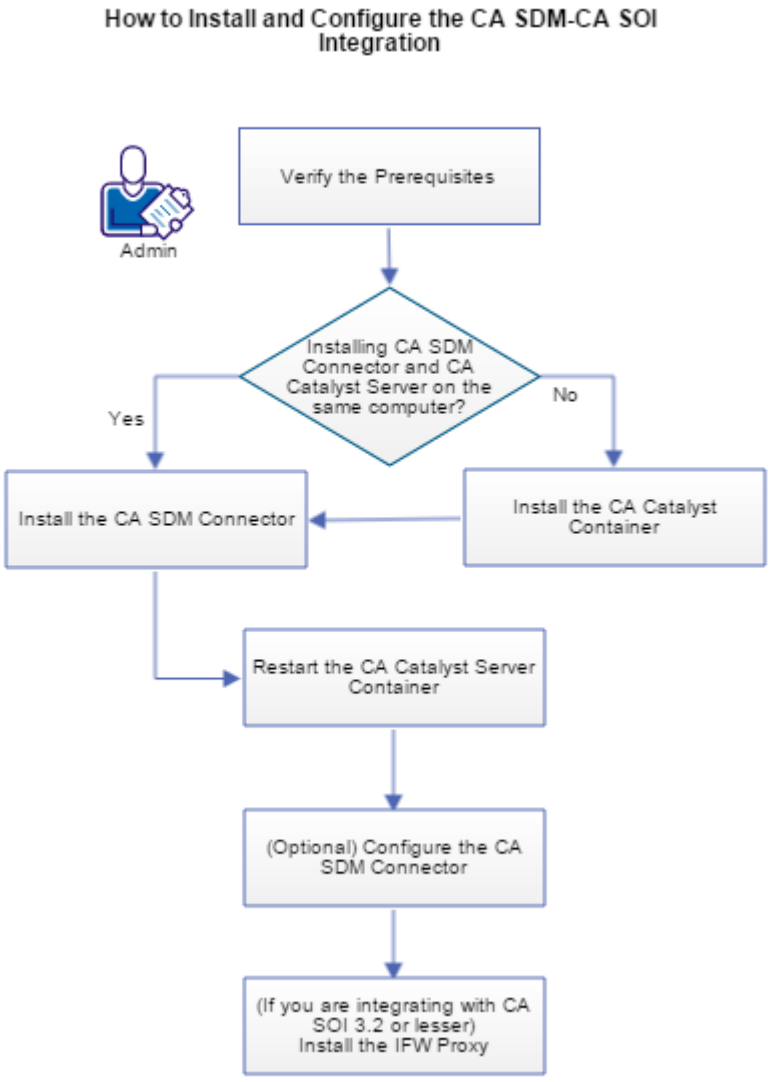
1. On the Administration tab, click CMDB, CI List.
2. Search for the Enterprise.Service and Contract Family CIs that you integrated with CA BSI.
3. Open an Enterprise.Service Family CI to view the BSI Service and BSI Service Metric tabs.
4. Click BSI Service to view Exceed and Violation information from *Service Level Compliance* data in CA BSI.
   The Exceeds and Violations data from the CA BSI *Service Level Compliance* report appears for Service 1.
5. Click BSI Service by Metric to view the Metric, Violation, Compliant, and Target report from the *Modified Service Level by Metric vs Target* data in CA BSI.
6. Open a Contract Family CI that you integrated with CA BSI and click the BSI Contract by Metric tab.

> **Note:** Contact CIs contain the BSI Contract by Metric tab. This tab contains a text box where you enter the Contract Party of the Contract to retrieve information from the *Modified Service Level by Contract vs Target* report in CA BSI.

You have now successfully integrated CA BSI with CA SDM to view SLM information in CA SDM.

Integrate with CA Service Operations Insight

The following diagram describes how to install and configure the CA SDM and CA SOI integration:



Follow these steps:

1. Verify the Prerequisites (see page 3401).

2. If you plan to install the CA SDM Connector and CA Catalyst Server on different computers, install the CA Catalyst Container on the same computer where you plan to install the CA SDM Connector (For more information about installing the CA Catalyst Container, see the *CA Catalyst Implementation Guide*).

   Important! If you are installing CA SOI r3.2 or lesser, ensure that you install CA Catalyst Container r3.2. If you are installing CA SOI r3.4, ensure that you install CA Catalyst Container r3.4.1.

3. Install the CA SDM Connector (see page 533).
4. Restart the CA Catalyst Server Container.
5. (Optional) Configure the CA SDM Connector (see page 535).
6. (If you are integrating with CA SOI r3.2 or lesser) Install the IFW Proxy (see page 3402).

Verify the Prerequisites

Verify the following prerequisites before installing and configuring the integration:

- Hardware and Software Requirements (see page 3401)
- Supported Versions of the Integrated Products (see page 3401)
- Integration Considerations (see page 3401)

Hardware and Software Requirements

CA Catalyst, CA SDM, and CA SOI support a number of hardware, software, operating systems, and databases. For complete information about CA Catalyst and CA SOI, see the respective documentation. For CA SDM, see the following:

- Windows Server 2008 SP1 and SP2 (x64-bit and x86-bit)
- Windows Server 2008 R2 (x64-bit)
- Windows Server 2012 R2 (64-bit only)
- Windows Server 2012 (64-bit only)

Supported Versions of the Integrated Products

The integration between CA SDM and CA SOI supports the following product versions:

- CA SDM r12.9 CUM1, r14.1.01
- CA SOI r3.1, r3.2, r3.2 CUM3, r3.3, r3.3 CUM1
- CA Catalyst Server r3.2
- CA Catalyst Container r3.2, r3.4.1
- CA EEM r8.4, r12.5, r12.5.1
- IFW Proxy r3.1, r3,2

Integration Considerations

Consider the following information before you begin the integration:

- You installed and configured a supported version of CA Catalyst. For more information, see the *CA Catalyst Installation Guide.*
- You upgraded to CA SDM 14.1.01 (see page 633). Ensure that you first apply RO80318 (Windows Master) patch and then the following patches:

Language	Patch
German	T52Y463
Japanese	T52Y464
French	T52Y465
French Canadian	T52Y466
Spanish	T52Y467
Italian	T52Y468
Brazilian Portuguese	T52Y469

- You installed and configured a supported version of CA SOI. For more information, see the *CA SOI Implementation Guide.*

  Important! If you are installing CA SOI r3.2 or lesser, ensure that you install CA Catalyst Container r3.2. If you are installing CA SOI r3.4, ensure that you install CA Catalyst Container r3.4.1.

- Verify that the CA SOI server, the CA Catalyst server (Registry, Container, and Administrator), and CA SDM server are up and running, and all these servers have network connectivity with each other.
- We recommend that you install CA Catalyst, CA SDM and CA SOI on different computers for this integration to work properly.
- You verified the CA SDM Connector Installation Considerations (see page 527).
- (Optional) Migrate Data from CA SDM Connector r2.5 (see page 529)
- (Optional) Migrate Data from CA SDM Connector r3.1 or r3.2 (see page 530)

Install the IFW Proxy

The IFW Proxy enables CA SOI to visualize and manage data provided by the CA SDM Connector. Install the IFW Proxy on each CA Catalyst Container system hosting the CA SDM Connector that you want to manage in CA SOI.

By default, the IFW Proxy is installed on the CatalystConnector container. If you want to install in a custom container you must provide the soi.ifwproxy-<build_number>.exe -Dcatalyst.container_id="<custom_container" command line argument.

Follow these steps:

1. Run IFWProxy.exe on the computer where the CA SDM Connector is installed.
   The Introduction screen appears.

2. Click Next, accept the terms of the license agreement, and click Next.
   The Integration Services Configuration screen appears.

3. Enter the following information, and click Next.

   - **SA Admin**
     Defines the administrator user name created during the CA SOI installation.

   - **Password**
     Defines the password for the administrator user.

   - **Manager host**
     Defines the host name where CA SOI is installed.

   - **ActiveMQ port**
     Defines the ActiveMQ Server port through which connector communication occurs.

   - **UCF broker port**
     Defines a valid port for the UCF Broker to send information created or updated in CA SOI to the CA Catalyst Connector.

   - **Use DNS for name resolution**
     Defines whether to use DNS for name resolution. Leave this check box selected if DNS is not configured in your environment.

   The Install Summary screen appears.

4. Click Install.
   The IFW Proxy is installed and the Install Complete screen appears. If errors occur, check the CA_IFWProxy_InstallLog.log file under the CATALYST_HOME\logs directory for details (CATALYST_HOME denotes the root CA Catalyst installation directory).

Uninstall the CA SDM and CA SOI Integration

If you do not need the integration services, uninstall the following components:

- Uninstall the IFW Proxy (see page 3403)
- Uninstall CA SDM Connector (see page 542)
- Uninstall the CA Catalyst Server (for more information about the uninstallation process, see *CA Catalyst documentation).*
- Uninstall CA SOI (for more information about the uninstallation process, see the *CA SOI documentation*).

Uninstall the IFW Proxy

Uninstalling the IFW Proxy deletes the connection between CA SOI and CA Catalyst Container running the CA SDM Connector.

Follow these steps:

1. Select Uninstall Service Operations Insight IFW Proxy from the Start menu of the computer where CA SDM Connector is installed.

2. Find the connector entry in the CA SOI Administration Web UI and click Remove Connector. The IFW Proxy is uninstalled.

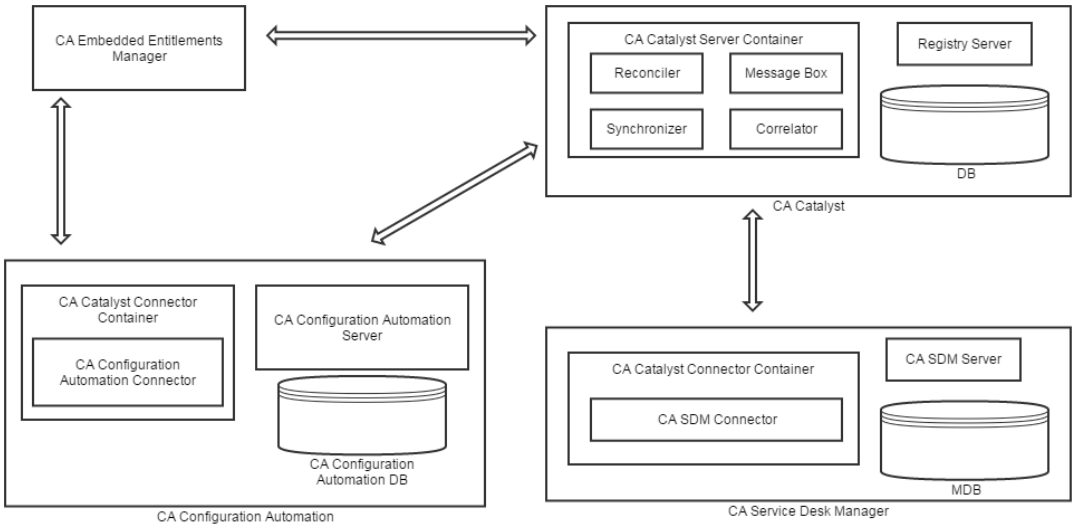
Integrating CMDB with CA Configuration Automation SP1 and SP2

This topic contains information intended for administrators who want to configure CA Catalyst to leverage key CA Configuration Automation data in the CMDB module of CA SDM. Ensure that you are familiar with the following processes:

- Performing administrative tasks in CA Catalyst, CA Configuration Automation, and CA SDM.
- Accessing product updates from CA Support Online
- Performing system administration for Windows and UNIX operating environments
- Managing CIs and CI Relationship data in GRLoader and CA SDM.

Integration Architecture

CA Catalyst integrates the CMDB module of CA SDM with CA Configuration Automation. The following diagram provides a high-level view of the integration architecture:



1. CA Configuration Automation server, database, and connector are installed on a set of servers.

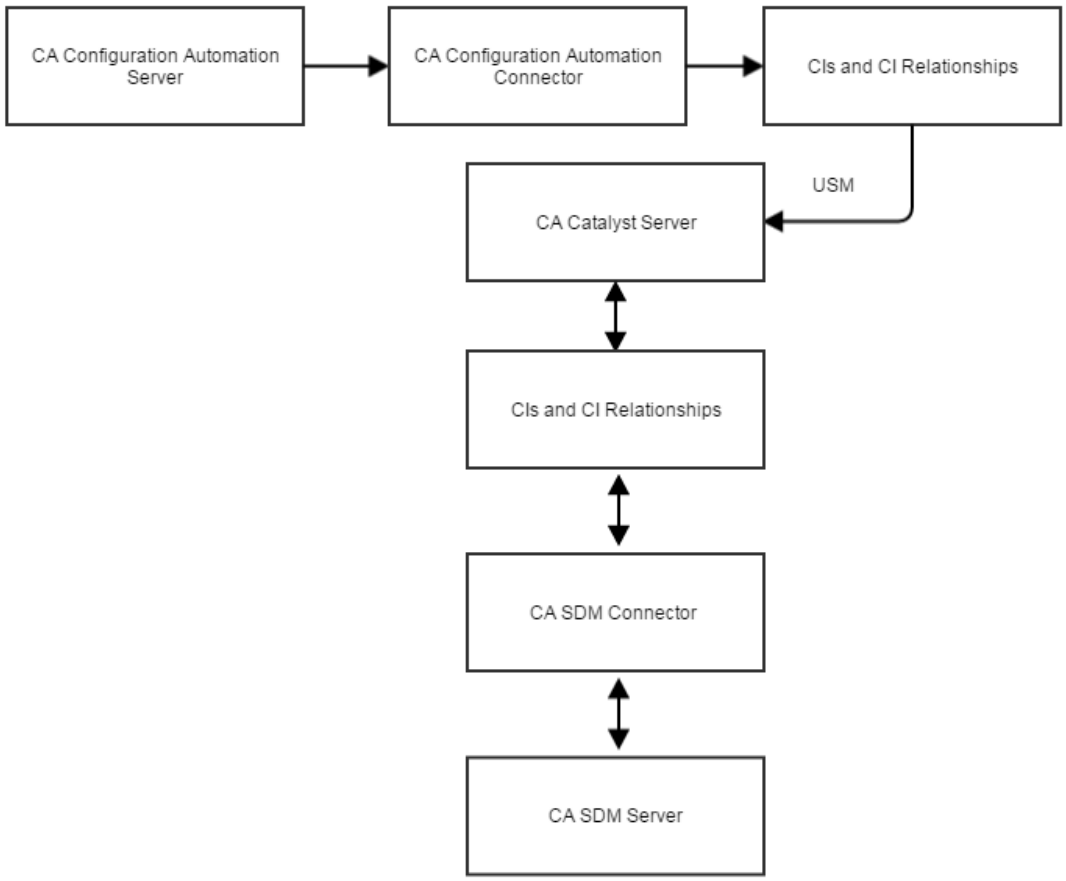
2. CA Catalyst server and database are installed on a separate set of servers.

3. CA SDM server, MDB, and connector are installed on a separate set of servers.

> **Note:** The CA SDM Connector must reside with one of the CA SDM servers.

4. CA Embedded Entitlements Manager is installed on another server.
5. CA Configuration Automation server and CA Catalyst server communicate with CA Embedded Entitlements Manager for authentication and authorization service.
6. CA Configuration Automation uses the CA Configuration Automation connector to communicate with the CA Catalyst server and push the discovered data.
7. CA SDM uses the CA SDM Connector to communicate bidirectionally with the CA Catalyst server and push and receive data.
8. Together all the components are integrated to form a solution and represent the CA Configuration Automation discovered data in the CMDB module of CA SDM.

The following information and diagram provide a summary of how the integration works:



1. The CA Configuration Automation Connector discovers CIs and CI relationship data in CA Configuration Automation.

2. The CA Configuration Automation Connector transforms the data to USM values and publishes the data to CA Catalyst.

3. The CA SDM Connector transforms the USM data into CA SDM values and publishes the CIs and CI data to the Transaction Work Area (TWA) or into CA SDM, directly.

> **Note:** When you enable the TWA flag the CI relationships are loaded to the TWA, only after the CIs are loaded from the TWA to CA SDM.

Install and Configure the Integration

This integration requires installing and configuring the CA Catalyst Server, the CA Configuration Automation Connector, and the CA SDM Connector.

Follow these steps:

1. Verify the Prerequisites (see page 3406).

2. Inactivate the MDR (see page).

3. Create an MDR Definition in CA SDM (see page 3409).

4. Install the CA Configuration Automation Connector (see page 3410).

5. If you plan to install CA SDM Connector and CA Catalyst Server on different computers, install the CA Catalyst Container on the same computer where you plan to install the CA SDM Connector (For more information about installing the CA Catalyst Container, see the *CA Catalyst documentation*).

6. Install the CA SDM Connector (see page 533).

7. (Optional) Configure the CA SDM Connector (see page 3406)
   The integration is installed and the connectors are configured.

8. Restart the CA Catalyst Container service on the CA Catalyst server.

Verify the Prerequisites

Verify the following prerequisites before starting the integration:

Hardware and Software Requirements

CA Catalyst, CA SDM, and CA Configuration Automation support a number of hardware, software, operating systems, and databases. For complete information about CA Catalyst and CA Configuration Automation, see the respective documentation. For CA SDM, see the Supportability Matrix (see page 119).

Supported Version of the Integrated Products

This integration supports the following product versions:

- CA SDM r12.9 CUM1, r14.1.01
- CA Configuration Automation r12.8 SP1, r12.8 SP2
- CA Catalyst Server r3.2
- CA EEM r12.5, r12.5.1
- CA Catalyst Container r3.2, r3.4.1

Integration Considerations

Consider the following information before you begin the integration:

- If you have previously used the CA Cohesion product, note that CA Cohesion ACM r5.0 and CA Configuration Automation are different products with different architectures. The data that these two products discover may also differ.
- If you upgraded to the supported version of CA SDMCA Configuration Automation, CA Catalyst replaces CA Business Intelligence as the integration point.
- You upgraded to CA SDM 14.1.01 (see page 633). Ensure that you first apply RO80318 (Windows Master) patch and then the following patches:

Language	Patch
German	T52Y463
Japanese	T52Y464
French	T52Y465
French Canadian	T52Y466
Spanish	T52Y467
Italian	T52Y468
Brazilian Portuguese	T52Y469

- You installed and configured the supported version of CA Configuration Automation. For more information, see the *CA Configuration Automation Implementation Guide.*
- Ensure that the services and servers discovered in CA Configuration Automation can be exported to CMDB module of CA SDM. For more information about CA Configuration Automation discovery, see the following sections in the *CA Configuration Automation Product Guide:*
  - Service Management
  - Server Management
  - Network Management

- Blueprint Management

- You applied the patch to enable the reactivation of the federated CI mapping. When a CI is deactivated in the CMDB module of CA SDM, the ID mappings also get deactivated by default. When this CI is activated again, the ID mappings remain deactivated because of the post trigger issue in CA SDM. Use the following text fixes to fix this issue:

  - RO42342 (for CA SDM r12.6)

  - RO42343 (for CA SDM r12.5)

  Note: When you apply the patch, the CA SDM service stops automatically. Start the CA SDM server after applying the patch.

- Verify that the CA Configuration Automation Server, the CA Catalyst Server (Registry, Container, and Administrator), and CA SDM server are up and running. Verify that all these servers have network connectivity with each other.

- We recommend that you install CA Catalyst, CA Configuration Automation, and CA SDM on different computers for this integration to work properly.

- You verified the CA SDM Connector Installation Considerations (see page).

- Reviewed the Frequently Asked Questions for the Integration (see page 3420).

Inactivate the MDR

If you want to import CIs and relationships from CA Configuration Automation r12.6 to the CA CMDB, you can first inactivate any MDRs defined in CA CMDB for CA Cohesion ACM r5.0, CA Application Configuration r12.0, and CA Configuration Automation r12.5. This action deactivates all the Federated CI Mappings for CA Cohesion ACM r5.0. View the Federated CI Mappings list in the Federated CI Mapping node on the Administration tab.

Important! If you want to retain both CA Cohesion ACM r5.0 and CA Configuration Automation as active MDRs, do *not* inactivate the r5.0 MDR. CIs imported from CA Configuration Automation reconcile to existing CIs imported from CA Cohesion ACM r5.0. For those CIs that are imported from both CA Configuration Automation and CA Cohesion ACM r5.0, both of these MDRs appear as MDR buttons on the CI detail page.

Follow these steps:

1. Launch CA SDM by entering the following URL in the web browser:

   ```
   http://<SDM Server Name>:<Port>/CAisd/pdmweb.exe
   ```

2. From the Administration tab, navigate to CA CMDB, MDR Management, MDR List.
   The MDR List appears.

3. Open the MDR that you want to deactivate and click Edit.
   The Update MDR Definition page appears.

4. From the Active drop-down list, select Inactive and click Save.
   The MDR is inactivated.

Create an MDR Definition in CA SDM

Create the MDR definition to specify information about the MDR contributing to the CIs. The MDR definition completes the Launch-in-Context URL configuration. You can verify the configuration from a CI detail page within CA SDM

Example: Create an MDR Definition to specify the CA Configuration Automation server information. Follow these steps:

1. Log in to the CA SDM as a user with Administrator access such as ServiceDesk.

2. On the Administration tab, click CA CMDB, MDR Management, MDR List.
   The Management Data Repository (MDR) List page appears.

3. Click Create New.
   The Create New MDR Definition page appears.

4. Complete the following required information:

   - **Button Name**: Defines the MDR button label that appears on the CI Detail page. Enter CCA.
   - **MDR Name**: Specifies the data that is sent in the mdr_name field in XML. Enter CCA.
   - **MDR Class**: Specifies the data that is sent in the mdr_class field in the XML. Enter CCA.
   - **Active**: Denotes the MDR definition as active or inactive. Inactive MDR definitions are logically deleted, but they can be made active again by using the Search utility. Select Active.
   - **Owner**: Specifies the contact responsible for this MDR. Enter ServiceDesk.
   - **Description**: Specifies the description of the MDR. Enter CCA LIC URL.
   - **Hostname**: Specifies the host name, DNS name, or IP address of the host, which contains the web server that hosts the launched web page. **Example:** CA Configuration Automation server hostname.
   - **Port**: Specifies the TCP/IP port used by the MDR web server to serve up web pages. **Example**: CA Configuration Automation Port.
   - **Path**: Specifies the portion of the URL that precedes the question mark (?) character. Enter CCAUI.jsp.
   - **Parameters**: Specifies the portion of the URL that follows the question mark (?) character. Keep the default selection.

- **CMDBf Timeout**: Specifies time limit for CMDBf endpoint query. Enter 10.
- **URL to Launch in Context**: Required for launch in context. Keep the default URL.

5. Click Save.
   The MDR definition is created.

6. Complete the following steps to modify the ServiceDeskManager_ConnectorSB.xml file:

   a. Open the Catalyst Server Registry UI using the following URL:

   ```
   https://<registryserver:port>/registry/carbon/admin/login.jsp
   ```

   b. Log in to Catalyst Registry UI and browse to the following directory:

   ```
   \topology\physical\<CA_Catalyst_Server>\ServiceDeskManager_ConnectorSB.xml
   ```

   c. Click Edit as Text.

   d. Search for the following lines:

   ```
   <Field output="temp_mdr_class" type="map" input="MdrProductLastUpdated">
   </Field>
   ```

   e. Enter the following code just before the </Field> tag:

   ```
   <mapentry mapin="CA:00033" mapout="CCA" />
   ```

   f. Search for the following lines:

   ```
   <Field output="temp_mdr_name" type="map" input="MdrProductLastUpdated,
   MdrProdInstanceLastUpdated">
   </Field>
   ```

   g. Enter the following code just before the <Field> tag:

   ```
   <mapentry mapin="CA:00033,.*" mapout="CCA" />
   ```

   h. Click Save Content.

Install the CA Configuration Automation Connector

You can install the CA Configuration Automation Connector locally on the CA Configuration Automation Server (recommended), on the CA Catalyst Server, or on a Windows system that is in the same domain as the CA Configuration Automation Server.

Note: If you install the CA Configuration Automation Connector on the same server hosting the CA Catalyst Server, then Choose Installation Folder, CA EEM, and Peer Node Configuration screens are not displayed when you run the installation program. The information in these screens is collected when you install the CA Catalyst Server.

Important! We recommend that you do *not* install the CA Configuration Automation Server on the CA Catalyst Server host because performance problems can occur. If you install CA Catalyst on the CA Configuration Automation server host, you run into port conflicts. To avoid conflicts change the default ports. Ensure that the CA Catalyst Registry Server is up and running before you start the CA Configuration Automation Connector installation.

Follow these steps:

1. Open CA Configuration Automation installer and complete the following steps:

   a. Click Run the CA Catalyst CA Configuration Automation Connector Installation Wizard.
   The installer introduction page appears.

   b. Click Next, accept the terms of the License Agreement, and click Next.
   The Choose Install Folder page opens.
   Note: This page is *not* displayed if the CA Catalyst components already reside on the system.

   c. Specify the installation folder and click Next.
   Note: The maximum installation path length is 150 characters. The installation program blocks paths with more than 150 characters.
   The Administration Configuration screen appears and displays the default CA Catalyst user in the Username field.

   d. Enter the CA Catalyst administrator user password and click Next.
   The CA Embedded Entitlements Manager Server Configuration screen appears.

2. Enter the following CA Embedded Entitlements Manager information and click Next.

   - **Server**
   Specifies the CA Embedded Entitlements Manager host server.

   - **User**
   Specifies the name of the CA Embedded Entitlements Manager administrator user.

   - **Password**
   Specifies the password for the CA Embedded Entitlements Manager administrator.

   - **Application Name**
   Identifies the CA Catalyst and CA Embedded Entitlements Manager integration using the following format: CATALYST-<*CA_Catalyst_host_name*>.

     Note: Use the same EEM Application name that you used during the CA Catalyst server installation.

   - **Default Catalyst Access for all users**
   Select READ-WRITE as the default access for all users.

   The Remote Registry Server Configuration screen appears.

Note: You can use the same CA Embedded Entitlements Manager Server for CA Catalyst and CA Configuration Automation.

3. Enter the following information and click Next.

   - **Registry Host**
     Specifies the CA Catalyst Registry host server. This repository contains the USM schema and policies that control the behavior of other components in the CA Catalyst container.
     Note: For detailed information about CA Catalyst architecture and components, see the *CA Catalyst Installation Guide*.

   - **HTTP Port**
     Specifies the server port number where you installed the CA Catalyst Registry.

   - **Secure Server Port**
     Specifies the secure server port number where you installed the CA Catalyst Registry.

   The Catalyst Container Server Configuration screen appears.

4. Enter the following information and click Next.

   - **Node Name**
     Specifies the name of the host where the CA Configuration Automation Connector is installed.

   - **Bus Port**
     Specifies the bus port number for the CA Catalyst server.

   - **HTTP Port**
     Specifies the HTTP listening port of the CA Catalyst server.

   - **HTTP Service Port**
     Specifies the SOAP-based web service HTTP network port on the CA Catalyst server. Other systems use this port to make API remote procedure calls to the CA Catalyst server.

   - **HTTPS Service Port**
     Specifies the SOAP-based web service HTTPS network port on the CA Catalyst server. Other systems use this port to make secure API remote procedure calls to the CA Catalyst server.

   The Peer Node Configuration screen appears.

5. Enter the following information and click Next.

   - **Peer Host**
     Specifies the name of the CA Catalyst server.

   - **Peer Port**
     Specifies the WS Endpoint port number of the CA Catalyst server.

- **Message Bus Host**
  Specifies the server where the CA Catalyst message bus is deployed; typically the same computer that hosts the CA Catalyst server.

- **Message Bus Port**
  Specifies the bus port number where you installed the Message Bus.

The CA Configuration Automation Connector Configuration screen appears.

6. Enter the following information and click Next.

   - **CA Configuration Automation Server Hostname**
     Specifies the name of the CA Configuration Automation server that the CA Configuration Automation Connector monitors for alarms and updates.

   - **CA Configuration Automation Server Port**
     Specifies the port the CA Configuration Automation Connector uses to communicate with the CA Configuration Automation server.

   - **CA Configuration Automation Server User**
     Specifies an administrator user who can access the CA Configuration Automation server.

   - **CA Configuration Automation Server Password**
     Specifies the password for the specified user.

   - **Verify CA Configuration Automation Server Password**
     Ensures that the password was entered correctly by matching the passwords.

   - **CA Configuration Automation Notification Listener Port**
     Specifies the port that receives events from CA Configuration Automation.

   - **HTTPS**
     Enables https on the target CA Configuration Automation Server.

   - **X.509 Certificate Authentication**
     Enables client authentication on the target CA Configuration Automation Server.

   - **Certificate Path**
     Specifies the path to the certificate for the CA Configuration Automation Server User that you configured.

   - **Certificate Password**
     Specifies the password for the certificate file.

   The Database Server screen appears.

7. Enter the following information and click Next.

   - **Database Type**
     Specifies the type of database that the CA Configuration Automation server uses.

   - **Server Name**
     Specifies the name of the CA Configuration Automation Database host.

- **Port Number**
  Specifies the listening port that the CA Configuration Automation database host uses.

- **Instance Name (Optional)**
  Specifies the name of the CA Configuration Automation Database instance.

The Database Configuration screen appears.

8. Enter the following information and click Next.

   - **Database Name**
     Specifies the name of the CA Configuration Automation Database.

   - **Database User**
     Specifies the name of the CA Configuration Automation Database administrator user.

   - **Database User Password**
     Specifies the password of the CA Configuration Automation Database administrator user.

   - **Retype Password**
     Ensures that the password is entered correctly by matching the passwords.

   The Change Detection Alert Metric and Threshold Levels page appears.

9. Enter the following information and click Next.

   - **Alert Metric**
     Specifics one of the following metrics that are used to determine the severity level of the alert when combined with the threshold values:

     - **CountChange**
       Specifies the number of changes from the source to the target server that the Change Detection operation discovers. This number of changes determines the severity level of an alert.

     - **CountSource**
       Specifies the number of changes to the source server that the Change Detection operation discovers. This number of changes determines the severity level of an alert.

     - **CountTarget**
       Specifies the total number of changes to the target server that the Change Detection operation discovers. This total number of changes determines the severity level of an alert.

     - **CountTotal**
       Specifies the total number of changes that the Change Detection operation discovers. This total number of changes determines the severity level of an alert.

   - **Information Threshold**
     Specifies the minimum number of changes for the specified Change Detection metric that is required to assign an Information severity level to an alert.

Note: The value in the threshold fields must increase with each severity level. The Information value must be the lowest, the Minor value must be next lowest, and so on, until the Fatal value, which is the highest.

- **Minor Threshold**
  Specifies the minimum number of changes for the specified Change Detection metric that is required to assign a Minor severity level to an alert.
- **Major Threshold**
  Specifies the minimum number of changes for the specified Change Detection metric that is required to assign a Major level to an alert.
- **Critical Threshold**
  Specifies the minimum number of changes for the specified Change Detection metric that is required to assign a Critical severity level to an alert.
- **Fatal Threshold**
  Specifies the minimum number of changes for the specified Change Detection metric that is required to assign a Fatal severity level to an alert.

The Installation Summary page appears.

10. Review your selections and click Install.
    The CA Configuration Automation Connector installs on the system and integrates with the appropriate CA Configuration Automation and CA Catalyst instances. The Install Complete page appears when the installation finishes.
    If the Installation Summary page displays installation errors, view the CATALYST_HOME\CA_Configuration_Automation_Connector_InstallLog.log file to troubleshoot the installation. This file is created when you click Done after the installation finishes. CATALYST_HOME specifies the folder where you installed CA Configuration Automation Connector.

How to Export CI Data

This integration lets you manage CI data in CA Catalyst, CA Configuration Automation, and CA SDM. You can export CI data from CA Configuration Automation to CA SDM.

Note: Management Profiles can also be used to export data instead of Catalyst Jobs.

Complete the following steps to create a Catalyst Job in CA Configuration Automation and execute a process to export the CI data:

1. Complete the following steps to create and execute the Catalyst Job:
   a. Log in to the CA Configuration Automation server UI from the following URL:

      ```
      http://<CA_Configuration_Automation_Server>:<port number>
      ```

Note: The default port number is 8080.

b. Click Administration.

c. On the Catalyst Integration tab, click Jobs.

d. From the Catalyst Job pane, click Table Actions, Create Catalyst Job.

e. Enter the following information:

- **Name**
  Specifies the name of the Catalyst Job.
- **Attribute Profile**
  Attaches an attribute profile with the necessary filter criteria. If you do not want to use the filter criteria, select Use Default.
- **Services/ Server Groups/ Servers**
  Specifies the Services, Server Groups, and Servers that you want to export, in that order, from the consecutive Wizard pages.
- **Blueprint Groups/ Blueprints**
  Specifies the Blueprint Groups and Blueprints that you want to export, in that order, from the consecutive Wizard pages.
- **Schedule**
  Schedules the job, if needed for synchronizing the updates on the CIs.

f. Click Finish to save the Job.

g. Select the check box next to the Job that you created.

h. Select Run Catalyst Job under Select Actions to execute the Job.

Note: For more information about creating and executing the Catalyst Job, see the CA Configuration Automation and CA Configuration Automation Connector Product documentation.

Important! Create a Catalyst profile or use the default catalyst profile before creating and executing the Catalyst Job.

2. You can view all the available CIs in [set value for the rose variable at the book level], CA Configuration Automation, and CA SDM in the CA Catalyst USM Web View. Complete the following steps:

a. Open the following URL to access CA Catalyst:

```
http://<CA_Catalyst_Server:port>/ca-rest/home
```

b. Log in to CA Catalyst and click Browse by CI Type.

c. Select the CA Catalyst (CMDB-view) data repository from the Now viewing data-source drop-down list.
The list of the available CI types appears.

d. Click a CI Type, such as Computer System.
The available CIs with the type set as Computer System appear.

e. Click a CI from the results.
The CI details appear.

Note: Similarly, you can view the CA Configuration Automation and ServiceDesk-CMDB Data Repositories.

CA Catalyst lets you view data repositories for CA Catalyst, CA Configuration Automation, and CA SDM.

3. After data exports from CA Configuration Automation to CA Catalyst, view the data that is imported to CA SDM from CA Catalyst. Complete the following steps:

a. Log in to CA SDM.

b. Complete *one* of the following actions:

Note: Use TWA as a staging area for unapproved changes and for checking duplicates.

c. Enter the search criteria and click Search to find a CI.

Note: If you click Search without entering the search criteria, the list of all CIs is displayed.

d. Open the exported CI from the CI List.
The Configuration Item Detail page appears.

Note: You can also use the CMDB Visualizer to display a visual representation of the relationship of a CI to other resources. Visualizer is available only if it was configured during the CA SDM installation.

CI details appear in CA SDM. Visualizer provides a graphical representation of the configuration item showing its relationship to other resources.

CA Catalyst User Interfaces

After you install the integration, the following CA Catalyst URLs help you configure the changes and verify the CI data:

- **CA Catalyst Registry Server UI**
  Lets you apply post-installation configuration changes. You can also verify that the connectors are installed correctly.
  URL: https://<catalyst_registry_server>:port/registry/carbon/admin/login.jsp
  Default Port: 8443

- **CA Catalyst USM Web View**
  Lets you view the CIs that are exported to CA Catalyst. Use Web View to verify that a CI exists in each of the CA Configuration Automation, ServiceDesk-CMDB, and CA Catalyst (CMDB-View) data repositories.
  URL: http://<catalyst_server>:port/ca-rest/home
  Default Port: 8080

- **CA Catalyst Admin UI**
  Lets you check the status of CA Catalyst and its connectors.
  URL: http://<catalyst_server>:port/adminui/portal
  Default Port: 8082

Uninstall the Integration

You can uninstall the CA Configuration Automation Connector when it is no longer required in your environment.

Follow these steps:

1. Click Start, All Programs, CA Catalyst, and uninstall in the following order:

   a. Uninstall CA Configuration Automation Connector.

   b. Uninstall CA Catalyst Container (You *must* uninstall the CA Catalyst Container only when the CA Configuration Automation Connector is installed standalone and not installed with any CA Catalyst component).

2. If you have installed the CA Configuration Automation Connector and CA Catalyst on different computers, complete the following steps to delete the CA Configuration Automation node in the CA Catalyst Registry UI:

   a. Enter the following URL to open the CA Catalyst Registry Server UI:

   ```
   https://<registryserver:port>/registry/carbon/admin/login.jsp
   ```

b. Select CA Configuration Automation Server Node from the \topology\physical directory.

c. Click Delete.

3. If you have installed the CA Configuration Automation Connector and CA Catalyst on the same computer, delete specific files from the CA Catalyst Registry UI after uninstalling the CA Configuration Automation Connector. Complete the following steps:

   a. Delete the CCAConnector.conf and CCAConnector.xml files from the following directory:

      `\topology\physical\<CA_Catalyst_Server>\modules\configuration\`

   b. Delete the cca_policy.xml and cca_policySB.xml files from the following directory:

      `\topology\physical\<CA_Catalyst_Server>\modules\policy\`

   c. Click the connector-modules.xml file name from the following directory:

      `\topology\physical\<CA_Catalyst_Server>\`

   d. Complete the following steps to edit the connector-modules.xml file:

      i. Click Edit as Text.

      ii. Delete the lines from the <feature name="catalyst-cca-connector"> tag to < /feature> tag in the file.

      iii. Click Save Content.

   e. Click the startup.properties file name from the following directory:

      `\topology\physical\<CA_Catalyst_Server>\`

   f. Complete the following steps to edit the startup.properties file:

      i. Click Edit as Text.

      ii. Delete the catalyst-cca-connector;3.0.0 text from the file.

      iii. Click Save Content.

4. Restart the CA Catalyst Container service on the CA Catalyst server.

5. Uninstall CA SDM Connector (see page 3418).

6. Restart the CA Catalyst Container service on the CA Catalyst server.

7. Uninstall the CA Catalyst Server. For more information, see the CA Catalyst documentation.

Frequently Asked Questions for the Integration

The following categories lists the commonly asked questions for CA Configuration Automation integration:

System Requirements

I am currently using CA Catalyst Container r2.5 to integrate CA SDM with CA Spectrum Service Assurance (CA SSA) or CA Service Operations Insight (CA SOI). Can I also integrate my CA SDM environment with CA Configuration Automation?

Use Catalyst connector 3.2 to integrate CA SDM with both CA SOI and CA Configuration Automation. For more information on the supported products, see the Supportability Matrix (see page 119).

Installation and Uninstallation

During installation of the CA Configuration Automation and SDM Connectors, I have to enter a Node Name on the Catalyst Container Server Configuration panel. What do I enter as the Node Name?

The Node Name is the host name of the computer on which you installing the connector. For example, if you are installing the SDM Connector on server A, enter Server A as the Node Name.

After installing the integration, there are three different application instances in the Embedded Entitlement Manager (EEM) for the integration (for example, CATALYST-<CACatalystServer>, CATALYST-<CCAConnectorServer>, CATALYST-<CASDMConnectorServer>). Is this correct?

No, there must only be one application instance for the integration with EEM. When installing the connector, enter the same application name that was used during the CA Catalyst installation (CATALYST-<CatalystServer>).
If, after installing your connector, you have multiple application instances for the integration in EEM, uninstall the connector. Next, you unregister the extraneous application instances from EEM using the following steps:

1. Log in to the EEM UI using the <Global> application instance, https://<EEMServer>:5250/spin/eiam
2. Select the Configure, Applications submenu.
3. From the list of applications in the left pane, click on the name of the application instance added by the CA Configuration Automation or CA SDM connector.
4. On the right-hand pane, click Unregister.
5. Repeat for any other incorrect application instances.
6. Log out of EEM.

Once the steps for EEM are executed, reinstall the connector, ensuring to use the same application instance name used during the CA Catalyst installation.

When installing the CA SDM Connector, I noticed there was an option to 'Enable TWA'. What does this option do? Why would I use it?

When the 'Enable TWA' option is selected, CIs are imported into a staging location within CA SDM called the Transaction Work Area (TWA) instead of directly into the CMDB. This allows you to vet the data (remove or modify) before the CIs are loaded into the CMDB. After reviewing the CIs, you would be responsible for transferring the CIs to the CMDB using the GRLoader import utility. This approach gives you much more control over which CIs are stored in the CMDB, but it is also a more manual and time-consuming method.

Exporting

How do I export CIs from CA Configuration Automation?

There are two ways to export CIs from CA Configuration Automation. The first way is to execute a CA Catalyst Job. To configure a job, you must log into the CCA UI and navigate to Jobs sub-menu option on Catalyst Integration tab within the Administration section. From the Catalyst Jobs table, click on Table Actions and select Create Catalyst Job. The second way is to run an integration-enabled Management Profile. To enable the integration within a Management Profile, you must create a Management Profile or edit an existing profile. On the Profile tab, in the Catalyst Integration, select the Enable Integration option and select an Attribute Profile. Save the Management Profile and run it.

What is the best method of pushing the data from CA Configuration Automation into CA Catalyst (and ultimately CA CMDB) – using Management Profiles or Catalyst Jobs?

The Catalyst jobs in CA Configuration Automation give you more control over the data entering the CMDB. When you define a Catalyst Job, you select exactly which services/servers and blueprints to export. When using Management Profiles, any service/server assigned to the integration-enabled management profile will be exported and any blueprints configured within the profile will also be exported.

When exporting CIs from CA Configuration Automation, do all chosen CIs get sent to CA Catalyst regardless of whether they were previously exported?

CA Configuration Automation maintains a check sum table in its database called acm_catlst_ci_cksum. When a CI is exported, CA Configuration Automation queries the table to see if a check sum for the CI exists. If the CI is not present in the table, a check sum of the CI's attributes is stored within the table and the CI is sent to Catalyst. If the CI is present in the table but the check sum is different, then the new checksum is entered into the table and the CI is sent to Catalyst for an update. If the CI is present and the checksum is the same, the CI is dropped and not sent to Catalyst as there were no changes to the CI.

After exporting my selected CIs from CA Configuration Automation, I see server CIs within SDM that are not listed in the Servers table within CA Configuration Automation and were not part of my Catalyst Job or Management Profile. Where did these CIs come from?

These server CIs most likely are a result of selecting to export communication or configuration relationships or both from CA Configuration Automation. The 'unknown' server CIs are typically the source/target servers discovered as part of those relationships. From the CA Configuration

Automation UI, click on a server from the Servers table to bring up the server details, select the Relationship tab and then select the Communication or Configuration sub-menu option. View the list of relationships, noting the servers listed in the source and target columns. The 'unknown' servers should be among those in the list.

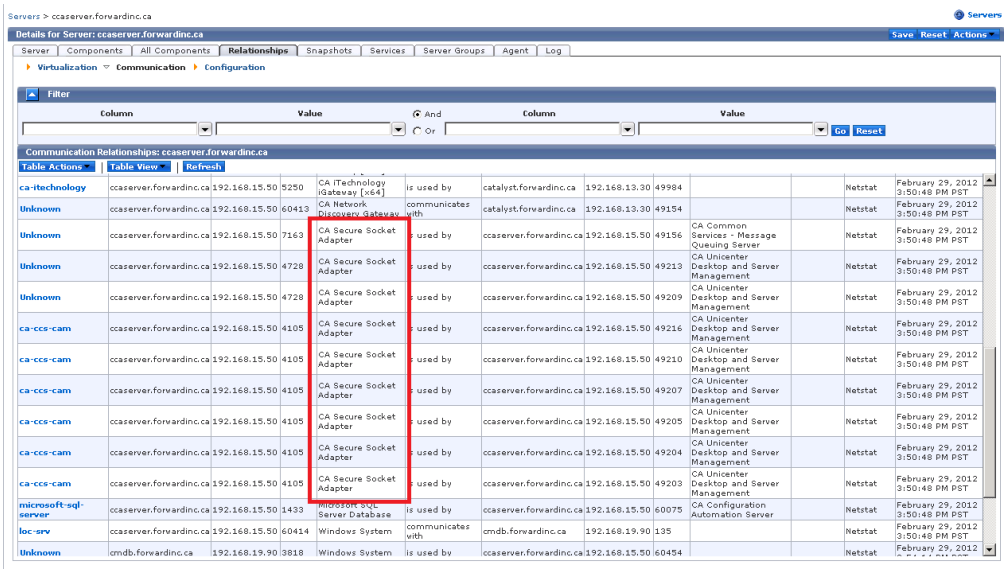
When I view my CIs within CA SDM, why do I see multiple entries for the same application?

When exporting Component CIs (for example, ProvisionedSoftware CIs) from CA Configuration Automation, the CA Configuration Automation Connector uses the Blueprint Name as the name of the CI. Although the blueprint name is not unique, the CORA attributes, specifically the system name, make the CI unique.

I ran a CA Catalyst Job or integration-enabled Management Profile in CA Configuration Automation. Then I used the CA Catalyst USM Web View to verify the CI counts in the three data repositories: CA Configuration Automation, CA Catalyst (CMDB-View) and ServiceDesk-CMDB. Why are the CI counts between the CA Configuration Automation and CA Catalyst (CMDB-View) or ServiceDesk-CMDB are different?

When CA Configuration Automation exports the CI or CI relationships, it is possible that multiple instances of the same server or same relationship exist. When the information is processed for export, the duplicate instances are reconciled and only one instance of the CI is sent to Catalyst.

For example, see the following screenshot:



This screenshot shows the communication (Netstat) relationships for the server, ccaserver. forwardinc.ca, discovered using the Softagent technology during Network Discovery. The highlighted portion shows that there are 9 instances where the CA Secure Socket Adapter application on ccaserver.forwardinc.ca is communicating with target servers.

From the CCA relationships, a BackgroundProcess CI is created in the Unified Service Model (USM) to represent the process attributes on the relationship. For the CA Secure Socket Adapter application, 9 processes would have been derived based upon what is seen in the screenshot. However, these 9 processes essentially represented the same process when each of the CCA relationships is prepared for export (the target servers are all in fact the same although communication is on different ports). Consequently, only one BackgroundProcess CI (out of the 9) is stored in Catalyst.

Also, as part of the CI processing, an 'IsHostFor' relationship is established from the ComputerSystem /VirtualSystem to the BackgroundProcess causing the relationships to be reconciled . This is the expected behavior as Catalyst helps to reconcile all duplicate CIs.

Why do the number of relationships in CA CMDB and ServiceDesk-CMDB Projection Sheet of the CA Catalyst differ?

The Unified Service Model (USM) enforces a constraint that relationships are correlated using source, target, and scope. Scope is an attribute which represents the service object the relationship affects. When CA Catalyst sends relationships to CMDB for creation, the CA SDM connector creates the CI and traverses the CMDB network of CIs to find its scope. If the scope is not found, the CA SDM connector publishes the unscoped version of the relationship to CA Catalyst. Later, if the CA SDM connector finds the scope due to some update activity on the relationship, it publishes the scoped relationship to CA Catalyst. The scoped and the unscoped relationships do not correlate which results in extra relationships in the CA Catalyst database. There is no side-effect of having both scoped and unscoped version of relationships in the CA Catalyst database. However, the relationships tend to persist in CA Catalyst until they are removed from CMDB. When the relationship is removed from CMDB, it deletes the scoped, and the unscoped relationships from CA Catalyst.

When I delete servers or components from CA Configuration Automation, are those deletions reflected in CA Catalyst and CA SDM?

Yes. The CA Configuration Automation Connector has a timer thread and, at an interval specified by the delete_thread_interval configuration parameter defined in CA Configuration Automation (default: 15 minutes). The thread identifies the CIs marked for deletion in the checksum table and publishes a delete event to CA Catalyst.

I have multi-tenancy enabled in CA Configuration Automation but not in CA SDM (or vice versa). Will this cause any problem?

Yes. Catalyst does reference the tenant of a CI when performing a reconciliation. Tenancy that is enabled within CA Configuration Automation, but not within CA SDM may create a problem with reconciliation of information within Catalyst. We recommend that if you are using multi-tenancy, enable it in both products and ensure that the names of the tenants exist in both. If you are not using tenancy in CA Configuration Automation, but have it enabled in CA SDM you should not run into a problem if the CI is tenanted to "Public". The problem will only occur if it were assigned to a specific tenant. Possible problems that you may see includes updates to the CIs within CA Configuration Automation not propagating to CA SDM, or relationships not being imported into CA SDM from CA Configuration Automation.

Integrate with CA Configuration Automation 12.8.3

Integrating CA SDM 14.1 with CA Configuration Automation 12.8.3 includes the following steps:

Step 1: Verify the Prerequisites (see page 3424)

Step 2: Create CA Configuration Automation MDR in CA SDM (see page 3425)

Step 3: Define the CA SDM Configuration Properties in CA Configuration Automation (see page 3425)

Step 4: Create CA SDM Job to Export CIs to CA CMDB (see page 3425)

Step 1: Verify the Prerequisites

Verify the following prerequisites before starting the integration:

Hardware and Software Requirements

CA SDM and CA Configuration Automation support several hardware, software, operating system, and database. For more information about CA Configuration Automation, see System Requirements (https://docops.ca.com/display/CATCA1283/System+Requirements). For CA SDM, see the Supportability Matrix (see page 119).

Supported Version of the Integrated Products

This integration supports the following product versions:

- CA Configuration Automation 12.8.3
- CA EEM r12.51 CR02

Integration Considerations

Consider the following information before you begin the integration:

- Install CA SDM (see page 269).
- Install CA Configuration Automation (https://docops.ca.com/pages/viewpage.action?pageId=272568213) .
- Ensure that the services and servers that are discovered in CA Configuration Automation can be exported to CMDB module of CA SDM. For more information about CA Configuration Automation discovery, see the following sections:
  - Service Management (https://docops.ca.com/display/CATCA1283/Service+Management)
  - Server Management (https://docops.ca.com/display/CATCA1283/Server+Management)
  - Network Management (https://docops.ca.com/display/CATCA1283/Network+Management)
  - Blueprint Management (https://docops.ca.com/display/CATCA1283/Blueprints)
- Verify that the CA Configuration Automation and CA SDM servers are up and running. Verify that all these servers have network connectivity with each other.
- We recommend that you install CA Configuration Automation, and CA SDM on different computers for this integration to work properly.

Step 2: Create CA Configuration Automation MDR in CA SDM

For the CA SDM server to identify the details of the CA Configuration Automation server, create an MDR in the CA SDM server. For more information about creating the MDR, see Create CA Configuration Automation MDR in CA SDM (https://docops.ca.com/display/CATCA1283/Export+CI+data+from+CCA+Database+to+CA+CMDB#ExportCIdatafromCCADatabasetoCACMDB-CreateaCAConfigurationAutomationMDR).

Step 3: Define the CA SDM Configuration Properties in CA Configuration Automation

Define the CA SDM configuration properties, before you export the CIs from CA Configuration Automation to CA SDM. For more information about defining the CA SDM configuration properties, see Define the CA SDM Configuration Properties in CA Configuration Automation (https://docops.ca.com/display/CATCA1283/Export+CI+data+from+CCA+Database+to+CA+CMDB#ExportCIdatafromCCADatabasetoCACMDB-SDMConfigurationProperties).

Step 4: Create CA SDM Job to Export CIs to CA CMDB

To export the CIs to the CA CMDB, create an SDM job in CA Configuration Automation. For more information about creating an SDM job, see Create CA SDM Job to Export CIs to CA CMDB (https://docops.ca.com/display/CATCA1283/Export+CI+data+from+CCA+Database+to+CA+CMDB#ExportCIdatafromCCADatabasetoCACMDB-CreateSDMJobtoExportCIstoCACMDB).

Integrating CA Service Catalog

This section contains the following articles:

Integrate CA SiteMinder with CA Service Catalog

This article contains the following topics:

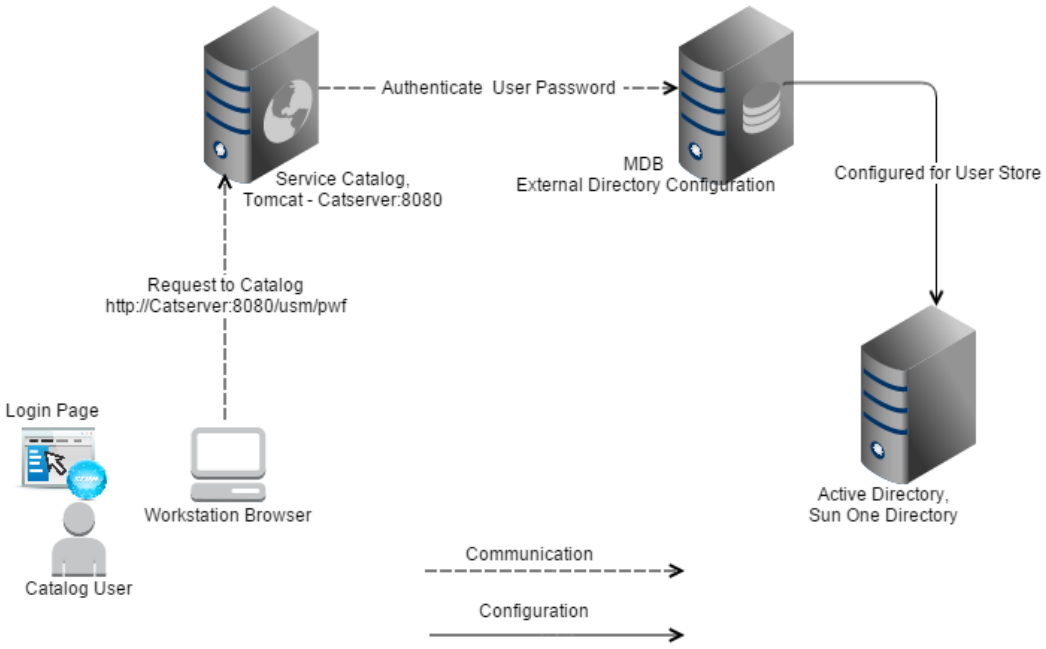
By default, CA Service Catalog uses CA EEM to authenticate the requests. You can optionally use CA SiteMinder to provide Web based single sign-on (SSO) and enhanced authentication to CA Service Catalog users.

Options to Authenticate Users

This section explains the two possible authentication flows for authenticating CA Service Catalog users. The first authentication flow uses CA EEM alone. The second authentication flow uses CA EEM with CA SiteMinder, enabling single sign-on and providing enhanced security.

Authentication Flow Using CA EEM

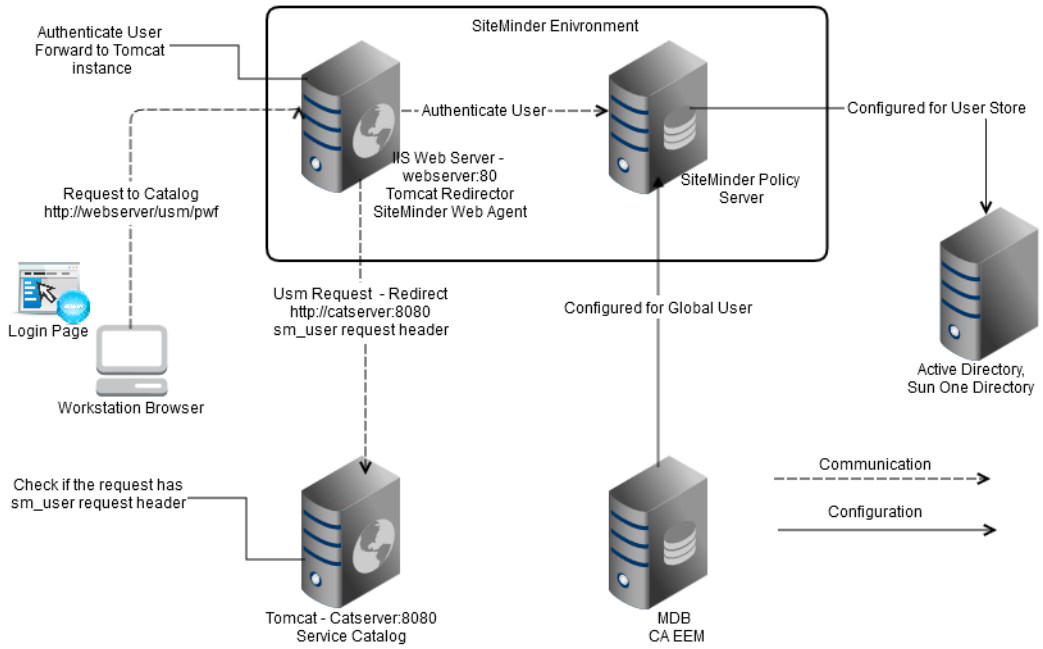
By default, CA Service Catalog uses CA EEM to authenticate users. In this example of the basic authentication flow, requests from CA Service Catalog users first pass through Tomcat. The requests then pass through the MDB, and end at your authentication server, for example, Active Directory. The following diagram illustrates the basic authentication flow with CA EEM and Active Directory:



Authentication Flow Using CA SiteMinder

In this authentication flow with CA SiteMinder, requests from CA Service Catalog users go to CA SiteMinder for authentication. If the request is authorized, then the requests are forwarded to the Tomcat instance of Catalog Component by the web server hosting CA SiteMinder. Thus, in this flow, CA SiteMinder validates the authentication requests from CA Service Catalog users. The following diagram illustrates the enhanced authentication flow with CA SiteMinder.

Note: As shown in the following diagram, CA SiteMinder requires a web server: either Microsoft Internet Information Server (IIS) or Apache Tomcat. CA SiteMinder does *not* work directly with Tomcat and relies on the request being redirected from the web server to the Tomcat instance.



Set Up Web Single Sign-on

To implement web-based (SSO) and enhanced authentication to CA Service Catalog users, complete the following tasks:

1. Install and configure CA SiteMinder, including its Policy Server and CA SiteMinder Web Agent. For more information, see your CA SiteMinder documentation.

2. Redirect the authentication requests from your web server to Tomcat. Here, your web server (such as Apache or Microsoft Internet Information Server [IIS]) has the CA SiteMinder web agent installed.
   For more information, see your web server documentation.

3. In the SiteMinder Administration GUI, configure CA SiteMinder to protect CA Service Catalog resources by performing the following tasks. For more infromation, see your CA SiteMinder documentation.

   a. Open the policy server UI.

   b. Create an agent object for CA Service Catalog; do *not* check support 4.x Agents".

   c. Create an agent configuration object for the agent you just created.

   d. Create a host configuration object.

   e. Optionally, create an authentication scheme.

   f. Create a realm and a rule with the resource filter as usm/*.

   g. Create a CA Service Catalog domain and add the user directories, administrator, and realm to the domain.

h. Create a policy and add the rule that you just created to the policy.

4. In the Administration, Configuration section of the CA Service Catalog GUI, configure the single sign-on authentication parameters to match CA SiteMinder.

Integrate CMDB with CA Service Catalog

This article contains the following topics:

CMDB Overview

A configuration management database (CMDB) is a repository of asset information defining the critical configuration items in your environment and their relationships. A service catalog fits into that framework as a tool to help with financial governance, workflow, management of service requests, and service definition. The closer the relationship between the infrastructure assets that are represented by the configuration items and the logical services that the users consume, the more useful the integration between the CMDB and the service catalog is to your organization.

CMDB is a comprehensive, integrated solution for managing the IT components and services and their relationships. You can store reliable, up-to-date details on assets, which are known as configuration items, and their relationships with each other. These relationships form the basis for impact analysis, an important tool for controlling change within an organization.

When the two are integrated, the CA Service Catalog services are associated with CMDB configuration items. Using the CMDB Visualizer, you can trace the dependencies of the services on other configuration items. You can therefore determine the impact of configuration items on services. An important application is when a configuration item used by one or more services either suffers loss of performance or stops working. You can visually pinpoint the impact of this event to the service.

When a specific change affects a configuration item, use the CMDB impact analysis tools to figure out how the change affects the services. Then you can use CA Service Catalog to determine the organizations and users that have subscribed to the impacted services. This information helps you plan the change that is required. Also, you can use the service level agreements between the subscribing organization and the providers to help plan the change. For example, if a heavily used server slows down or crashes, determine the impact on CA Service Catalog services by using the integration. You can answer the following questions:

- Which specific services use that server?
- Do those services use any other server?
- Are other servers available to replace the affected server?
- Which accounts and subscriptions are affected?

- What are the possible financial risks? For example: do the affected services or configuration items have associated service-level agreements (SLAs)? Do the impacted services help generate revenue?

Your analysis can include impact analysis, efficiency analysis, financial analysis and profitability, and ITIL considerations. Both CMDB and CA Service Catalog support ITIL principles.

Key Terms

Configuration Management Database (CMDB) is a functional data repository that unifies and simplifies the management of configuration information. CMDB consolidates and reconciles disparate sources of IT-related data in the context of business priorities. CMDB provides visibility into configuration item information such as resource attributes, relationships and dependencies.

Configuration items form the basis of configuration management solutions. Typically, a configuration item is a collection of objects that are related to the specific functionality of a larger system. Examples of these objects are requirements, code, documentation, models, and other files.

Visualizer provides a unified graphical view of relationships between configuration items and inter-dependencies of business processes. It helps you determine which CA Service Catalog services are connected to which CMDB configuration items.

Types of Association Between Services and Configuration Items

You can view, modify, and create associations between any CA Service Catalog services and any CMDB configuration items. Typically, the most suitable configuration items belong to the Business Service class in the Enterprise Services family. Several configuration items in this family and class are provided by default. You can create any new ones that you require.

The following types of association between CA Service Catalog services and CMDB configuration items are possible:

- One service to one configuration item
- One service to many configuration items
- Many services to one configuration item
- Many services to many configuration items

The many-to-many relationship between CA Service Catalog services and CMDB configuration items is the most commonly used.

You can also:

- Associate existing services to existing configuration items.
- Use an existing service to create one or more new configuration items.
- Create a service for one or more existing configuration items.

Prerequisites for CMDB - CA Service Catalog Integration

- Be familiar with basic functions and administration of CMDB, such as families, classes, configuration items, and relationships between configuration items. Understand how to use the analysis tools, such as root cause analysis and impact analysis.
- You must be familiar with basic functions and administration of CA Service Catalog.
- Ensure that both CA Service Catalog and CMDB are installed, configured, and running.
- If you are using Service Accounting Component, ensure that it is installed, configured, and running.
- Use the same MDB installation for CMDB and CA Service Catalog.

After you have installed and configured CA Service Catalog and CMDB, integrate them by performing the setup tasks first.

Step 1 - Perform Common Setup Tasks

This article contains the following topics:

The CMDB and CA Service Catalog administrators can work together to perform the following common setup tasks:

Step 1a - Verify Access Rights

CA Service Catalog administrators must ensure that CMDB administrators, analysts, and other users have the required access rights in CA Service Catalog to components (such as requests, subscriptions, business units, or accounts) that are associated to configuration items.

Assign CA Service Catalog administrator roles to these CMDB users. By doing so, you ensure that they have required access rights.

CMDB administrators must ensure that CA Service Catalog administrators have the required access rights to CMDB configuration items that are associated to CA Service Catalog components.

Step 1b - Configure for Single Sign-on

Bypass user login by configuring CA Service Catalog and the CA products with which it integrates to use single sign-on.

To configure CMDB and CMDB Visualizer to use single sign-on, configure them to use either CA SiteMinder or Windows NTLM authentication.

To configure CA Service Catalog to use single sign-on, configure it to use either CA SiteMinder or Windows NTLM Authentication. For more information about how to configure, see in Integrating with CA SiteMinder (see page 3425). You can also use Windows NTLM authentication, as explained in Enable External Authentication of Users (see page 1429) section.

Step 2 - Perform Setup Tasks for CMDB

As a CMDB administrator, on the CMDB computer, log on to CMDB. Access the CMDB Administration tab, and perform the following tasks.

1. Using the Web Services Policy option, create the Web Services Access policy.

    a. Assign a name. The suggested name and code are USM_CMDB_Policy, but you can use any name that meets your needs.

    b. Assign a proxy user to this policy.

    > **Important!** This proxy user *must* have administrative access to CMDB.

    c. Verify that the Allow Impersonate property of CMDB is set to Yes.

    CMDB checks the access type of the CA Service Catalog user to be impersonated against the access type of the policy proxy user. If the access level of the CA Service Catalog user is less than or equal to the grant level of the proxy user's access type, CMDB replaces the CA Service Catalog user with the proxy user. For more information, see your CMDB documentation.

2. Generate the policy key file for the Web Services Access policy that you created. To generate the key file, use the pdm_pki tool.
   The suggested name is USM_CMDB_Policy.p12, but you can use any name that meets your needs.
   Verify that the HasKey property is set to Yes in the newly created Web Services access policy. The system typically configures this setting automatically when you generate the policy key file.
   Copy the policy key file to the CA Service Catalog server and save it in the USM_HOME directory.

   > **Important!** If you are using application clustering, copy the policy key file to the USM_HOME directory of *every* Catalog Component cluster node.

3. Verify that the Business Service class of the Enterprise Service family exists. This class is required for CA Service Catalog users to create a configuration item in CMDB. If this class does not exist, create it manually or run the CMDB installation again to load default data.

Step 3 - Perform Setup Tasks for CA Service Catalog

This article contains the following topics:

As a CA Service Catalog administrator, on the CA Service Catalog computer, log in to CA Service Catalog.

Update the Configuration Settings

Specify the configuration settings for CA CMDB.

Follow these steps:

1. Click Configuration, CMDB, on the Administration tab of CA Service Catalog.

2. Complete the Configuration settings, as follows:

   - **Enable HTTPS**
     Specifies the option (Yes or No) that matches your implementation.

   - **Host Name**
     Specifies the host name of CMDB computer.

     Note: This recommendation applies after you have configured the integration and have started to use it: Do *not* change the host name of the CMDB computer or the CA Service Catalog computer, *unless* the two host computers share MDB.

   - **Port Number**
     Specifies the port number on the CMDB computer that listens for incoming calls from CA Service Catalog.

   - **Key File Name**
     Specifies the name of the Web Services policy key file that you created earlier.
     The default value is USM_CMDB_Policy.p12.

   - **Policy Code**
     Specifies the name of the Web Services policy code that you created earlier.
     The default value is USM_CMDB_Policy.

   - **Default New CI State Inactive**
     Specifies whether new configuration items that you create through this integration have a default state of *inactive* or *active*.
     Specify Yes for inactive or No for active.

3. Verify the CMDB Configuration by clicking Test Connection.
   If the test fails, perform the following actions:

   a. Verify that your settings are completed correctly, especially the host name and port number of the CMDB computer.

   b. Verify that the CMDB service is up and running.

Update the Visualizer Settings

Specify the configuration settings for the CMDB Visualizer.

Follow these steps:

1. Click Configuration, CMDB Visualizer on the Administration tab.
2. Specify the following Visualizer Configuration settings:
   - **Enable HTTPS**
     Select the option (Yes or No) that matches your implementation.
   - **Host Name**
     Specifies the host name of the CMDB Visualizer computer, typically the CMDB computer.
   - **Port Number**
     Specifies the port number of the CMDB Visualizer.
3. Verify the CMDB Visualizer by clicking Test Connection.
   If the test fails, perform the following actions:
   a. Verify that your settings are completed correctly, especially the host name and port number of the CMDB Visualizer computer.
   b. Verify that the CMDB Visualizer service is up and running.

Step 4 - Set Up the CMDB - CA Service Catalog Integration

This article contains the following topics:

Follow these steps to enable the integration between CMDB and CA Service Catalog:

1. Ensure that CA Service Catalog, Service Accounting Component (if used), and CMDB are installed, configured, and running.
2. Ensure that you verify the MDB version compatibility for all CA products that you plan to integrate, including CMDB.
   - Review the level of maturity of each product in your environment.
   - Review standard process and procedures in your organization, especially external standards that you must follow. Examples of standards are ITIL, ISO, COBIT, and CORA. ITIL is especially applicable because both CMDB and CA Service Catalog support ITIL concepts.

- In CMDB, review the configuration items in the Business Service class of the Enterprise Services family. These configuration items are considered to be the most likely candidates for integration with CA Service Catalog services. Remember, however, that you can associate *any* configuration item or items with one or more CA Service Catalog services.
- In CA Service Catalog, review the existing services.
- In both, review the existing associations if any.

3. Review the key terms (see page 3429) for the integration.
4. Review the types of association between services and configuration items (see page 3429) that you can create.
5. Review the associations that already exist, if any; for more information, see View Associations Between Services and Configuration Items (see page 3438).
6. Determine any *new* Catalog-CMDB associations that make sense for your business. Ask these questions:
   - Which existing configuration items must be associated with one or more services? Do those services already exist, or do you have to create new ones?
   - Which existing services must be associated with one or more configuration items? Do those configuration items already exist, or do have to create new ones?
   - Do you want to populate the CMDB service by service?
   - Have you started or finished populating the CMDB, using the guidelines for doing so in the CMDB documentation? Or do you want to start by seeding CA CMDB with a few mission critical applications and business services?
   - Have you checked the business continuity plan of your organization? Review this plan and determine which business services and respective components in your infrastructure are critical.
     As you answer the questions, consider the following factors:
   - Keep in mind that the goal of all associations is to use IT to support your business needs.
   - If applicable, begin thinking about associations starting from the perspective of the product that is most mature in your environment. For example, if you have an established CMDB implementation but a newer CA Service Catalog implementation, then CMDB is the more mature product. Start by viewing your existing configuration items in the Business Service class of the Enterprise Services family. Determine which ones could use CA Service Catalog services, to serve your business needs. In this model, it is likely that you first create the needed services and next create the associations.
     Conversely, if you have mature services but your CMDB implementation is just starting, create configuration items corresponding to the services. For example, for critical services connected to service level agreements, create configuration items that are based on the hardware or other infrastructure that is required to support the CA Service Catalog services.

For example, define your email application and server as configuration items and associate them to an email service in CA Service Catalog. Similarly, you can also associate that email application and server with a service for requesting Blackberry units and subscriptions.

- If you are using Service Accounting Component, consider creating and associating configuration items with the services related to your most important subscriptions and most important financial reporting items.

7. Create any configuration items that you need for the integration.

8. Create any services that you need for the integration.

   Note: When a service is copied or inherited, its associations to CIs are *not* copied.

9. Consider service level agreements (SLAs).
   Whenever the availability of services is affected, the SLA can have a significant effect on impact analysis. For example, if a server used by a service that your company provides is down, the ability to meet the SLA obligations to your customers is affected. Therefore, you want to set up your service-to-configuration item associations to include services and computers that are involved in meeting SLA obligations.

10. Associate the services to configuration items. These associations are *from* CA Service Catalog *to* CMDB. You associate a CA Service Catalog service ID with a CMDB UUID (not a logical ID). For example, consider the New Hire Onboarding service, which is one of many services that are supplied with CA Service Catalog. This service can be used for requesting office equipment that is required by a newly hired employee. Create a configuration item for each of these assets and associate them to the service. In this case, the association is many to one (many configuration items to one service).

11. Using the CMDB Visualizer, leverage the analysis tools of CMDB, such as impact analysis and root cause analysis. For more information, see How to Leverage Information from Analysis Tools (see page 3440).

Create a Configuration Item for a Service and Associate Them

Many of the associations that you create involve CA Service Catalog services and existing CMDB configuration items. You can *create* a configuration item specifically for a service, if no suitable configuration item exists already. You do not have to create and associate a configuration item for every service. Instead, create and associate such configuration items *only* when they support your business needs and goals.

Before associating a service to a configuration item, ensure that the service is *defined* in CA Service Catalog. The service option groups and service options for that service have been specified. For more information about defining services, see the Manage Services (see page 2987) section.

> **Note:** If you associate a CA Service Catalog service with a CMDB configuration item that does *not* display the Attributes tab, you *cannot* view the service-related details of the configuration item from CA Service Catalog. For more information, see the CMDB documentation.

For more information to associate services with *existing* configuration items, see Associate Services with Configuration Items (see page 3436).

Follow these steps:

1. From the CA Service Catalog home page, select Catalog, CMDB CI Association.
2. Under the line "The current business unit is: *business-unit-name*," click the Catalog tab.
   The list of existing folders, sub folders, and services appears.
3. Expand the folders and sub folders as needed, until the services you want appear.
4. Check the box next to the service or services for which you want to create and associate a configuration item.
5. Click the right arrow next to the Selected Services box.
6. Click Next.
   The screen refreshes, and the CI List for Association appears. The names of any configuration items that are already associated with the selected service appears.
7. View the list of existing associations under the CI Name heading.
8. Click Create CI to *create* a configuration item for each selected service.
   For each selected service, a new configuration item is created in the Business Service class of the Enterprise Services family. Also, a one-to-one association is created between each service and its new, same-named configuration item. By default, the system also displays the names of several CMDB configuration item attributes. While the *names* of these attributes are listed by default, the *values* of these attributes are not populated by default. You can optionally populate these values. In addition, you can add and populate other attributes of your choosing. For more information, consult your implementation team, including your CMDB administrator and CA Service Catalog administrator.
9. Click Save to associate the new configuration item and all selected service.

Associate Services with Configuration Items

Create only the associations that support your business goals and needs.

Before associating a service to a configuration item, ensure that the service is *defined* in CA Service Catalog. The service option groups and service options for that service have been specified.

Note: If you associate a CA Service Catalog service with a CMDB configuration item that does *not* display the Attributes tab, you *cannot* view the service-related details of the configuration item from CA Service Catalog.

Follow these steps:

1. From the CA Service Catalog home page, select Catalog, CMDB CI Association.
2. Under the line "The current business unit is: *business-unit-name*," click the Catalog tab.

   Note: If you know the name of the service or folder that you want, you can optionally use the Search tab to display services.

3. Expand the folders and sub folders as needed, until the services you want appear.
4. Check the box next to the service or services that you want to associate with one or more configuration items.
5. Click the right arrow next to the Selected Services box.
   This action selects the services. The names of the selected services appear in the Selected Services box.
6. Click Next.
   The screen refreshes, and the CI List for Association appears, displaying the names of the service that you selected. The services are listed in the service column. If any service is already associated to one or more configuration items, the item is listed next to the service in the CI Name column.

   You can associate each of these services (either individually or as a group) to one or more configuration items.
7. Check the service or services that you want to associate to one or more configuration items in the same action. Leave any other services unchecked; you can optionally associate such services to configuration items in a separate action.

Note: To *create* a configuration item for each selected service and associate them, click Create CI, as explained in Create a Configuration Item for a Service and Associate Them (see page 3435). If you click Create CI, new configuration item is created for each selected service. Also, a one-to-one association is created between each service and its new, same-named configuration item.

To associate a single service with one or more existing configuration items, perform the following actions:

1. Check the service and click Associate CIs.

2. Click Search or use a search string to display the available configuration items.

3. Verify that all configuration items that you want to associate with the service that you checked, and click OK.
   If you selected only one configuration item, a one-to-one association is created between the checked service and that item.
   If you selected two or more configuration items, a one-to-many association is created between the checked service and those items.

To associate two or more services with one or more existing configuration items, perform the following actions:

1. Check the services and click Associate CIs.

2. Click Search or use a search string to display the available configuration items.

3. Verify that all configuration items that you want to associate with the services that you checked, and click OK.
   If you selected only one configuration item, a many-to-one association is created between the checked services and that item.
   If you selected two or more configuration items, a many-to-many association is created between the checked services and those items.

4. Click Save after associating the items.

Your associations are saved. The associations are used for impact analysis, root cause analysis, and other analysis functions for your integration between CMDB and CA Service Catalog.

View Associations Between Services and Configuration Items

You can quickly view existing associations from CA Service Catalog services to CMDB configuration items. It is helpful to see such quick views for many reasons, including saving time, avoiding duplicate associations, and gaining quick access to the CMDB Visualizer for the service and any associated configuration items.

Note: If your implementation requires you to log in to CMDB Visualizer, see your administrator to obtain a user name and password for accessing CMDB Visualizer.

Follow these steps:

1. Click Catalog, Service Offerings.

2. Search the folders and services, expanding them if necessary, until you locate the service you want.

3. Under the Actions icons, click the CMDB Association icon. Its tooltip text is "CMDB CI Associations."
   The Service Offerings dialog appears, showing the configuration items that are currently associated with the service.

4. Optionally, perform one of the following actions:

   a. Click the Visualizer icon to view the relationship of those configuration items currently associated with the service. Its tooltip text is "CMDB Visualizer."
      Log in to CMDB Visualizer and use the Visualizer features to find the most critical relationships; you use this information for impact analysis, root cause analysis, and other analysis.

   b. Delete the association by selecting the configuration item or items and clicking Remove Association.

View the Service-Related Details of a Configuration Item

The service-related details of a CMDB configuration item are the CA Service Catalog service or services associated with the item, the number of requests for each associated service, and any other related properties that your organization deems important. This information can be a critical part of your analysis activities for the associated services and configurations items. For example, a high number of associated requests, subscriptions, or accounts may indicate that a configuration item is very critical for business continuance and therefore merits special attention.

If your implementation requires you to log in to CMDB Visualizer, see your administrator to obtain a user name and password for accessing CMDB Visualizer.

Note: If you associate a CA Service Catalog service with a CMDB configuration item that does *not* display the Attributes tab, you *cannot* view the service-related details of the configuration item from CA Service Catalog.

Follow these steps:

To begin in CA Service Catalog, perform the following actions.

1. Click Catalog, Service Offerings.

2. Search the folders and services, expanding them if necessary, until you locate the service you want.

3. Under the Actions icons, click the CMDB Association icon. The tooltip text for this icon is "CMDB CI Associations."
   The Service Offerings dialog appears, showing the configuration item or items that are associated with the service.

4. Click Visualizer.

5. (Optional) Log in to CA CMDB Visualizer.
   The associated items appear in CMDB Visualizer. If these items have relationships with other configuration items, the related items and the relationships also appear.

To begin in CMDB Visualizer, perform the following actions:

1. Log in to CMDB Visualizer.

2. Display the configuration items that are associated with the service of interest.
   If these items have relationships with other configuration items, the related items and the relationships also appear.

3. Right-click the configuration item and select View Properties.

4. Click the Attributes tab and click the Service Catalog button, which is the managed data repositories (MDR) button for CA Service Catalog.

   The CA Service Catalog GUI opens.

   Note: Optionally right-click the configuration item and select View, MDR. From the list of MDRs, select Service Catalog.

5. If the CA Service Catalog GUI does not open, perform the following actions:

6. a. Verify that the CA Service Catalog host name property specified in the MDR button is correct.

   b. Verify that the CA Service Catalog services are started.

7. If necessary, log in to CA Service Catalog.
   The CI Associated Offering Details dialog appears.

8. View the count for the requests, subscriptions, accounts, and business units that are related to the configuration item and its associated service or services.
   If multiple services are associated to the configuration items whose properties are viewing, the counts for all associated services are listed.
   For requests, accounts, subscriptions, and business units, optionally click the links for further details about each count:

Use this information along with any information you obtain from the CMDB Visualizer analysis tools. These tools are summarized in Leverage Information from Analysis Tools (see page 3440).

Leverage Information from Analysis

After you have established the relationships between configuration items, you can use the CMDB Visualizer for the following tasks:

- Provide a 360-degree view of the relationships between business-critical configuration items within your organization.

- Perform root cause analysis for Incidents and Problems.
- Perform impact analysis on changes to configuration items.
- Create filters in the CMDB Visualizer to customize your views of configuration items.

Performing these tasks helps you detect and strengthen the connections between IT and business: specifically, between your IT components (configuration items) and business services. Each analysis also helps you understand the connections between configuration items and helps you maximize their value.

A service can both *be* a configuration item and can also involve *changing* the IT infrastructure. While the distinction sometimes seems obvious, distinguishing between these two types of services explicitly can be helpful.

Consider a managed application service example: A department requests that the IT department supply and maintain a server, install an application, and administer the application. The interaction with the CMDB is through a workflow. The workflow includes change orders for configuration items. The workflow also sets up relationships between the server, application, application service, and other configuration items.

Integrate CA Business Service Insight with CA Service Catalog

This article contains the following topics:

CA Business Service Insight automates, activates, and accelerates the management, monitoring, and reporting of business and technology *service level agreements* (*SLAs*) and service delivery agreements for enterprises and service providers. CA Business Service Insight enables organizations to understand the performance and cost implications of these agreements in real time. Enterprises and service providers can leverage one solution to manage service delivery across the business and technology infrastructure, efficiently.

The top-down methodology for service level management begins with contracts that use business language and metrics. These contracts integrate with technical data sources for continuous measurement of service performance in relation to contract terms and conditions. The resulting transparency and control enable you to manage more efficiently both the expectations between IT and the business and your contracts with external service providers, such as CA Service Catalog.

Benefits of the Integration

The *integration* of the two products provides the following benefits:

- As a CA Service Catalog administrator, when defining a service option, you can browse the list of contracts in CA Business Service Insight. You can select a contract, and can associate it with the service option. You can also select a service component, contractual metrics, and incentive metrics from that contract to associate it with the service option. Together, they specify the quality of service that is expected for the service option. The service component specifies *what* is being monitored. The "what" can be a component that is related to the service option. And the metrics specify *which data* is being monitored. The "which" can be kilobytes per second or violations per month.

- Using the integration, you measure adherence to CA Business Service Insight contracts according to the service as a whole.

- This association of a service option with a contract and the monitoring that both products provide, supports the transparency of service quality. The association also provides financial adjustments as specified by the contract. For example, the adjustments can include reduced charges when the service does not meet the terms of the contract.

- You can use either CA Business Service Insight or CA Service Catalog to view the level of compliance of a CA Service Catalog service to the terms of its associated CA Business Service Insight contracts.

- You can use the billing features of Service Accounting Component to determine any financial adjustments that a service requires.

Comparison to Request SLA

CA Service Catalog enables administrators to create request SLAs to monitor whether service options in a request are processed within the time period that you specify for each monitored state. Your request SLAs specify time to warning and time to violation for a selected service option. A single request SLA specifies the amount of time that is permitted between specified statuses. For example, the time that is taken to move from Submitted to Approved or from Approved to Completed.

Request SLAs is a feature of CA Service Catalog. Quality of Service SLAs is available only if CA Service Catalog is integrated with CA Business Service Insight. You define QoS SLAs in CA Business Service Insight.

Request SLAs remain in CA Service Catalog as a time metric during the request life cycle of an *individual* request. In contrast, QoS SLAs in CA Business Service Insight measure averages and other values for *all* requests of a specific service during a certain time period. Examples follow:

- The average approval time for Desktop procurement service must not exceed 15 calendar days during a single one-month period.

- The maximum fulfillment time for the Desktop procurement service must not exceed 20 calendar days during a single one-month period.

CA Business Service Insight also uses QoS SLAs to provide several more metrics of various types, either during the request life cycle or after it has ended and while the requested service is being delivered. For example, a QoS SLA stipulates that the service must be available an average of 99% of the time every day. Another QoS SLA requires that the maximum time that a service can be unavailable on any one day is 15 minutes.

Request SLAs in CA Service Catalog cover *business* days while QoS SLAs in CA Business Service Insight cover *calendar* days.

Metrics in Contracts and Services

Administrators in CA Business Service Insight can obtain request processing data from CA Service Catalog to evaluate whether service options in services met, exceeded, or failed to meet the metrics that are defined in the contract for the service. For example, a contract defines metrics for a laptop service to meet the following goals:

- A service must be available for users 99% of each one-week period to meet a Gold metric, 95% for a Silver metric, and 90% for a Bronze metric.
- Fulfill each request for a laptop computer in 15 or fewer calendar days. If a request for laptop service is not fulfilled in 15 or fewer business days, credit the requestor's (or business unit's) account with an adjustment of 5% of the laptop cost.
- Fulfill all requests for a laptop computer in an average time of 10 or fewer calendar days. If the average fulfillment time of the laptop requests is more than business 10 days, credit the requestor's (or business unit's) account with a fixed adjustment of $1000.
  The fulfillment time starts when the request is approved and ends when the fulfillment process is completed.

Such metrics that define the maximum time period for requests to move from one status to another -- either individually or on average -- are named request SLAs (see page 3442).

Finally, administrators can optionally report on this data and publish it in dashviews in dashboards (see page 3461).

Prerequisites for CA Business Service Insight - CA Service Catalog Integration

This task is required to establish the communication between the two products.

Important! Verify that Microsoft Internet Explorer is installed on the computers from which you plan to access CA Business Service Insight. Even when you access CA Business Service Insight indirectly through CA Service Catalog, use Internet Explorer.

1. Verify that both CA Service Catalog and CA Business Service Insight are installed and running.
   For more information, see the respective documentation.
   As part of this task, verify that both products support the browser you are using.
2. Verify that you have administrator rights in both products, specifically:
   - The Service provider role (SP administrator) in CA Service Catalog.
   - The Super administrator role in CA Business Service Insight
3. Enable the CA Business Service Insight openAPI. By doing so, you ensure that CA Service Catalog can access the CA Business Service Insight secured web services.
   For more information, see your CA Business Service Insight documentation.

Note: If you require SSL support for this API, if necessary, see the Windows Communication Foundation (WCF) documentation on the Microsoft MSDN web site, msdn.microsoft.com. For further assistance enabling SSL support for the CA Business Service Insight openAPI, if necessary, contact CA Business Service Insight CA Support at http://ca.com/support (http://www.ca.com/support).

4. Verify that you have a copy of the digital certificate that contains the CA Business Service Insight public key for the server certificate that is used to enable the openAPI.

5. Import the CA Business Service Insight public key certificate into a Java keystore file, in CA Service Catalog:

```
keytool -import -file  publickey.cer -keystore  oblicorekeyfile -alias
oblicoreauthcert
```

   a.
   - **publickey.cer**
     Specifies the client certificate file for communicating with CA Business Service Insight using the open API.
   - **oblicorekeyfile**
     Specifies the name of the Java keystore file that this command generates. CA Service Catalog uses this file to access CA Business Service Insight.
   - **oblicoreauthcert**
     Specifies the alias name for the publickey.cer file.

   Enter the password that you want to use for this keystore file.

Set Up the CA Business Service Insight - CA Service Catalog Integration

This article contains the following topics:

Administrators of CA Service Catalog and CA Business Service Insight set up the integration between the products as follows.

1. Verify that CA Business Service Insight includes contracts, service domains, and metrics useful for measuring the quality of the CA Service Catalog services with which you plan to use them. For example, you want to monitor quality for services that include internet connectivity. In that case, you want to verify that the metrics include related quality measures, such as maximum wait time to establish connections, refesh screens, change addresses.
   Consider the following:

   - In CA Business Service Insight, consider naming such contracts with a special prefix, such as "Catalog_" for easy reference.

   - If your implementation of CA Service Catalog, uses multi-tenancy, then consider mapping the contract parties in CA Business Service Insight to your CA Service Catalog business units.
     Alternatively, consider naming your CA Business Service Insight contracts with a special prefix, such as "Service_Provider_name_" or "Tenant_name" for easy reference.

2. Create reports to access metric-related SLA data (see page 3445).

3. Verify that all CA Service Catalog and CA Business Service Insight computers are set to the same exact date and time and are adjusted, if necessary, for the time zone that you have chosen. This requirement includes the DBMS server for both integrating products.
   For example, suppose that you decide to use the Eastern USA time zone. In that case, if the current time is November 11, 6:27 p.m. Eastern USA, then set all computers to November 11, 6:27 p.m. Eastern USA or its equivalent, regardless of the physical or geographic location of the computer.

4. In CA Service Catalog, set the administration configuration parameters (see page 3448) for connecting to CA Business Service Insight.

5. In CA Service Catalog, set the request management configuration parameters (see page 3449).

6. In CA Service Catalog, for each applicable service option group, add the service option element for the CA Business Service Insight contract (see page 3454) you want to associate. When you do so, you specify important details such as the contract name, the service component, metrics.

7. Understand how the integration works after the request life cycle is completed (see page 3458).

8. In CA Business Service Insight, import the adapter package (see page 3450).

9. In CA Business Service Insight, create the adapter (see page 3452).

10. Test the Adapter (see page 3453).

Step 1 - Create Reports to Access Metric-Related SLA Data

This task is required to meet the prerequisites for setting up the integration. In CA Business Service Insight, create specific parameterized reports to access metric-related SLA data from CA Service Catalog. CA Service Catalog requires these reports to obtain service level data from CA Business Service Insight. To create the reports, run the SQL queries in this procedure on the Oracle database of CA Business Service Insight.

Follow these steps:

1. Open the Oracle database for CA Business Service Insight.

2. To create the Service Level by Metric report, run the following SQL query:

```
insert into t_report_galleries (report_id, report_name, report_type,
report_description, report_xml, is_executable, schedule_id, report_owner,
report_hirarchy, is_grouped, report_gallery_create_date,
report_gallery_modify_date, is_inherit_parent_permissions, folder_id,
is_ready_type, is_parameterized, e2e_type, inherit_permissions)values(90000001,
'Service Level by Metric parameterized report', 'NORMAL', 'This report is
parameterized report which return service level data by metric. This report is
used by CA Service Catalog. Please do not modify this report.','<REPORT_GROUP
TYPE="NORMAL" MARGIN="Y"><REPORT_ITEM><REPORT LOCALE="0" ORDER="ASC" ORDER_BY="
VALUE" TOP="0"><Y ID="PROVIDED" AGG="AVG" WITH_CORRECTION="1" SHOW_CORRECTION="
1" WITH_EXCEPTION="1" WITH_ADJUST="1" WITH_INCOMPLETE="1" INCLUDE_TARGET="1"
INCLUDE_FORECAST="0" WITH_THRESHOLDS="0" BUSINESS_DATA="1"/><X ID="RULE"
/><FILTER IS_PARAMETERIZED="Y"><TIME FORMAT="DD/MM/YYYY" TYPE="span"
IS_PARAMETERIZED="Y" IS_MANDATORY="Y"><SPAN LAST="0"><UNIT>QUARTER</UNIT><
/SPAN></TIME></FILTER><STEPS NUM="0"/><DISPLAY_PROPERTIES><GRID_COLOR>0<
/GRID_COLOR></DISPLAY_PROPERTIES><FILTER_DEFAULTS><CONTRACT IS_PARAMETERIZED="
Y" IS_MANDATORY="N">-1</CONTRACT></FILTER_DEFAULTS></REPORT><
/REPORT_ITEM><pdf><!--<option><name>parameter name</name><value>parameter value<
/value></option>--></pdf></REPORT_GROUP>', 1, null, 100, 1, null, sysdate,
sysdate, 0, 500, 0, 1, 0, 0)
```

3. To create the Deviation by Metric report, run the following SQL query:

```
insert into t_report_galleries (report_id, report_name, report_type,
report_description, report_xml, is_executable, schedule_id, report_owner,
report_hirarchy, is_grouped, report_gallery_create_date,
report_gallery_modify_date, is_inherit_parent_permissions, folder_id,
is_ready_type, is_parameterized, e2e_type, inherit_permissions)values(90000002,
'Deviation by Metric parameterized report', 'NORMAL', 'This report is
parameterized report which return Deviation data by metric. This report is used
by CA Service Catalog. Please do not modify this report.','<REPORT_GROUP TYPE="
NORMAL" MARGIN="Y"><REPORT_ITEM><REPORT LOCALE="0" ORDER="ASC" ORDER_BY="VALUE"
TOP="0"><Y ID="DEVIATION" AGG="COUNT" WITH_CORRECTION="1" SHOW_CORRECTION="1"
WITH_EXCEPTION="1" WITH_ADJUST="1" WITH_INCOMPLETE="1" INCLUDE_TARGET="0"
INCLUDE_FORECAST="0" WITH_THRESHOLDS="0" BUSINESS_DATA="1"/><Y_FILTER
CONDITION="GT"><NUM1>0</NUM1></Y_FILTER><X ID="RULE"/><FILTER IS_PARAMETERIZED="
Y"><TIME FORMAT="DD/MM/YYYY" TYPE="span" IS_PARAMETERIZED="Y" IS_MANDATORY="Y"
><SPAN LAST="0"><UNIT>MONTH</UNIT></SPAN></TIME></FILTER><STEPS NUM="0"
/><DISPLAY_PROPERTIES><GRID_COLOR>0</GRID_COLOR><
/DISPLAY_PROPERTIES><FILTER_DEFAULTS><CONTRACT IS_PARAMETERIZED="Y"
IS_MANDATORY="N">-1</CONTRACT></FILTER_DEFAULTS></REPORT></REPORT_ITEM><pdf><!--
<option><name>parameter name</name><value>parameter value</value></option>--><
/pdf></REPORT_GROUP>', 1, null, 100, 1, null, sysdate, sysdate, 0, 500, 0, 1,
0, 0)
```

4. To create the Compound report that includes the Service Level by Metric and Deviation by Metric reports, run the following SQL query:

```
insert into t_report_galleries (report_id, report_name, report_type,
report_description, report_xml, is_executable, schedule_id, report_owner,
report_hirarchy, is_grouped, report_gallery_create_date,
report_gallery_modify_date, is_inherit_parent_permissions, folder_id,
is_ready_type, is_parameterized, e2e_type, inherit_permissions)
values(90000003, 'Compound report which has Service Level and deviation
reports', 'COMPOUND', 'This report is compound report which return Service
Level and Deviation data by metric. This report is used by CA Service Catalog.
Please do not modify this report.','<REPORT_GROUP TYPE="COMPOUND" MARGIN="Y"
ITEMS="2" INLINE="0"><REPORT_ITEM ID="-100"><REPORT LOCALE="0" ORDER="ASC"
ORDER_BY="VALUE" TOP="0"><Y ID="DEVIATION" AGG="COUNT" WITH_CORRECTION="1"
SHOW_CORRECTION="1" WITH_EXCEPTION="1" WITH_ADJUST="1" WITH_INCOMPLETE="1"
INCLUDE_TARGET="0" INCLUDE_FORECAST="0" WITH_THRESHOLDS="0" BUSINESS_DATA="1"
/><Y_FILTER CONDITION="GT"><NUM1>0</NUM1></Y_FILTER><X ID="RULE"/><FILTER
IS_PARAMETERIZED="Y"><TIME FORMAT="DD/MM/YYYY" TYPE="span" IS_PARAMETERIZED="Y"
IS_MANDATORY="Y"><SPAN LAST="0"><UNIT>MONTH</UNIT></SPAN></TIME></FILTER><STEPS
NUM="0"/><DISPLAY_PROPERTIES><GRID_COLOR>0</GRID_COLOR><
/DISPLAY_PROPERTIES><FILTER_DEFAULTS><CONTRACT IS_PARAMETERIZED="Y"
IS_MANDATORY="N">-1</CONTRACT></FILTER_DEFAULTS></REPORT><NAME><![CDATA
[Deviation by Metric parameterized report]]></NAME></REPORT_ITEM><REPORT_ITEM
ID="-101"><REPORT LOCALE="0" ORDER="ASC" ORDER_BY="VALUE" TOP="0"><Y ID="
PROVIDED" AGG="AVG" WITH_CORRECTION="1" SHOW_CORRECTION="1" WITH_EXCEPTION="1"
WITH_ADJUST="1" WITH_INCOMPLETE="1" INCLUDE_TARGET="1" INCLUDE_FORECAST="0"
WITH_THRESHOLDS="0" BUSINESS_DATA="1"/><X ID="RULE"/><FILTER IS_PARAMETERIZED="
Y"><TIME FORMAT="DD/MM/YYYY" TYPE="span" IS_PARAMETERIZED="Y" IS_MANDATORY="Y"
><SPAN LAST="0"><UNIT>QUARTER</UNIT></SPAN></TIME></FILTER><STEPS NUM="0"
/><DISPLAY_PROPERTIES><GRID_COLOR>0</GRID_COLOR><
/DISPLAY_PROPERTIES><FILTER_DEFAULTS><CONTRACT IS_PARAMETERIZED="Y"
IS_MANDATORY="N">-1</CONTRACT></FILTER_DEFAULTS></REPORT><NAME><![CDATA[Service
Level by Metric parameterized report]]></NAME></REPORT_ITEM><pdf><!--
<option><name>parameter name</name><value>parameter value</value></option>--><
/pdf></REPORT_GROUP>', 1, null, 100, 1, null, sysdate, sysdate, 0, 500, 0, 1,
0, 0)
```

5. To create the Revenue by Metric report, run the following SQL query:

```
insert into t_report_galleries  (report_id, report_name, report_type,
report_description, report_xml, is_executable, schedule_id, report_owner,
report_hirarchy, is_grouped, report_gallery_create_date,
report_gallery_modify_date, is_inherit_parent_permissions, folder_id,
is_ready_type, is_parameterized, e2e_type, inherit_permissions) values
(90000006,'Revenue by Metric used by CA Service Catalog','NORMAL','This report
is parameterized report which return revenue by metric. This report is used by
CA Service Catalog. Please do not modify this report.','<REPORT_GROUP TYPE="
NORMAL" MARGIN="Y"><REPORT_ITEM><REPORT LOCALE="0" ORDER="ASC" ORDER_BY="VALUE"
TOP="0"><Y ID="REVENUE" AGG="SUM" WITH_CORRECTION="1" SHOW_CORRECTION="1"
WITH_EXCEPTION="1" WITH_ADJUST="1" WITH_INCOMPLETE="1" INCLUDE_TARGET="0"
INCLUDE_FORECAST="0" WITH_THRESHOLDS="0" BUSINESS_DATA="1"/><X ID="RULE"
/><FILTER IS_PARAMETERIZED="Y"><TIME FORMAT="DD/MM/YYYY" TYPE="range"
IS_PARAMETERIZED="Y" IS_MANDATORY="N"><RANGE><FROM>01/01/2010 00</FROM><TO>26/08
/2010 00</TO></RANGE></TIME></FILTER><STEPS NUM="0"
/><DISPLAY_PROPERTIES><GRID_COLOR>0</GRID_COLOR><
/DISPLAY_PROPERTIES><FILTER_DEFAULTS><RULE IS_PARAMETERIZED="Y" IS_MANDATORY="N"
```

```
>-1</RULE></FILTER_DEFAULTS></REPORT></REPORT_ITEM><pdf><!--
<option><name>parameter name</name><value>parameter value</value></option>--><
/pdf></REPORT_GROUP>',1,null,100,1, null,sysdate,sysdate,0,500,0,1,0,0)
```

You have created the reports for accessing metric-related SLA data.

Step 2 - Set the Administration Configuration Parameters

Setting and testing the administration configuration parameters for CA Business Service Insight in the CA Service Catalog GUI is a required task for this integration.

Follow these steps:

1. Click Configuration and click the CA Business Service Insight link under Options on the Administration tab of CA Service Catalog.

2. Click the Modify icon to next to each property that you want to update:

   - **Certificate Alias Name**
     Specifies the alias name (logical name) of the CA Business Service Insight certificate that is stored in the trusted store. If your CA Service Catalog implementation uses multiple certificates from other products, you can optionally merge all certificates into a single keystore file. You can do so with or without using Secure Socket Layer (SSL) and Hypertext Transfer Protocol Secure (HTTPS).

   - **Enable HTTPS**
     Specifies that CA Service Catalog and CA Business Service Insight use Hypertext Transfer Protocol Secure (HTTPS) to communicate.
     Select Yes to use HTTPS to communicate with CA Business Service Insight; otherwise, specify No.

     Important! If you specify Yes, verify that CA Business Service Insight is using HTTPS. If necessary, configure it to use HTTPS.

   - **Host Name**
     Specifies the computer name on which CA Business Service Insight is hosted.

   - **Keystore Name**
     Specifies the filename of the Java keystore file that includes the CA Business Service Insight public key certificate.

     Important! This file *must* reside in the USM_HOME directory.

   - **Keystore Password**
     Specifies the password for opening the keystore file, to read the certificate in the trusted store.

   - **Organization**
     Specifies the name of the CA Business Service Insight organizational unit.

- **Port Number - {1-65535}**
  Defines the port on which the CA Business Service Insight host listens for incoming connections. The default is 80.

- **User ID and User Password**
  Specifies the user ID and password that CA Service Catalog uses to log in to CA Business Service Insight.

3. Verify that you are finished updating configuration properties.

4. Click Test to test all connections between CA Service Catalog and CA Business Service Insight. The connections include the Open API and the login credentials.

5. Click the Launch button to open CA Business Service Insight.
   The connection is tested, using the new values that you specified. If the connection fails, try using a different value.

6. Recycle Catalog Component.

The CA Business Service Insight configuration details are updated with the values that you specified.

Step 3 - (Optional) Set the Request Management Configuration Parameters

Setting the request management configuration parameters is an optional but recommended task when you set up the integration with CA Business Service Insight. The catalog users who are requesting a service can view the related performance data for the service.

1. Select CA Service Catalog, Configuration, Request Management Configuration.

2. Click the Modify icon to next to each property that you want to update.

3. Verify the setting for the following parameter and update it if necessary.

- **Display Service Health**

Specifies whether to enable catalog users requesting a service to view actual, current data regarding the quality or "health" of a service, which is based on the level of compliance of the service to its associated metrics. The contractual metrics, incentive metrics, and SLA health period that is specified in the contract-specific details for the service option elements in the service being requested determine this data.The metric data includes both the performance criteria and the actual number of violations, including the time increments measured. If you enable this option, catalog users can view this actual, current metric data for the service they are requesting.

You have set the request management configuration parameters.

Step 4 - Add the Service Option Element for the Contract

A required task for integrating CA Business Service Insight and CA Service Catalog is creating a service option element that associates a meaningful CA Business Service Insight contract to a service option group.

For more information, see add the service option element for the contract (see page 3454).

Step 5 - Understand how the Integration Works After the Request Life Cycle Is Completed

The integration between the two products is most meaningful after the CA Service Catalog request has been approved and fulfilled. At that point, the requested resource is made available to the requestor, and CA Business Service Insight begins to monitor whether the resource meets the terms of contract. For example, for availability, efficiency, or other metrics.

For more information, see the section Understand how the Integration Works After the Request Life Cycle Is Completed (see page 3458).

Step 6 - Import the Adapter Package

The adapter package contains two files that package the CA Business Service Insight: CA Service Catalog adapter (the adapter) and related files. The adapter enables you to connect CA Business Service Insight contracts (including metrics) with CA Service Catalog services, so that you can monitor whether the delivery of the requested services meets or exceeds the terms of the contract. With that data, you can adjust the billing for the services, as needed, to include any contract-related adjustments.

Follow these steps:

1. Locate the file that is named CAServiceCatalogRequestSLA.mpxx in the Utilities folder of the CA Service Catalog installation media.

2. Log in to CA Business Service Insight as an administrator.

3. Import the CAServiceCatalogRequestSLA.mpxx file, as follows:

    a. Click Administration, Content Transfer, Packages.

    b. Click Upload Package.

    c. Browse to the CAServiceCatalogRequestSLA.mpxx file, select it, and click Upload.
    The package is uploaded and is available for import. If the file already exists, you receive an error message from CA Business Service Insight. If you receive such a message, verify that the file exists by opening the Import page that is mentioned in the next step. Verify whether the file appears in the list of files available for import.

4. Import the CAServiceCatalogRequestSLA.mpxx file, as follows:

    a. Click Administration, Content Transfer, Import from Menu bar.
    The CA Business Service Insight Import page opens.

    b. Select the package that is named CAServiceCatalogRequestSLA from the drop-down list.

    c. Select Skip and Continue as the On Collision option.

    d. Click Import.

    If the import process fails, verify that none of the artifacts being imported already exists on the target computer.
    This process requires a few minutes to complete.

5. Locate the SQL adapter configuration file for your DBMS:

   - CA Service Catalog Request Mgmt Sys AdapterConfig_Oracle.xml
   - CA Service Catalog Request Mgmt Sys AdapterConfig_SqlServer.xml

   You use this file to read CA Service Catalog request data from your database depending on whether you are using Oracle or Microsoft SQL Server.
   Verify that the file for your DBMS resides on the computer on which you open CA Business Service Insight.

6. Verify that the following artifacts are created:

   - A service domain named *Request Management*.
   - Two domain categories that are named *Number of times the Permissible Time Exceeded Target* and *Response Time*.
   - A Service component named *Service Catalog Request Management System*.
   - An event type named *Catalog Request Status Time Event Template*.
   - A resource type named *Catalog Request Management System*.

   Two translation tables *SOE_Resource_Map_Table*

   and*Catalog_Event_Transl_Table (SOE=service option elements)*

   - Two translation scripts: one for creating resources from CA Service Catalog service option elements and another for creating event type for different statuses
   - Two business logic templates *Number of Violations* and *Average Time*.
     The Average Time template calculates the average time for a request to transition from one status to another. For example, from Submitted to either Approved or Rejected, or from Pending Fulfillment to Fullfilled.

   These artifacts form a "framework" for holding contract-related data about CA Service Catalog services.

7. Obtain the ID of the event type that is named *Catalog Request Status Time Event Template*. This ID is required when you create the adapter (see page 3452). To obtain the ID:

   a. Open the Configuration menu and click Event Types.

   b. Move the mouse over the event type to display the ID.

   c. Record the ID for use when you create the adapter.

You have imported the adapter package and are now ready to create the adapter.

Step 7 - Create the Adapter

After you have imported the adapter package, you are ready to create the adapter. This task is required to enable the integration between CA Service Catalog and CA Business Service Insight.

Follow these steps:

1. On the computer where CA Business Service Insight is hosted, open the SQL adapter configuration file for your DBMS:
   - CA Service Catalog Request Mgmt Sys AdapterConfig_Oracle.xml for Oracle
   - CA Service Catalog Request Mgmt Sys AdapterConfig_SqlServer.xml for Microsoft SQL Server (SQL Server)
2. Locate the following line in that file:

   ```
   "FieldDisplayName="Catalog Request Status Time Event Template" AdditionalData="
   1500"
   ```

3. Verify that the value for the AdditionalData= expression in this file matches the ID you recorded for the event type that is named *Catalog Request Status Time Event Template* at the end of the procedure to import the adapter (see page 3450).
   If the ID in the file is different than the ID you recorded, update the ID in the file to match the one you recorded.
   Save your changes (if applicable) and close the file.
4. Log in to CA Business Service Insight.
5. Click Administration, Configuration, Adapters.
6. Click the Add New button and select the option that is named Create from configuration file.
7. Browse the local computer on which you opened the browser. Select the SQL adapter configuration file for your DBMS (from Step 1), and click OK.
   After a short wait, the adapter is created, and a configuration window opens.
8. Configure the newly created adapter, as follows:
   a. Specify a suitable name to the adapter, such as CA Service Catalog Adapter.
   b. Select the address for the adapter.
      You typically specify the address of the CA Business Service Insight server.
      If applicable, select the Localhost option.
      Otherwise, click Add adapter address to create an address.
   c. Select a time zone and click Next.
   d. Update the server name and user credentials for the database to match the CA Service Catalog database.
   e. Click Test Connection and click Next.

f. Click Test Query and click Next.

g. Verify that the results are valid and click Next.
The mapping screen appears.

9. Click Finish.

You have installed the adapter and can now test the adapter (see page 3453).

Step 8 - Test the Adapter

After you have imported and installed the adapter, test it to verify that it works properly in your implementation. This task is required to enable the integration between CA Service Catalog and CA Business Service Insight.

Follow these steps:

1. Open the Windows Control Panel and verify that the following CA Business Service Insight services are running. If necessary, start them:
   - Oblicore - AdapterDeployment
   - Oblicore - AdaptersListener
   - Oblicore - ScriptHost
   - Oblicore - TaskHost (For translation)
2. Verify that your CA Service Catalog implementation includes active services and requests.
3. Log in to CA Business Service Insight. Use its scheduler to schedule the adapter to run every 30 through 60 minutes.
4. Wait for the first scheduled run of the adapter to complete. Log in to CA Business Service Insight, and select Configuration, Translation, Translation Entries.
5. Verify that the adapter has generated at least a few pending entries. The adapter cannot process the pending entries now, because the event types and resources that are related to these entries are not yet created.
6. Wait for the next scheduled run to complete. Log in to CA Business Service Insight, and select Configuration, Translation, Translation Entries.
7. Verify that the following changes have occurred:
   - The pending entries are translated.
   - The new resources of the type that is named *Catalog Request Management System* are created. These represent service option elements in requests that CA Service Catalog users have submitted.
   - New event types are created, similar to the following examples:

- 101-2-CatalogRequestStatusChangeEvent
- 101-200-CatalogRequestStatusChangeEvent
- 101-2000-CatalogRequestStatusChangeEvent

Using these event types, resources, and other imported artifacts, you can optionally create new contracts with metrics and link them to CA Service Catalog services.

Add the Service Option Element for the Contract

This article contains the following topics:

You can associate *only one* CA Business Service Insight contract to a service option.

Follow these steps:

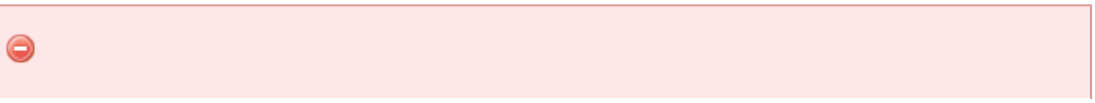
1. Navigate to CA Service Catalog, Service Offerings, Option Groups tab.
2. Click the service option group name to which you wish to add the new service option element.
3. Double-click the new row or column heading to add a new row or column of cells.
   a. Double-click a new, empty cell to define a new service option element.
   b. Double-click an existing service option element to edit the definition of an existing service option element.

   The Service Option Element Definition window is displayed.
   The Service Option Element Definition window is used to specify the characteristics of a service option element using two tabs, Definition and Options.
4. Select CA Business Service Insight Contract for Type on the Definition tab and specify the contract-specific details (see page 3454).
   This option associates a CA Business Service Insight service level agreement and enables you to specify details for this association.
5. Also on the Definition tab, complete the remaining fields and click Update.
   These remaining fields are not related to the CA Business Service Insight integration. But, these fields are required for all service option elements in CA Service Catalog.

The changes to the service option element are updated.

Contract-Specific Details for the Service Option Element

Specify the contract-specific details when you add the service option element for the contract.



Important! Consult an administrator with knowledge for assistance to complete these fields. This knowledge is critical for specifying meaningful values that result in effective monitoring of the quality of services.

- **Display Text**
  Specifies a brief summary of the contract for the catalog user requesting the service.

- **Contract**
  Select the contract that you want from the drop-down list. The list shows contracts that have been created, tested, and committed in CA Business Service Insight.
  Typically, an organization has relatively few contracts, each with service components and metrics that you can associate to a service option element. Optimally, an organization develops services and contracts together.
  Click the View link to see the contract details, especially the effective period (starting and ending dates) of the contract. Review the effective period of *both* the contract and the service option group. Verify that they match or that effective period of the service option group is contained within the effective period of the contract. If a conflict exists, you can still associate the contract to the service option element. But, you *cannot* measure performance (obtain metric data) during the discrepancy period.
  Viewing the contract details helps you make more informed decisions when you complete the other remaining fields on this dialog.

- **Service Component**
  Select the service component (service) to monitor the contract that is selected in the previous field. A contract typically covers one or more service components.
  In each service option element, you can select one service component to monitor.
  Verify that this service component is meaningful for *both* the selected contract and the service option group you are modifying.
  Click the View link to see details about the metrics that apply to the selected service component details.
  Service components are related to, but independent of, contracts.

- **Contractual Metrics and Incentive Metrics**
  Contractual metrics specify minimum quality-of-service requirements. For example, average response time of two business days to fulfill requests to fix or replace broken laptops.
  Incentive metrics can specify one or both of the following options:

  - Discounts to the customer from the service provider, for the service provider failing to meet the minimum requirements of the contract. For example, an incentive metric can specify a discount of $100 each day the service provider fails to fulfill an average of 100 requests per hour during normal business hours and 10 requests per hour outside of normal business hours.

  - Extra charges to the customer from the service provider, for the service provider exceeding the minimum requirements of the contract. For example, an incentive metric can specify an extra $100 charge for every day when the average response time is less than one-half of the maximum response time.

  The specific metrics available depend on the selected contract and service component. Typically, you associate ten or fewer of each type (contractual and incentive) to a service option element. The metrics that you select determine both the financial adjustments for the associated service at

invoice time (if any) and the health of each service that contains this service option element. CA Service Catalog displays this data to catalog users requesting a service when they click the link to check the health of a service that contains this service option element.

- **SLA Health Period**
  Defines the time increments to use for filtering and displaying the metric-related SLA data. Examples include per hour, day, week, month, year, or a custom-specified time period.
  Verify that the increments you select are meaningful for the contract, service component, and metrics that are selected.
  You can configure the request management configuration parameters (see page 3449) to display the selected contractual metrics and the SLA health period to catalog users when they request a service that contains this service option element.

- **Charge for SLA**
  Specifies the charge for maintaining an SLA. If you check this box, more fields open for you to specify the details of the charge (see page 3456).

- **Associate Service Option Group**
  Indicates that a service option group is associated with this service option element. Checking this field exposes a list of tiered service option elements, allowing the administrator to select an associated service option element and tier type (see page 3458).

  Note: These fields are intended for use by customers who formerly integrated CA Service Catalog and now want to integrate CA Service Catalog with CA Business Service Insight to achieve compatible results.

Charge for SLA - Details

If you check Charge for SLA on the Contract-specific Details for the Service Option Element, the following fields appear. These fields provide a means of specifying charges or credits to an account, *either* instead of *or* in addition to the metrics specified in the contract.

- **Cost Type**
  Specifies the type of cost for the SLA. Select from the following list:

  - **Specify Value**
    Specifies the cost value that appears in the catalog and the requesting or subscribing user cannot change the value.
    This setting exposes the following field:
    Unit Cost - The cost per SLA that is to appear in the catalog.

  - **User Specified**
    Specifies the default cost value that appears in the catalog. The requesting or subscribing user can change the value.
    This setting exposes the following field:
    Default Unit Cost - The default cost value that is to appear in the catalog.

  - **Allocate Cost**
    The cost is allocated based on a Set as established in Budgeting and Planning in Service Accounting Component.
    This setting applies only if Service Accounting Component is installed.

This setting exposes the following fields:
Default Unit Cost - This value in this field is set to 0, because the cost value is determined from the Set value that is specified and the associated value for this service option element in that set, together with the Allocation Method.
Set - List of Budgeting and Planning sets available through Service Accounting Component.
Allocation Method - The list of allocation methods for the value in the budgeting and planning set for this service option element.
Assign - Use the value in the set for the total cost of this service option element.
Distribute by Subscribed Account - Use the value in the set for this service option element that is divided by the number of accounts that are subscribed to this service option element.
Distribute by Subscription - Use the value in the set for this service option element that is divided by the number of subscriptions to this service option element.
Weighted Distribution - Use the value in the set for this service option element that is allocated according to actual usage by the account.

- **Standard Cost**
  The cost is allocated based on a Set value as established in Budgeting and Planning in Service Accounting Component.
  This setting applies only if Service Accounting Component is installed.
  This setting exposes the following fields:
  Default Unit Cost - This value in this field is set to 0, because the cost value is determined from the Set value that is specified and the associated value for this service option element in that set, together with the Allocation Method.
  Set - List of Budgeting and Planning sets in Service Accounting Component.
  Allocation Method - The list of allocation methods for the value in the budgeting and planning set for this service option element.
  Assign - Use the value in the set for the unit cost of this service option element.

- **Display Unit Type**
  Specifies the text value that appears with the cost value.

- **Billing Cycle**
  Indicates how the cost value is applied to an invoice if Service Accounting Component is installed. Select from the following list:

  - **One-Time**
    The charge is applied one time.

  - **Installments**
    Cost is applied on an "installment plan": the entire cost is spread across several payments over time, rather than a single payment of the entire cost.
    This setting exposes the following fields:

    - Periodic Type: The type of interval to be used when applying the cost: Daily, Weekly, Monthly, or N/A.

    - Periodic Type Interval: The frequency of the interval that is specified in Periodic Type field that is used to determine the billing interval of the cost.

    - Number of Installments: The number of times the cost must be applied.

- **Periodic**
  This setting exposes the following fields:
  Periodic Type: The type of interval to be used when applying the cost: Daily, Weekly, Monthly, or N/A.
  Periodic Type Interval: The frequency of the interval that is specified in Periodic Type field that is used to determine the billing interval of the cost.

- **N/A - Not applicable**
  Specifies that this field does not apply.

- **Charge Type**
  Indicates whether cost value must appear as a Charge or a Credit on an invoice from Service Accounting Component.

- **Budget**
  Indicates whether the item is associated with a budget.
  If Service Accounting Component is installed, the Administrator can associate a cost value with a Budgeting and Planning set value that is associated with this service option element.
  If Service Accounting Component is not installed, this field serves as additional categorization for the service option element.

Tier Type - Details

If you check Associate to Service Option group on the Contract-specific Details for the Service Option Element, the following fields appear. These fields mainly provide a means of specifying charges or credits to an account, either *instead of* or *in addition to* the metrics specified in the contract.

Tier Type

Specifies the name of the tier type that you select; the default is Lookup.

A tier is a single row in a tiered service option group. Association into a tiered service option group starts at the top row and moves down, with the top tier having the lowest tier values.

A service option element with a defined tier type matches the right tier in the specified tiered service option group (where the tier service option group is specified in the same service option element when the tier type is defined).

Lookup

Use the first tier that matches the value being passed to the tiered service option group.

Lookup Multiple

Use each tier that matches the value being passed to the tiered service option group.

Understand how the Integration Works After the Request Life Cycle Is Completed

This article contains the following topics:

1. Once the request is fulfilled and the user attempts to begin using the requested service or services, CA Business Service Insight monitors:

   - The resources that are specified in the service component.
   - The metrics that are selected in the service option element or elements that are associated with a contract.

2. CA Business Service Insight retains the contract metric-related data (see page 3459). CA Business Service Insight retrieves related data from CA Service Catalog to:

   - Display service health, which the contractual metrics determine, incentive metrics, and SLA health period that are included in the contract-specific details for service option elements.
   - Calculate SLA violations and adjustments. When you run invoices in CA Service Catalog, it queries CA Business Service Insight for statistics regarding the contractual and incentive metrics, to determine any applicable extra charges or discounts to be included in the invoice.

Create Billing Adjustments for Metric-Related SLAs

The metrics that you select when you specify the contract-specific details for the service option element essentially define SLAs for the service that includes the service option element. These SLAs provide extra charges for services that exceed contract terms and also provide discounts for services that fail to meet contract terms. To include these extra charges and discounts when you run invoices, you create an SLA violation adjustment for either all accounts or specific accounts. Once you create the adjustment, CA Service Catalog automatically includes it during invoice runs and adjusts the final amount of the invoice.

Follow these steps:

1. Verify that the effective dates of the service, service option group, and service option element are included within the effective dates of the contract associated with the service option element (see page 3454).
   Adjustments for the invoice do not include any discrepancy period between these effective dates. For example, suppose the effective dates for the service, service option group, and service option element include the entire calendar year, January through December, while the effective dates for the contract cover February through December. In this case, the invoice for January includes no extra charges and no discounts that are related to SLAs.

2. Click Accounting, Adjustments, SLA Violation, Add SLA Violation Adjustment.

3. Complete the fields on the page.

   - **Business Unit**
     Specifies that this adjustment applies to all accounts in the service provider business unit.

- **Adjustment Name**
  Specifies an intuitive name for the adjustment.
  You can optionally create a single adjustment for all accounts that use a specific service, or you can create individual adjustments for individual accounts that use that service. The latter approach is required if you want to specify different adjustment criteria for different accounts that use the same service.

- **Adjustment For:**
  Specifies either all accounts or a specific account.
  If you select a specific account, the adjustment types (fixed or proportional) do not apply. Instead, the account you specify receives the entire adjustment and other accounts are not affected.

- **Description**
  Specifies a brief description for the adjustment.

- **Status**
  Specifies whether the adjustment is active or inactive.

- **Adjustment Type**
  Specifies whether the adjustment in the invoice is fixed or proportional.
  Fixed adjustments divide the total extra charge or discount equally across all accounts, as illustrated in the example of fixed charges (see page 3460).
  Proportional adjustments divide the total extra charge or discount proportionally across all accounts, which are based on the number of subscribers per account, as illustrated in the example of proportional charges (see page 3461).

- **Apply to Service**
  Specifies the service to which this adjustment applies.

- **Service Option Group**
  Specifies the service option group to which this adjustment applies.

- **Service Option Element**
  Specifies the service option element to which this adjustment applies.
  The CA Business Service Insight contract, service component, and metrics that determine the adjustment are defined in this service option element.

4. Click OK.

The adjustment is saved.

Example of Fixed Charges

Fixed adjustments divide the total extra charge or discount equally across all accounts, as illustrated in this example.

The extra adjustment for a service is $20. Two accounts are subscribed to the service: Account-A and Account-B.

Account-A includes seven subscriptions, while Account-B includes three subscriptions.

Both Account-A and Account-B each receive a $10 adjustment.

Example of Proportional Charges

Proportional adjustments divide the total extra charge or discount proportionally across all accounts, which are based on number of subscribers per account.

The extra adjustment for a service is $20. Two accounts are subscribed to the service: Account-A and Account-B.

Account-A includes seven subscriptions, while Account-B includes three subscriptions.

The adjustments are calculated as follows:

Total number of subscriptions = 7 + 3 = 10

Total number of accounts = 2

Adjustment for Account-A = (20x7)/10 = 14

Adjustment for Account-B = (20x3)/10 = 6

Thus, Account-A receives a $14 adjustment, while Account-B receives a $6 adjustment.

Publish Dashviews in Dashboards

Dashviews are important components in CA Business Service Insight for publicizing performance measurements from contracts, especially metric-related data. As an administrator, you can create dashviews in CA Business Service Insight and can publish them in CA Service Catalog. By doing so, CA Service Catalog users better understand the quality and performance of services over time.

CA Business Service Insight administrators create dashviews as graphical representations of performance data for CA Service Catalog services. The performance data shows the quality of the services over time. Dashviews are containers that typically hold either a widget (speedometer) or a report that helps to organize information.

You can embed dashviews in portals and can resize them. You can configure dashviews to display a background image that helps represent the status of multiple entities The entities can be countries, organizational units, and stages of a process.

Note: For more information about creating and managing dashviews in CA Business Service Insight, see your CA Business Service Insight documentation.

Follow these steps:

1. Design your dashviews to meet your requirements in CA Business Service Insight.

2. Identify the dashviews that you want to publish in CA Service Catalog; if necessary create new ones. Select dashviews related to services better understand the quality and performance of services over time.
   You can optionally do either or perform both of the following actions:

   - Select dashviews for one or more contracts that are linked to your most commonly used services.
   - Select a dashview that highlights specific metrics in such a contract.

3. Record the following information about the dashviews that you have chosen to publish in dashboards:

   - Dashview ID
   - User name who owns the dashboard
   - Organization to which the user belongs
   - Name of the CA Business Service Insight server on which the dashview resides

Create a dashboard item of type External Web Content for each dashview, in CA Service Catalog.

- Using the information from Step 2, replace the text field that is named Content URL in each dashboard item with the following URL:

  ```
  http://[ServerName]/NewDashboard/DashboardWebPart.aspx?dashviewId=[ID]&username=[CA Oblicore Guarantee username]
  &organization=[Organization]
  ```

  For example:

  ```
  http://hesed333/NewDashboard/DashboardWebPart.aspx?dashviewId=32&username=sadmin&organization=CA
  ```

Verify the Health of Services

As an administrator, advise catalog users to view the health of a service when they create a request, if *all* of the following conditions are met:

- The service is associated to metrics in a CA Business Service Insight contract.
- The association is configured to display the health of the service.
  Administrators optionally specify both of these settings when they configure the contract-specific details for the service option elements (see page 3454) in the service being requested.
- The Display Service Health configuration parameter (see page 3449) is enabled.

Catalog users can view the quality or "health" of a service, which is based on the level of compliance of the service to its associated metrics.

Note: For individual services, verify that the dashview data (from Step 1) matches the health-of-service data (from Step 2).

Follow these steps:

1. Click Home, Requests.
2. Find the service that you want in the catalog, using one of these sections.
3. Open the service that you want and view its details.
4. Click View Service Health.
   The metric data for the service appears. The data includes both the performance criteria and the number of violations during the time increments specified by the administrator. Time increments can be per hour, day, week, month, or year.
5. Review the data and decide whether the service levels meet your expectations.

Using the data, you can either finish and submit the request or cancel the request.

Integrating CA Asset Portfolio Management

Integrate with CMDB

The article contains the following articles:

This section explains how to integrate CA APM with CMDB Release 12.7 and CMDB that is included in CA Service Desk Manager Release 12.7.

CMDB is a comprehensive, integrated solution for managing the IT components and services in an enterprise and their relationships, in heterogeneous computing environments. CMDB lets you provide and store reliable, up-to-date information about assets, known as configuration items (CI), and their relationships with each other. These relationships form the basis for impact analysis, an important tool for controlling change within an organization.

CMDB integrates with CA APM in several areas, including the following areas:

The CA APM audit history records can include all of the changes that have been made to asset/CI records by CA Service Desk Manager, CMDB, and CA APM.

- When CA Service Desk Manager and CMDB are installed, the asset/CI audit history records include any CA APM audit history records on the CMDB Versioning tab.
- When you define an asset in CA APM, you can categorize and control the asset and CI records by selecting or clearing the Asset and CI check boxes. This flexibility is provided because CIs that CMDB creates may not be relevant to CA APM. Conversely, assets that CA APM creates may not be relevant to CMDB.
- CA APM can extend the fields on an asset/CI within the context of *asset families*. The extended fields can be shared in CA APM. For example, a CA APM administrator can configure the Asset page and define an asset extended field to let users view and update a CI that is created in CA Service Desk Manager and CMDB.
- You can define an event on a field that is shared with CMDB in CA APM and trigger the event in either CA APM or CMDB. For more information about managing events and notifications, see Events and Notifications (see page 2376).
- A CA Service Desk Manager and CMDB user can define a Management Data Repository (MDR) and allow the CMDB CI to launch the corresponding asset in CA APM.

How to Integrate CA APM and CMDB

When you integrate CA APM and CMDB, you integrate and delineate the assets that CA APM manages from the configuration items (CIs) that CMDB manages in a simple and concise manner. The CA APM users can move to a shared classification model for the assets and CIs. To integrate CA APM and CMDB, complete the following steps:

1. Share asset and configuration item audit history records.
2. Categorize the asset and configuration item records.
3. Define an asset extended field.
4. Define an event on a shared field.
5. Define a Management Data Repository (MDR) from CA Service Desk Manager and CMDB.

Share Asset and Configuration Item Audit History Records

To integrate CA APM and CMDB, the CA APM audit history records can include all of the changes that were made to asset/CI records by CA Service Desk Manager, CMDB, and CA APM. In addition, when CA Service Desk Manager, CMDB, or both are installed, the asset/CI audit history records in CMDB (Versioning tab) includes any CA APM audit history records.

CMDB 11.2 and greater includes audit history records from CA APM. The audit history records are updated in both CMDB and CA APM when the CA Asset Portfolio Management - Event Service service is started. For more information, see Start the Services.

Categorize the Asset and Configuration Item Records

In this step to integrate CA APM and CMDB, you can categorize and control the asset and CI records when defining an asset in CA APM by selecting or clearing the Asset and CI check boxes. This flexibility is provided because CIs that CMDB creates may not be relevant to CA APM and conversely, assets that CA APM creates may not be relevant to CMDB.

Consider the following information when using these check boxes:

- **Default Values**
  - All new asset records that CA APM creates are initially set both as an Asset only and Managed by CA APM. On the New Asset page in CA APM, the Asset check box is selected, the Managed by CA APM check box is selected, and the CI check box is not selected.
  - All asset records that CMDB creates (with or without CA Service Desk Manager) are initially set to CI only. On the CI pages in CMDB, the CI? column heading is set to Yes and the Asset? column heading is set to No.
  - Both CA APM and CMDB have the Asset and CI fields available on the New Asset and CI pages. However, the Managed by CA APM check box is only viewable in CA APM. The existing audit and security features for each product applies to these check boxes.
- **Appearance**
  - The Asset and CI fields appear in CA APM and CMDB even when other CA Technologies products are installed. The Asset and CI fields do not appear in CA Service Desk Manager when CMDB is not installed.
  - The CA APM administrator can configure the user interface and move the Asset and CI fields to a new location, make the fields read-only, required, or optional, and hide the fields.

    Note: For more information about configuring the user interface, see How to Configure the User Interface (see page 1520).
- **Viewing and Updating**
  - **CA CMDB**
    - By default, the CMDB analyst and administrator can update the Asset and CI field values.
    - CMDB, by default, does not allow the Asset? value to be changed when the Asset? value is set to Yes.
  - **CA APM**
    - By default, CA APM sees asset and CI records.

- The CA APM administrator can configure the user interface and move the Asset and CI check boxes to a new location, make the check boxes read-only, required, or optional, and hide the check boxes. After you select the CI check box and save the asset, the CI check box is not available and you cannot change the setting.

  Important! We strongly recommend that you configure the CI check box in CA APM as read-only and restrict changes to the check box to only the CMDB analyst and administrator.

- An asset in CA APM in which the Managed by CA APM check box is selected is always an asset. You cannot save an asset in CA APM in which the Managed by CA APM check box is selected without also selecting the Asset check box.

- **Searching**
  - **CMDB**
    - The CMDB search initially displays, by default, all records. However, an option is provided to filter records.

      Note: If CA Service Desk Manager is installed, the same default search rules apply.

  - **CA APM**
    - The default asset search includes a drop-down list for Managed by CA APM, CI, and Asset. This flexibility is provided so that you can differentiate between assets and CIs.

- **Hardware Reconciliation**
  Hardware reconciliation analyzes all asset and CI records. Searches provide a way to view any CIs that are related to discovered assets as the result of running hardware reconciliation. A CA APM user can view the exceptions and determine whether they want to select the Asset check box. As a result of selecting the Asset check box, the asset records are available in a CA APM asset search.

Define an Asset Extended Field

In this step to integrate CA APM and CMDB, CA APM can extend the fields on an asset within the context of *asset families*. The extended fields can be shared in CA APM. For example, a CA APM administrator can configure the Asset page and define an asset extended field to let users view and update a CI that is created in CA Service Desk Manager and CMDB.

Important! These steps work only the first-time you complete the wizard and define the asset extended field. Before you define the extended field, verify that you have the following information from the usp_owned_resource table in CA CMDB for reference: table name, format (character, boolean, currency, date, decimal, or integer), field name, attribute name, and field size. After you complete the wizard, you can configure the extended field like any field in CA APM.

Example: Define an Asset Extended Field for Warranty Start Date

In this example, you define an asset extended field for Warranty Start Date. In CA Service Desk Manager/ CA CMDB on the Inventory tab, you view the label in the CI as Warranty Start Date. Next, you view the information for the associated nr_wrty_st_dt column from the usp_owned_resource table in CMDB. In this example, the nr_wrty_st_dt column format is integer, the field name is nr_wrty_st_dt, the attribute name is nr_wrty_st_dt, and the field size is 4. Record and enter this information exactly as it appears in the appropriate Format, Field Name, Attribute Name, and Field Size fields in the wizard. We also recommend that to avoid confusion, you use the same label for the CI (Warranty Start Date) on the Label field in the wizard.

To define an asset extended field

1. Determine the CA Service Desk Manager and CMDB extension table name and database field name by reviewing the CA Service Desk Manager and CMDB schema files.

   Note: For more information about the CA Service Desk Manager and CMDB schema files, see the CA Service Desk Manager and CMDB documentation.

2. Log in to CA APM using login credentials in which you have permissions to define an extension.

3. Click Asset, New Asset.

4. On the left, click CONFIGURE: ON.
   The configuration of the page is enabled.

5. In the Configuration Information area of the page, define and save a global configuration.

6. Click Add Extension.
   A wizard appears.

7. Follow the on-screen instructions to enter the information for the extended field.

8. In the Type page of the wizard, complete the following steps:

   a. Select the Simple Field option.

   b. Select the part of the page on which the new field appears.

   c. Select the Across all extended types check box.

d. Click Next.

9. In the Fields page of the wizard, complete the following steps:

> **Important!** Enter the column information from the usp_owned_resource table in CMDB. We also recommend that to avoid confusion, you use the same label for the CI on the Label field.

a. Click Add Field.

b. Enter the field label to appear on the page.

c. Select the data format.

d. Enter the database field name.

e. Enter the attribute name.

f. Enter the field size.

g. (Optional) Enter a description for the field.

h. Specify whether an entry for the field is required.

i. Click the checkmark icon to save the field.
The product displays the field information you enter.

j. Click Next.

10. In the Summary page of the wizard, review the field information and click Save and Exit.

11. Verify that the field appears on the Asset page.

12. Click Save Configuration.
All users see the extended field on the page. You can define an event in CA APM and trigger the event in either CA APM or CMDB. For more information about managing events, see Events and Notifications (see page 2376).

Define an Event on a Shared Field

You can define an event in CA APM on any field that is shared between CA APM and CMDB. When the criteria for the event occurs by a change in CA Service Desk Manager/CMDB or CA APM, the event will complete and the notification will be sent. For example, you can define an event on the Asset page for the Contact field. If the event is a change event, the event can be completed when you change the Contact field in either the asset or the related configuration item (CI). Once the event has completed, a notification will be sent.

Note: For more information about managing events and notifications, see Events and Notifications (see page 2376).

Define a Management Data Repository (MDR) from CA Service Desk Manager and CMDB

In this step to integrate CA APM and CMDB, a CA Service Desk Manager and CMDB user can define a Management Data Repository (MDR) and allow the CMDB CI to launch in context the corresponding asset in CA APM.

To define a MDR from CA Service Desk Manager and CMDB

1. In the CA Service Desk Manager web interface, log in as an administrator.
2. Select the Administration tab. From the Administration browser, select CMDB, MDR Management, MDR List.
3. Click Create New.
   The MDR Provider definition appears.
4. Enter the following required MDR provider information:
   - **Button Name**
     Specify *ITAM* as the button name.
   - **MDR Name**
     Specify *ITAM* as the MDR name.
   - **MDR Class**
     Specify *GLOBAL* as the MDR class.
   - **Hostname**
     Specify the CA APM server name by using the network address or the DNS name of the CA APM web server.

   Important! The MDR provider form automatically populates the URL for Launch in Context field based on the information that you provide, so you do *not* enter a value for this field.
5. Click Save.
   The CA APM MDR provider is defined.
6. In CMDB, define a CI.
7. Click the Attributes tab in the CI detail form.
8. Click the ITAM button that you previously defined.
   The corresponding asset in CA APM appears.

Integrate with CA Service Catalog Manually

Important! Review the following section only if you want to manually integrate CA Asset Portfolio Management with CA Service Catalog when the automatic integration between the two has failed.

CA Service Catalog integrates with CA Asset Portfolio Management in several areas, including these areas:

- Requested items can be associated with CA Asset Portfolio Management Assets. Asset managers can associate CA Asset Portfolio Management assets with items requested from the catalog during request fulfillment.
- Catalog entries can be associated with CA Asset Portfolio Management Models. CA Service Catalog catalog administrators can associate one or more CA Asset Portfolio Management models with a service option. This association can assist with automated asset creation and association during request fulfillment using a workflow process and the CA Service Catalog web services.

Important! CA Service Catalog and CA Asset Portfolio Management must share the same MDB and the same CA EEM for this integration to work properly.

Requirements for the integration:

- You must have a role defined in CA Asset Portfolio Management.
- Verify that CA Asset Portfolio Management supports your internet browser.
- Check whether the CA Asset Portfolio Management application and web servers reside on the same computer or different computers. If they reside on different computers, complete the CA Asset Portfolio Management web services section in the administration configuration settings on the CA Service Catalog GUI.
- Authorized CA Service Catalog users use the CA Asset Portfolio Management Model Assignments window to assign eligible assets during the fulfillment of a request.

You can assign the assets through CA Service Catalog services if the following requirements are met:

- The assets must be active.
- The assets must not be assigned to any user.

You can associate one or more CA APM models with a service option, if the following requirements are met.

CA Service Catalog and CA Asset Portfolio Management administrators work together to use one of the following methods to authorize CA Service Catalog users (typically request managers) to assign assets:

1. Assign to the user the Fulfiller role in CA Asset Portfolio Management.

2. Assign to the user another role in CA Asset Portfolio Management that can update the Asset Fulfillment object. If you use another role, it must have the same Asset Fulfillment security settings as the CA Asset Portfolio Management Fulfiller role.

3. Specify a proxy user for CA Asset Portfolio Management in CA Service Catalog. To specify this proxy user, select **Administration**, **CA APM Web Services**, and complete the fields. Specify this CA Asset Portfolio Management user in the **User ID** field.
   In this case, CA Service Catalog users inherit the authority of the proxy user to assign assets.

Note: For information about fulfilling requests from inventory, see How to Fulfill Requests from Inventory (see page 2088).

Follow these steps:

Step 1 - Create Users in CA Service Catalog

To enable the integration between CA APM and CA Service Catalog, create customized users in CA Service Catalog specifically for use with this integration.

Follow these steps:

1. Determine a CA APM user ID that CA Service Catalog can use as a proxy user.
   You can supplement the proxy user with the following CA Service Catalog users:

   - The Service Delivery administrator, service designers, and catalog administrators can associate service options to models.

   - Request managers can use the gold brick icon to fulfill the requests pending action that are assigned to them.

Note: If you specify a proxy user, the Catalog system uses the proxy user, *not* authorized request managers, to fulfill the requests.

2. As a catalog administrator, work with a CA APM administrator to meet these criteria:
   - This user must be an authorized user in CA APM.
   - In the user details in CA APM, under Permissions, for Role Details, Asset Fulfilment Access is required.
3. Log in to CA Service Catalog as the spadmin user or another user with the Service Delivery Administrator role.
4. Select Administration, Configuration, CA APM Web Services in CA Service Catalog. Specify the CA APM user ID from the previous step in the User ID field.
5. Set up the following users:
   - Catalog User
   - Request Manager (Approver for the Catalog User)
   - Service Delivery Administrator, typically spadmin (Fulfiller)
6. Enable all rules for Event Type: Request/Subscription Item Change except When Status is Pending Fulfillment.
7. Log out of CA Service Catalog.

Step 2 - Create or Update Administrator in CA EEM

To enable the integration between CA APM and CA Service Catalog, create customized users in CA EEM specifically for use with this integration.

Follow these steps:

1. Log in to CA EEM as EiamAdmin. For Application, select Global.
2. Select Manage Identities, Users and click Go, without specifying any search criteria.
3. If the Administrator user already exists under the Users node, skip this step.
   Otherwise, create the Administrator user under Users node, and specify Administrator for the Name and the Display Name.
   Set the password for this Administrator user and click Save.
   For more information about creating global users in CA EEM, see the CA EEM (https://wiki.ca.com/display/eem1251/Create+Global+Users) documentation.
4. Log out of CA EEM.

Step 3 - Configure CA APM

To enable the integration between CA APM and CA Service Catalog, configure CA APM for use with this integration.

Note: The CA EEM-related steps apply specifically to CA APM 11.3.4. For equivalent steps for CA APM Release 12.6, see the CA APM documentation.

To configure CA APM

1. Log in to CA APM as an administrator.
2. In CA APM Security, assign the Service Delivery Administrator (the Fulfiller created in Create Users in CA Service Catalog (see page 3471)) to act as UAPM Fulfiller.
   For more information to perform this task, see Administering CA Asset Portfolio Management (see page 1568).
3. Start the CA APM Configurator and open CA APM.
4. In CA APM, under Option 3, Choose Your Security Type, select EIAM with Single DB Login.
5. Enter the host name of the computer on which CA EEM is installed for EIAM Host Name, click Update.
6. Start the CA APM Configurator and open CA APM Web Services.
7. In CA APM Web Services, under Option 3, Choose Your Security Type, select EIAM with Single DB Login.
8. Enter the host name of the computer on which CA EEM is installed for EIAM Host Name, click Update.
9. Exit from CA APM Configurator.
10. Reset Microsoft Internet Information Server (IIS) by opening the Windows command prompt window and entering iisreset.
11. Restart the following Windows services:
    - UAPM Cache Service
    - UAPM Tomcat Service
    - CA Catalog Component

Step 4 - Update CA APM Web Services in CA Service Catalog Configuration

Update the CA APM Web Services in CA Service Catalog Configuration.

Follow these steps:

1. Log in to CA Service Catalog as a user with the Service Delivery Administrator role.
2. Click **Administration**, **Configuration**, **CA APM Web Services**.

3. Click on Modify icon for **Host Name** property and update CA APM Application Server Host Name.

4. Click on Modify icon for **Port Number** property and update CA APM Web Services Port Number.

5. Save these configurations.

6. Restart CA Service Catalog Service.

Step 5 - (Optional) Create New Rules and Actions

You may need to create new rule actions in CA Service Catalog to enable the integration with CA Asset Portfolio Management. As supplied, CA Service Catalog rules and actions can have only limited changes made by users. However, you can create new rules and actions, if required. For maximum efficiency, create new rules and actions by copying and modifying existing rules and actions. These steps illustrate how to copy and modify a predefined rule and its actions. You can optionally use these steps as a model to copy and modify other predefined rules and their actions.

Follow these steps:

1. Log in to CA Service Catalog as a user with the Service Delivery Administrator role.

2. Click **Administration**, **Events-Rules-Actions**.

3. Click the **Request/Subscription Item Change** event.

4. Click the Copy icon for the rule that you want to copy and modify, for example, the rule named **When Category is Hardware and Status is Pending Fulfillment**. The Copy icon apears in the icon columns next to the Description field.
   A dialog appears prompting you to enter the name of the new rule.

5. Enter the new name and click **OK**.
   You return to the Event Type Details page. The new rule is added to the list of rules for the event.

6. Click the Edit icon to edit the details of the rule, for example, its name, description, status, or event type.
   The Edit Rule page appears.

   a. Select Enabled in the Status drop-down list.
      The new rule is enabled. You must enable the new rule to activate it, because new rules are disabled by default.

   b. Update the remaining fields, as needed, to meet your requirements.

   c. Click OK.

   You return to the Event Type Details page.

7. Click the new rule to open it.
   The Rule Details and Actions page opens.
   The rule details that you modified earlier appear in read-only format.
   The actions for the rule also appear, so that you can view and modify them as needed: Actions that were enabled in the old rule are enabled in the new rule. Similarly, actions that were disabled in the old rule are disabled in the new rule.

8. (Optional) Add, edit, or copy the action.

9. When you are finished modifying actions, click Done to close the rule.
   You return to the Event Type Details page.

10. Locate the original rule that you copied and click the Disable button; this button appears on the Rules bar.
    The rule is disabled. Disabling the original rule is important to help prevent duplicate rules and actions from being triggered.

Step 6 - Create a Service and Request

A required task of integrating CA Asset Portfolio Management and CA Service Catalog is creating at least one service and request that use the features enabled by the integration.

Follow these steps:

1. Define a Service using a service option group
   As part of defining the service option group, do the following from the Options tab of the service option element:

   a. Ensure that Track As An Asset is checked.

   b. Specify the same category for the service option element as you specified in the rule condition associated with the service.
      For example, if you created a new rule and action (see page 3474) using the Hardware category, then you *must* create your service option group elements as Hardware Category. For more information about how to create service option groups, see the section Service Option Groups.

2. Log out of CA Service Catalog.

3. Log on to CA Service Catalog as the Catalog User created earlier.

4. Submit a request using the service that you defined earlier. The request will proceed through its life cycle.

5. Log out of CA Service Catalog.

6. Log on to CA Service Catalog as the Request Manager (Approver for the End User) that you created earlier.

7. Approve the request in the Pending Actions queue.

8. Log out of CA Service Catalog.

9. Log on to CA Service Catalog as the Service Delivery Administrator (Fulfiller) that you created in an earlier step.

10. To fulfill the request that you submitted in an earlier step, do the following:

    - Become familiar with the Assign Assets window.
    - Assign an Available Asset to a Requested Service Option.

Note: For more information about fulfilling requests, see the section Request Management from an Administrator Perspective (see page 2115).

Step 7 - Configure for Single Sign-On

You can optionally bypass user login by configuring CA Service Catalog and the CA products with which it integrates to use Single Sign-On.

To configure CA Asset Portfolio Management to use Single Sign-On, see Maintaining Security (see page 1570).

Similarly, to configure CA Service Catalog to use Single Sign-On, configure it to use either CA SiteMinder (see page 3425) or NTLM authentication on Windows.

Verify the CA Asset Portfolio Management - CA Service Catalog Integration

This article contains the following topics:

When you are viewing the Fulfill Request or Edit Request window (and the request is past the approval phase of its life cycle), you may see the Assigned Assets gold brick icon in the Actions column for a requested service option. The gold brick icon indicates this service option is eligible to have one or more assets assigned to it from available inventory.

To search available inventory, click the Assigned Assets gold brick icon. The CA APM Assign Assets window appears. By default, the Assigned Assets action is selected so the list of assets already assigned to the requested service option appears.

Using the Assign Assets window, you can do the following:

- View the list of assets assigned to the requested service option by selecting Assigned Assets in the Actions list

- Search for and assign assets to the requested service option
- Indicate that an available asset could not be found in inventory
- Display assigned assets and remove the assignment

Associate a CA APM Model with a Service Option

This information is available during workflow-driven fulfillment and can be useful if CA APM assets are automatically created or assigned to the request.

Follow these steps:

1. Click Catalog, Service Offerings.
2. Click the Option Groups tab.
3. Select any service option group and click the Definition tab.
4. Click the CA APM Model icon.
5. Click Assign Models to display the UAPM Model Assignments window and perform the following actions:
   - **View Assigned Models**
     Select Assigned Models from the Action list.
   - **Assign Models**
     Select Assign from the Action list. You can search for both active and inactive CA APM models that match the criteria you enter and check the ones you want to assign to the service option. Click Assign Models to save the assignment.

     Note: To search for both active and inactive CA APM models, before running the search, do not select the option to include only active records.
   - **Remove Assigned Models**
     Select View Assigned Models from the Action list. Check the models you want to remove from the Assigned Models list and click Remove Assignment.
6. Click Go.
   The Assign Models window is closed.

Assign an Available Asset to a Service Option for Software

Use the Search for Assets section of the Assign Assets window to search for available assets and assign one or more of them to the requested service option for software. Doing so is required to fulfill a service option for software.

Follow these steps:

1. Select an asset in the Search Results List to assign to the requested service option.
   The Asset window appears for the selected asset.

2. Navigate to the Entitlements for the Software asset and select an entitlement to assign or create a new entitlement.

3. Click the Assign and Save button.
   The Asset page refreshes and displays a confirmation message.

4. Click the Refresh button on the CA Service Catalog Fulfill Request window.
   The service option status is changed.

Note: Do not change the status manually. After the Assign Assets window changes the status of the requested service option, you may no longer be assigned a fulfillment task for that service option. Therefore, you may no longer permitted to change its status.

Assign an Available Asset to a Service Option for Hardware

Use the Search for Assets section of the Assign Assets window to search for available assets and assign one or more of them to the requested service option for hardware. Doing so is required to fulfill a service option for hardware.

Follow these steps:

1. Select an asset in the Search Results List to assign to the requested service option.
   The Asset window appears for the selected asset.

2. Click the Assign button.
   The Asset page refreshes and displays a confirmation message.

3. Click the Refresh button on the CA Service Catalog Fulfill Request window.
   The service option status is changed.

Note: Do not change the status manually. After the Assign Assets window changes the status of the requested service option, you may no longer be assigned a fulfillment task for that service option. Therefore, you may no longer permitted to change its status.

Mark a Requested Service Option as Not Filled From Inventory

If you have used the Assign Assets window to search the available asset inventory and have been unable to find an eligible asset, you can indicate that the requested service option could not be filled from inventory.

Follow these steps:

1. Click the Not Assigned From Inventory button.
   The status of the requested service option is automatically changed to Not Filled From Inventory.

   Note: You must have conducted an asset search for the Not Assigned From Inventory button to appear.

2. Click the Refresh button on the CA Service Catalog Fulfill Request window.
   The service option status is changed.

   Note: Do not change the status yourself since once the Assign Assets window changes the status of the requested service option you may no longer be assigned a fulfillment task for that service option and therefore no longer permitted to change its status.

Remove Asset Assignment

If an asset has been incorrectly assigned to a requested service option, you can remove the incorrect assignment. Click Remove Assignment from the Actions drop down list on the Assign Assets window. The list of assigned assets is displayed.

To remove the assignment for one or more non-Software assets assigned to the requested service option:

1. Select the check box for each asset in the Search Results List for which assignment is to be removed for the requested service option.

2. Complete the Asset Information section of the Assign Assets window.
   The assets for which assignment is to be removed are updated with the specified information.

   Note: If a field is left blank, the associated field on the assigned assets is set to blank. For more information on the meaning of the asset-related fields, see the CA APM documentation.

3. Click the Remove Assignment button.
   The Remove Assignment list of assigned assets is displayed. The status of the requested service option is not affected by a remove assignment.

To remove the assignment for a Software asset assigned to the requested service option

1. Select an asset in the Search Results List for which assignment is to be removed for the requested service option.
   The Asset window is displayed for the selected asset.

2. Navigate to the Entitlements for the Software asset and select an entitlement for which to remove the assignment.

3. Click the Remove Assignment and Save button.
   The asset is removed from the list of assigned assets. The status of the requested service option is not affected by a remove assignment.

How Assets Are Filtered During Fulfillment

By default, when a request reaches fulfillment, CA APM filters assets *only* according to models associated with service options.

You can optionally replace the default filtering with advanced filtering by issuing the equivalent custom query at the database console.

Example

For example, consider the following query:

```
update usm_configuration
set value =
'model=$model_ids$&loc=$loc_id$&org=$org_id$&dept=$dept_id$&ccenter=$costcenter$&tenan
t=$tenant_id$'
name = 'asset_fulfillment_url_params'
```

This query filter assets according to the following criteria:

1. Models: Associated to service option

2. Location: Location of the user

3. Organization: Organization of the user

4. Department: Department of the user

5. Cost Center: Cost Center of the user

6. Tenant: BU of the user

Integrate with Common Components Manually

This article contains the following topics:

- Integrate with CA Process Automation Integration for a Data Importer Process Manually (see page 3487)
- Integrate with CA Process Automation Integration for a Notification Process Manually (see page 3489)

Integrate CA Asset Portfolio Management with CA EEM Manually

Important! Review the following section only if you want to manually integrate CA Asset Portfolio Management with CA EEM when the automatic integration between the two has failed.

Execute the following commands in the computer where CA EEM is installed.

1. Log in to the product and navigate to Administration, System Configuration, EEM.
2. Enter in the EEM Backend field the name of the server where CA EEM is installed. On the server where CA EEM is installed, register CA APM with CA EEM using the following steps:
   a. From the Start menu, select Run and open a command prompt (cmd) window.
   b. In the command prompt window, change the directory to the folder safex_12.51.2.11_win32.
   This folder can be found in the following path:
   [ITAM Root Path]\ITAM\InstallConfig\AlleghenyInstallFiles\EEMSetup\

   Note: If this folder is not available, copy the EEMSetup folder from the server where CA APM is installed (using the same folder path).

   c. Execute the following command:

   ```
   safex.exe -h localhost -u EiamAdmin -p [EEM login password] -f
   "[ITAM Root Path]\ITAM\InstallConfig\AlleghenyInstallFiles\EEMSetu

   EEM_CASCM_APP_CREATION.xml"
   ```

   Note: Replace [EEM login password] and [ITAM Root Path] with the actual values.

3. On the server where CA EEM is installed, create a certificate user using the following steps:
   a. From the Start menu, select Run and open a command prompt (cmd) window.

b. In the command prompt window, change the directory to the folder safex_12.51.2.11 _win32.

   This folder can be found in the following path:

   [ITAM Root Path]
   \ITAM\InstallConfig\AlleghenyInstallFiles\EEMSetup\EEMCertutilities\

   Note: If this folder is not available, copy the EEMSetup folder from the server where CA APM is installed (using the same folder path).

   This folder contains the CA.Common.Data.dll configuration file.

c. In the CA.Common.Data.dll configuration file, specify the database details.

d. Execute the following command:

```
EEMCertUtilities.exe localhost APM eiamadmin [EEM login password]
uapmadmin
```

Integrate CA Asset Portfolio Management with CA Business Intelligence Manually

Important! Review the following section only if you want to manually integrate CA Asset Portfolio Management with CA Business Intelligence when the automatic integration between the two has failed. If you have any other earlier version of CA Business Intelligence, install CA Business Intelligence 4.1 SP3 and migrate the data from your earlier version (see page 285) for the reports to work.

The article contains the following topics:

CA Business Intelligence is a set of reporting and analytic software that several CA products use to present information and support business decisions. CA products use CA Business Intelligence to integrate, analyze, and present vital information that is required for effective enterprise IT management.

CA Business Intelligence installs SAP BusinessObjects Enterprise as a stand-alone product that provides a complete suite of information management, reporting, query, and analysis tools. The installation operates independently of any CA product, allowing the products to share CA Business Intelligence services.

CA products leverage an extensive set of business intelligence capabilities, including reporting, query, and analysis, using BusinessObjects Enterprise technology. CA Asset Portfolio Management provides predefined BusinessObjects Enterprise reports. For more information about the predefined reports, see Reports (see page 2428). CA Business Intelligence provides users with additional configurable reporting capabilities.

Important! Install CA Business Intelligence before you install CA Asset Portfolio Management.

Integrate CA APM and CA Business Intelligence

CA APM supplies the required data to get started with BusinessObjects Enterprise reports. After you install BusinessObjects Enterprise and CA APM, you perform required setup tasks before using reports. To integrate CA APM with BusinessObjects Enterprise, complete the following steps:

1. Follow these best practices when maintaining and using CA Business Intelligence:
   - Install and maintain one universe per CA product.
   - Do *not* modify the default universe. Instead, copy it and modify the copy. Otherwise, your changes can be erased when you apply service packs, patches, and other updates. Back up all your changes and then apply the patches to your customized universe.
   - Reports:
     - Verify that the services in Central Configuration Manager (CCM) is running, when the reports stop running.
     - Do not overwrite predefined reports.
     - Always use a predefined report as a base to build a custom report and maintain consistent formatting in all reports.
     - Administrators *can modify all the reports and can create* new reports that are based on the existing universe. However, administrators must not add any reports to the existing folders.
     - Both administrators and end users *must not* change pre-defined reports. Any changes to those reports are applied to all other users using the same CA Business Intelligence instance. Instead, both administrators and end users must create their own custom folders, copy the reports there, rename them, and customize them.
     - Both administrators and end users must add new reports that they create to their custom folders.
2. Become familiar with BusinessObjects Enterprise, including the documentation, so that you can administer and use the product. You must be able to perform at least the following functions:

- Install CA Business Intelligence, which installs BusinessObjects Enterprise.
- Use predefined reports in BusinessObjects Enterprise.

3. Install CA Business Intelligence BusinessObjects Enterprise. Make a note of the following login credentials and connection information, that is required during the CA Asset Portfolio Management installation:
   - BusinessObjects Enterprise administrator ID
   - BusinessObjects Enterprise administrator password
   - BusinessObjects Enterprise Central Management Server (CMS) port. The CMS maintains a database of information about your BusinessObjects that you use with CA Business Intelligence. The default CMS port is 6400.
   - CA Business Intelligence Server Name
4. If you use MS SQL as the MDB, make sure you install Microsoft SQL Server Native Client (64-bit) on the server where CA Business Intelligence is installed.
5. If you use Oracle as the MDB, define an Oracle Net Service Name (64-bit) on the server where CA Business Intelligence is installed. Make a note of the NSN, which you are asked to enter during the CA Asset Portfolio Management installation.
6. Verify that BusinessObjects Enterprise is installed by logging into BI launch pad.
7. Install CA Asset Portfolio Management by using the CA Service Management Installer.
   a. Go to the CA Service Management Install path and locate the \filestore\BOXI\biconfig folder.
   b. Copy the contents of the biconfig folder on to the CA Business Intelligence computer.
   c. Create an XML file (with the contents of Example XML File (see page 3486)) and update this file, according to your requirements.

      Set the following parameters in your XML file:
      - Networklayer: OLE DB
      - RDBMS:
        - For Microsoft SQL Server: MS SQL Server 2008 or MS SQL Server 2012
        - For Oracle: Oracle Client
      - User name and password parameters for your database
        - For SQL Server: Use *sa* for the user name
        - For Oracle: Use *mdbadmin* for the user name

Note: These users have access to all required tables in the MDB.

- Path name of the CA_ITAM_Reporting.biar file on the CA Business Intelligence computer
- (For MS SQL Server only) Name of the database. For example, MDB
- (For Oracle only) Name of the NSN created previously in the data source parameters
- Server parameter: Computer name of your Oracle or SQL Server server

d. Open a Windows command prompt and navigate to the biconfig folder on the CA Business Intelligence computer and enter the following command:

```
biconfig -h "host" [-n "port"] -u "user" [-p "password"] -f "XML-c
```

The quotation marks (" ") *are* required as shown in the command. However, the brackets [ ] are *not* required; the brackets signify optional parameters.
The following parameters are required, unless noted otherwise.

- **host**
  Specifies the CA Business Intelligence Central Management Server (CMS) host.
- **port**
  (Optional) Specifies the CA Business Intelligence CMS port. The default is 6400.
- **user**
  Specifies the CA Business Intelligence CMS user.
- **password**
  Optional. Specifies the CA Business Intelligence CMS password.
- **XML-config-file-name**
  Specifies the path name of the XML file you modified.
  If the file resides in the biconfig folder, you can specify the file name only. Otherwise, specify the complete path name.
- **help**
  Optional. Displays the help for the biconfig utility.
  Enter *two* dashes to display the help.

Note: For more information about using biconfig, see the biconfig-readme.txt file in the biconfig folder.

e. Verify the Import as follows:

i. Review the biconfig.log file in the biconfig folder.
This file lists the status of the import. This file also includes error messages if the BIAR file is not imported successfully. A return code of zero (0) indicates a successful import.

ii. Log in to BI launch pad as a CA Business Intelligence administrator.

iii. Verify that you can view the CA Asset Portfolio Management Reports under Public Folders/CA Reports/CA Service Management/CA Asset Portfolio Management.

f. Specify a password for the uapadmin user in CA Business Intelligence. This password is empty by default.

8. Become familiar with and use the predefined reports. For more information about the predefined CA Asset Portfolio Management reports, see Reports (see page 2428).

Example XML File to Import BIAR

```
<?xml version="1.0"?>
<biconfig version="1.0">
<!-- Import BIAR file -->
<step priority="1">
<add>
<biar-file name="Specify path of CA_ITAM_Reporting.biar file on the CA Business
Intelligence computer">
<networklayer>OLE DB</networklayer>
<rdbms> <Specify the name of your RDBMS> </rdbms>
<username> <Specify sa (SQL Server) and mdbadmin (Oracle)> </username>
<password> <Specify the sa password or mdbadmin password> </password>
<datasource> <Database name (SQL Server) or NSN name created in data source
parameters (Oracle)> </datasource>
<server><Specify the Database Server name></server>
</biar-file>
</add>
</step>
<step priority="2">
<add-if-missing>
<user name="uapadmin">
<password mode="normal"><Specify the password for uapadmin user in CA Business
Intelligence></password>
<description>ITAM Admin User</description>
<password-expiry>false</password-expiry>
<can-change-password>true</can-change-password>
<change-password-on-next-logon>false</change-password-on-next-logon>
</user>
</add-if-missing>
</step>
<step priority="3">
<add-if-missing><membership>
<group>CA ITAM Administrators</group>
<user>uapadmin</user>
</membership>
</add-if-missing>
</step>
</biconfig>
```

Report Configurations and Product Updates

When you install updates to CA APM, the update process overwrites the existing product components. The update process may, in some cases, overwrite the reporting components. As a result, any reporting configurations you previously made may be lost. However, CA Technologies

provides you with a method to retain your report configurations when you apply CA Asset Portfolio Management updates. Follow the instructions in a CA Technologies-provided white paper, which you can open from http://ca.com/support.

Under Technical Support, navigate to the product page for CA Asset Portfolio Management. Search the Recommended Reading list for *White Paper: Reporting Components Upgrade and Version Control to Retain Customizations*. You can safeguard your report configurations by implementing the strategy that is outlined in the white paper.

Note: See CA Business Intelligence (https://docops.ca.com/display/CABI41SP3/CA+Business+Intelligence+Home) for information about configuring reports.

Integrate with CA Process Automation Integration for a Data Importer Process Manually

The article contains the following topics:

CA APM and CA Process Automation integrate to let you set up and configure a Data Importer process. This integration uses a sample data import XML file that you import into CA Process Automation and integrate with an overall process workflow. The Data Importer process launches the Data Importer and executes a data import.

Note: This integration uses CA Process Automation and a sample data import XML file that is company-provided. You can also use any other workflow provider to create your own overall workflow and Data Importer process.

How to Set Up the CA Process Automation Data Importer Process

Use the following steps to set up the Data Importer process:

1. Install CA APM and CA Process Automation.
2. Log in to the application server where you installed CA APM.
3. Access the following folder on the CA APM application server where the Storage Manager Service is installed.

   ```
   [ITAM Root Path]\Storage\Common Store\Import
   ```

4. Locate the Import_Automation_Workflow.xml file.
5. In CA Process Automation, import the Import_Automation_Workflow.xml file.

6. In CA Process Automation, integrate the Import_Automation_Workflow.xml into your overall process workflow.

7. In CA Process Automation, modify the settings for the Data Importer process parameters.

    a. Change the default Import Service URL to match your required setting.

    b. Change the default CA APM user ID and password to your own settings.

    c. Change the default data import name to match your data import.

    d. Specify the data file name that corresponds to your data import.

> **Note:** For information about using CA Process Automation, see the CA Process Automation documentation.

Modify CA Process Automation Workflow Process Parameters

After you install CA APM and CA Process Automation and import the Import_Automation_Workflow.xml file into CA Process Automation, the default workflow process parameters are defined in CA Process Automation. You can modify the default process parameters to include your required settings. You provide actual (hard-coded) values for the process parameters. You must verify that the values you enter are valid.

You can modify the process parameters in the main data set or in the individual process start request forms. The parameters that you specify for an individual process override the parameters in the main data set for that process.

Follow these steps:

> **Important!** CA APM and CA Process Automation do not validate the information that you enter for the parameters. You must verify that your input is valid and that you entered the data in the correct format.

1. Log in to CA Process Automation and navigate to the CA Process Automation client.

2. Enter the information for the Data Importer parameters. The following fields require explanation:

    - **ITAMImportServiceURL**
      Specifies the complete URL path where the Import Service is running.
      Example:

      ```
      http://server/ImportService/ImportService.svc
      ```

- **username**
  Specifies the CA APM user ID.

- **password**
  Specifies the CA APM user password.

- **Importname**
  Specifies the name of the data import that you want to execute.

- **FilePath**
  Specifies the complete path and name of the data file that is associated with your data import.
  Example:

```
C:\\CAITAMCostcenter.csv
```

3. Save the changes in CA Process Automation.

Note: For information about setting up a process in CA Process Automation, see your CA Process Automation documentation.

Integrate with CA Process Automation Integration for a Notification Process Manually

This article contains the following topics:

CA APM and CA Process Automation integrate to let you set up and configure a notification process that delivers notifications to specific recipients after a defined event occurs. CA APM provides email notification processes with the product. These processes are delivered in files that are included on the product installation media. You import the files into CA Process Automation and specify process parameters in CA Process Automation and CA APM.

How to Set Up the CA Process Automation Notification Process

Use the following steps to set up the email notification processes that are provided with CA APM.

1. Install CA APM and CA Process Automation.

2. In CA Process Automation, import the workflow provider notification process files (see page 3490).

3. In CA Process Automation, configure the mail server (see page).

4. In CA Process Automation, modify the settings for the workflow process parameters (see page).

    a. Change the default email address for the administrator (Admin_Email_To parameter) to specify your required setting.

    b. Change the default CA APM URL (ITAM_URL parameter) to specify your required setting.

    c. Change the default CA Process Automation URL (ITPAM_URL parameter) to specify your required setting.

    d. (Optional) Change any of the other parameters for which you want to specify your required settings.

5. In CA APM and CA EEM, permit CA APM users to use CA Process Automation (see page).

6. In CA EEM, create CA Process Automation user accounts for any non-CA APM users.

7. In CA APM, specify the workflow process parameters when you define an event.

> **Note:** For information about defining an event in CA APM, see Events and Notifications (see page 2376). For information about using CA Process Automation and CA EEM, see the CA Process Automation and CA EEM documentation (https://wiki.ca.com/display/eem1251/CA+Embedded+Entitlements+Manager+-+Source+Home).

Import the Workflow Provider Notification Process Files

CA APM provides default email notification process files. You import these files into CA Process Automation before you can set up and can configure email notifications in the products.

> **Note:** For more information about importing and working with the files, see the CA Process Automation documentation.

Follow these steps:

1. Log in to CA Process Automation as the administrator.

2. Navigate to the CA Process Automation client.

3. Locate the ITAM.xml file on the CA APM installation media using the following path:

    ```
    CD1\SetupFiles\ITPAM\
    ```

4. Import the ITAM.xml file into the **/** node.

Note: In CA Process Automation Release 3.1, you import the XML file from the client. In Release 4.0 SP1, you import the XML file from the Library tab.

Select the import options to set the imported versions as current and to make the imported custom operators and sensors available.
The notification process files are imported into the default /ITAM folder.

Configure the CA Process Automation Mail Server

To implement email notifications between CA Process Automation and CA APM, configure the mail server for CA Process Automation.

1. Log in to CA Process Automation as the administrator.
2. Navigate to the CA Process Automation client.
3. Navigate to the library browser.
4. Locate and lock the default environment.
5. Locate the alert module and clear the inherit check box.
6. Specify the SMTP (mail) server.
   Example: mail.company.com
7. Specify the From address.
   Example: admin@company2.com
8. Save the changes.
9. Unlock the default environment.
   The changes require a few minutes to take effect.

Note: You can send an email notification to an external email address if your SMTP (mail) server settings permit email delivery to the external address. Check your mail server settings to verify if you can send email to external addresses.

Modify CA Process Automation Workflow Process Parameters

After you install CA APM and CA Process Automation and import the notification process files into CA Process Automation, the default workflow process parameters are defined in CA Process Automation. You can modify the default process parameters to include your required settings. You provide actual (hard-coded) values for the process parameters. You must verify that the values you enter are valid.

You can modify the notification process parameters in the data set that applies to all notification processes or in the individual process start request forms. The parameters you specify for an individual process override the parameters in the main data set for that process.

Note: You specify some of the notification process parameters for the workflow provider when you define an event in CA APM. For more information about specifying process parameters in CA APM, see Workflow Provider Process Parameters (see page 2393).

To modify CA Process Automation workflow process parameters

Important! CA APM and CA Process Automation do not validate the information that you enter for the parameters. You must verify that your input is valid and that you entered the data in the correct format.

1. Log in to CA Process Automation and navigate to the CA Process Automation client.
2. In the ITAM folder, locate the data set that is named Dataset.
3. Enter the information for the parameters.
   The following fields require explanation:
   - **Ack_Interaction_Form_Full_Path**
     Full path to the file that contains the acknowledgment interaction form in CA Process Automation. The email notification recipient uses this form to acknowledge receipt of the notification. Each workflow process must have a unique user interaction form and a unique path to the form. You can find the acknowledgment interaction form files that are provided with the product in the folder that contains the processes and main data set (/ITAM or the folder where you imported the processes).
   - **Admin_Email_CC**
     Email address of the copy recipients for the email that is sent to the administrator when a notification error occurs.
   - **Admin_Email_To**
     Email address of the administrator for the email that is sent when a notification error occurs. Change the default value to your required setting.
   - **Log_Folder_Path**
     Full path of the error log file that is created when an error occurs with the notification process. If you do not specify a path, the log file uses the default CA Process Automation log file path.
   - **ITAM_Username**
     User name to log in to CA APM. CA Process Automation requires access to CA APM for information about notification recipients and escalation.

- **ITAM_Password**
  User password to log in to CA APM. CA Process Automation requires access to CA APM for information about notification recipients and escalation.

- **Admin_Email_Subject**
  Subject for the email that is sent to the administrator when a notification error occurs. This parameter can be set in the main data set or in the individual process start request form.

- **Admin_Email_Header**
  Header or introduction for the email that is sent to the administrator when a notification error occurs (for example, "Hello"). This parameter can be set in the main data set or in the individual process start request form.

- **Admin_Email_Footer**
  Signature for the email that is sent to the administrator when a notification error occurs (for example, "Thank You"). This parameter can be set in the main data set or in the individual process start request form.

- **Log_File_Name**
  Name of the error log file that is created when an error occurs with the notification process. The email that is sent to the administrator when a notification error occurs contains the log file name. If you do not specify a name, the log file uses the following default CA Process Automation log file name:

  ```
  process name_process instance number.log
  ```

- **ITAM_URL**
  CA APM URL that CA Process Automation uses to access CA APM for information about notification recipients and escalation. Change the default value to your required setting.
  Example:

  ```
  http://ITAMAPPSERVER:99/ITAMService/Service.asmx
  ```

- **ITPAM_URL**
  CA Process Automation URL that is included in the email notification message. Change the default value to your required setting.
  Example:

  ```
  http://PAMSERVER:8080/itpam
  ```

4. Save the changes in CA Process Automation.

Note: For information about setting up a notification process, see your workflow provider documentation.

Permit CA APM Users to Use CA Process Automation

The CA APM users who receive notifications need to access CA Process Automation to acknowledge the notifications. These users need to have permission to use CA Process Automation. You permit users to use CA Process Automation by performing steps in CA APM first and then in CA EEM. In CA APM you define and authorize users to log in to and use CA APM. In CA EEM, you permit the authorized CA APM users to use CA Process Automation.

To permit CA APM users to use CA Process Automation

1. Log in to CA APM.
2. Verify that both new users and existing users are authorized to log in to and use CA APM.

   Note: For information about defining and authorizing new users and authorizing existing users in CA APM, see Maintaining Security (see page 1570).

   The product defines and authorizes the CA APM users. CA EEM now includes the CA APM users in the list of available users.
3. Log in to CA EEM, selecting CA Process Automation from the application drop-down list.

   Important! You must select the CA Process Automation application when you log in to CA EEM to permit CA APM users to use CA Process Automation.
4. Select a CA APM user from the list of all users and click the application user details for the user.
5. Select a CA Process Automation user group for the user and save the selection.

   Note: For information about using CA EEM to add applications to user details, see this topic (https://wiki.ca.com/display/eem1251/Users) in the CA EEM documentation.

   The CA APM user can now access and use CA Process Automation.

Required Indicators and Multiple Line Text Fields for Parameters

The default notification processes that are delivered with the product contain the parameters that appear on the product Event Definition user interface and the parameters that you specify in the workflow provider. The default processes also contain XML formatting that lets you display a

required indicator and a multiple line text field on the product user interface. These items are not readily available from the workflow provider, and so they are specified in the process. In the CA Process Automation start request form for each default process, the following XML statement appears before the Description of each user interface parameter:

```
<FieldDescriptor><IsRequired>true_or_false</IsRequired><Length>number</Length><
/FieldDescriptor>
```

- **IsRequired**
  Specifies if the parameter is required (true) or not required (false). If the parameter is required, the product displays the standard required indicator on the user interface.
  Example: <FieldDescriptor><IsRequired>true</IsRequired></FieldDescriptor>

- **Length**
  Specifies the length of the parameter text entry field. To define a multiple line text field, specify a value greater than 255.
  Example: <FieldDescriptor><Length>275</Length></FieldDescriptor>

You can change the default notification processes that are delivered with the product, and you can also create your own new notification process. To include information about the required indicator and field length in your changed or new process, you must insert the XML statement before the Description of each user interface parameter in your process.

Note: If you are creating a new notification process, you must have a corresponding start request form for the process. For information about changing or creating notification processes, see your workflow provider documentation.

Reference

This section contains the following articles:

CA Service Desk Manager Reference Commands

This section contains CA Service Desk Manager reference commands.

Data Element Dictionary

This article contains the following topics:

Explains the definitions for the tables in the CA SDM database. The tables are found in schema (.sch) files. See the ddict.sch file in the $NX_ROOT/site directory (UNIX) or *installation-directory*\site directory (Windows) for the most current list of all database tables for your specific installation.

Important! Although several of the tables in this section are obsolete, for backward compatibility, or reserved for future use, it is important that you not delete these -- or any other table -- from the database schema. You can add new tables and add new fields /columns to the existing tables, but never delete any of the tables. Many applications access the mdb database, so deleting or modifying existing fields or tables could cause some applications to not function properly. Ensure that you follow supported schema modification best practices by using the Web Screen Painter.

admin_tree Table

Program control table used by CA SDM applications.

- **SQL Name** -- admin_tree
- **Object** -- ADMIN_TREE

Field	Data Type	Reference	Remarks
caption	STRING 50		
description	STRING 255		Specifies the textual description of this tree entry.
has_children	INTEGER		
id	INTEGER KEY		Unique (to the table) Numeric ID
kt_admin	INTEGER		
kt_ks_caption	STRING 50		
kt_ks_flag	INTEGER		
kt_manager	INTEGER		
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
parent_id	SREL		
resource	STRING 255		
sd_admin	INTEGER		

Animator Table

Program control table used by CA SDM applications

- **SQL Name** -- anima
- **Object** -- ANI

Field	Data Type	Reference	Remarks
a_act	INTEGER		
a_delta	INTEGER		
a_lock	STRING 200		
a_name	STRING 30 S_KEY		
a_org	LOCAL_TIME		
a_string	STRING 30		
a_time	LOCAL_TIME		
id	INTEGER KEY UNIQUE NOT_NULL		Unique (to the table) Numeric ID
t_method	STRING 30 S_KEY		
t_persid	STRING 30 S_KEY		
t_type	INTEGER		

Atomic_Condition Table

These define a single condition.

- **SQL Name** -- atomic_cond
- **Object** -- atomic_cond

Field	Data Type	Reference	Remarks
cond_code	STRING 500		
connecter	INTEGER NOT_NULL		
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
description	STRING 240		Specifies the textual description of this condition.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
l_paran	INTEGER NOT_NULL		
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified
lval	STRING 30 NOT_NULL	Act_Type_Assoc :: code	
operator	INTEGER NOT_NULL		
owning_macro	STRING 30	Spell_Macro::persid	
persid	STRING 30		Persistent ID (SystemObjectName:id)
r_paran	INTEGER NOT_NULL		
rval	STRING 50		
rval_assoc	STRING 30	Act_Type_Assoc :: code	
sequence	INTEGER NOT_NULL		Ordering

Attribute_Name Table

Provides corresponding user name for an object attribute. Default population for the table should set at_name and at_dflt to the same thing. The user sees and is able to modify only the at_name. at_dflt is used to restore the default name. at_desc could be user changeable or not. It is of use for identifying the attribute for an as yet unplanned user maintenance application. at_sys should never be seen by the user, nor should at_obj.

- **SQL Name** -- atn

Field	Data Type	Reference	Remarks
at_desc	STRING 240		Specifies the description of the attribute.
at_dflt	STRING 30		Specifies the default external name.
at_name	STRING 30		Specifies the user name for attribute.
at_obj	STRING 30	S_KEY	Specifies the system object name.
at_sys	STRING 30	S_KEY	Specifies the system name.
del	INTEGER NOT_NULL		Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL	KEY	Unique (to the table) Numeric ID

Audit_Log Table

Contains all audit log entries.

- **SQL Name** -- audit_log
- **Object** -- audlog

Field	Data Type	Reference	Remarks
analyst	Byte 16	ca_contact::uuid	Specifies the user whose update generated this audit record.**Note:** This is a foreign key.
attr_after_val	nvarchar (160)		Specifies the new value of the object's attribute that has changed.
attr_before_val	nvarchar (160)		Indicates the previous value of the object's attribute that has changed.
attr_name	nvarchar (80)		This is the object's attribute that has changed.
aud_opr	INTEGER		Indicates the type of operation that generated this entry, such as, update, insert, and delete.
audobj_name	nvarchar (10)		Used for tracking the object that has changed.
audobj_persid	nvarchar (30)		Used for tracking the object that has changed.
audobj_trkid	nvarchar (40)		Used for tracking the object that has changed.
audobj_uniqueid	nvarchar (30)		Used for tracking the object that has changed.
change_date	INTEGER		The change date value for this Audit_Log.
id	INTEGER		Specifies the unique (to the table) numeric ID.**Note:** This is a primary key.

Field	Data Type	Reference	Remarks
int1_rsrved	INTEGER		Reserved
int2_rsrved	INTEGER		Reserved
persid	nvarchar (30)		This is the Persistent ID (SystemObjectName:id).
str1_rsrved	nvarchar (25)		Reserved for future use by CA.

Behavior_Template Table

Each object includes a list of things to execute based on the state of the object. If no behavior is associated with the state transition then it simply controls whether the object can be transitioned to the state.

- **SQL Name** -- bhvtpl
- **Object** -- bhvtpl

Field	Data Type	Reference	Remarks
context_attrname	STRING 30		Specifies the attribute name, such as "state".
context_attrval	INTEGER		Specifies the attribute value.
context_type	STRING 30 NOT_NULL		Specifies information which determines whether the transition is valid for the consumercontext object. **Note:** For general use, the context_attrnamecontext_attrval pair was added. However, can't get the list of valid values very easily from the GUI so we've added an SREL to the object that context_attrnamecontext_attrval really represents. short name of object (eg. wf)
del	INTEGER NOT_NULL	Active_Boolean_Table:: enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
description	STRING 500		Specifies the textual description of this behavior template
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID

Field	Data Type	Reference	Remarks
last_mod_by	UUID	ca_contact:: uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
macro_condition	STRING 30	Spell_Macro :: persid	Specifies whether the macro executes.
object_id	INTEGER NOT_NULL		Specifies the id of creator object.
object_type	STRING 30 NOT_NULL		Specifies the short name of creator object.
persid	STRING 30		Persistent ID (SystemObjectName:id)
transition_errmsg	STRING 240		Specifies the text to display on failure.
transition_test	STRING 30	Spell_Macro :: persid	Specifies the condition.

Bop_Workshift Table

Workshift definition.

- **SQL Name** -- bpwshft
- **Object** -- wrkshft

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table:: enum	This is the Deleted flag:**0** -- Active**1** -- Inactive /marked as deleted
description	nvarchar (80)		Specifies the textual description of this workshift.
id	INTEGER		Unique (to the table) Numeric ID.
last_mod_by	Byte(16)	ca_contact:: uuid	Specifies the UUID of the contact who last modified this record.

Field	Data Type	Reference	Remarks
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).**Note:** This is a primary key.
sched	nvarchar (1000)		Describes the schedule of this workshift.
sym	nvarchar (30)		Represents the symbolic value for this workshift.

BU_TRANS Table

Program control table used by Knowledge Management.

- **SQL Name** -- BU_TRANS
- **Object** -- BU_TRANS

Field	Data Type	Reference	Remarks
BU_DATE	LOCAL_TIME		
BU_PROCESSED	INTEGER		
BU_RATING	REAL		
DOC_ID	INTEGER	SKELETONS::id	
HIT_NO_VOTE	INTEGER		
HIT_ORIGIN	INTEGER		
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
INDEX_ID	INTEGER	O_INDEXES::id	
User_slv	INTEGER		
Ticket_slv	INTEGER		
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
USER_ID	UUID	ca_contact::uuid	Specifies the UUID of the user id.
kd_duration	INTEGER		Specifies the duration of a specific event, such as how long a knowledge document was open.

Business_Management_Repository Table

Table that keeps track of CA NSM repositories used by Service Analyzer.

- **SQL Name** -- busrep
- **Object** -- bmrep

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
hostname	STRING 64 UNIQUE NOT_NULL		
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
nx_desc	STRING 40		
password	STRING 200		
persid	STRING 30		Persistent ID (SystemObjectName:id)
sym	STRING 60 UNIQUE NOT_NULL S_KEY		
userid	STRING 40		

Column_Name Table

Column Name list used by Web Screen Painter.

- **SQL Name** -- cn

Field	Data Type	Reference	Remarks
cn_desc	STRING 240		description of column
cn_dflt	STRING 30		default external name
cn_name	STRING 30		user name for column
cn_sys	STRING 30 S_KEY		system name
cn_table	STRING 30 S_KEY		system table name
del	INTEGER NOT_NULL		

Field	Data Type	Reference	Remarks
			Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID

Contact_Method Table

Defines contact method types. The cm_template field is a command string that gets executed as a script (with environment variables set) by the notify subsystem.

- **SQL Name** -- ct_mth
- **Object** -- cmth

Field	Data Type	Reference	Remarks
cm_template	nvarchar (240)		Specifies the method template.
del	INTEGER	Active_Boolean_Table::enum	Identifies the Delete flag, as follows:**0** -- Active**1** -- Inactive/marked as deleted)
id	INTEGER		Specifies the primary key of this table, this is also a unique, numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
nx_desc	nvarchar (40)		Specifies the Contact method description.
persid	nvarchar (30)		Specifies the Persistent ID (SystemObjectName:id).
supports_smtp	INTEGER		Determines if the method supports SMTP email addresses.
sym	nvarchar (60)		Identifies the Contact method symbolic name.
write_file	INTEGER		Flag that indicates the following:**1** -- write output to the file

D_PAINTER Table

Tables to be used for Form Server and Screen Painter For the new GUI.

- **SQL Name** -- D_PAINTER

Field	Data Type	Reference	Remarks
CNTLID	INTEGER		id of the control
CNTLTYPE	INTEGER		type of control
DDID	INTEGER		data dictionary id
ENTITYID	INTEGER		entity type
EXTRA_L1	INTEGER		user-definable
EXTRA_L2	INTEGER		user-definable
EXTRA_L3	INTEGER		user-definable
EXTRA_S1	STRING 50		user-definable
EXTRA_S2	STRING 50		user-definable
EXTRA_S3	STRING 50		user-definable
FORMGROUP	STRING 50		group in which the form is contained
FORMID	INTEGER		id number of the form
FORMNAME	STRING 50		name of the form
FORMTYPE	INTEGER		type of form
ID	INTEGER UNIQUE NOT_NULL KEY		key ID
MAPBACK	STRING 30		data dictionary owner
PARENTID	INTEGER		control id of parent control
PREDEFINED	INTEGER		**0** -- Normal screen **2** -- Default screen
PROPLIST	STRING 1000		properties for the control
SECLEVEL	INTEGER		security level
TSTAMP	REAL		time stamp

Delegation_Server Table

List of servers that can be delegated from this one along with xport methods.

- **SQL Name** -- dlgsrvr
- **Object** -- dlgsrvr

Field	Data Type	Reference	Remarks
anon_userid	STRING 8		Specifies the anonymous userid.
appl_addr	STRING 48		Specifies the name or address of application.
default_assignee	UUID	ca_contact::uuid	Specifies the assignee for incoming tickets.
default_userid	STRING 8		Specifies the default userid.

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL	Active_Boolean_ Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
metafile	STRING 256		Specifies the path to conversion metafile def.
nx_desc	STRING 40		Specifies the description.
password	STRING 16		Specifies the server password.
server	STRING 128		Specifies the server name or ip address.
sym	STRING 64 UNIQUE NOT_NULL S_KEY		Specifies the system name.
transport	INTEGER		

Controlled_Table Table

Program control table used by CA SDM applications.

- **SQL Name** -- ctab
- **Object** -- ctab

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_ Table:: enum	Indicates the Deleted flag, as follows:**0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER		Primary key to this table, it is a unique numeric ID.
nx_desc	nvarchar (40)		Specifies the Table description.
obj_name	nvarchar (30)		Specifies the Majic object name that corresponds to this table.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
sym	nvarchar (30)		Represents the symbolic name of this controlled table.

EBR_SUFFIXES Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_SUFFIXES

- **Object** -- EBR_SUFFIXES

Field	Data Type	Reference	Remarks
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
SUFFIX	STRING 50		

Priority Table

List of Priority entries. The priority reflects the time-frame in which a ticket must be resolved. For the ticket, it represents the highest priority of any problem attached to the ticket. Problem priorities are derived from the scope (impact) and severity of the problem.

- **SQL Name** -- pri
- **Object** -- pri

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Deleted flag that indicates the following:**0** -- Active **1** -- Inactive/marked as deleted
enum	INTEGER		Primary key of this table.
id	INTEGER		Specifies the unique (to the table) numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
nx_desc	nvarchar (40)		Describes the priority.
service_type	nvarchar (30)	Service_Desc:: code	Classic Service Type. Foreign key to the code field of the srv_desc table.
sym	nvarchar (12)		Indicates the symbolic name for this priority.

Queued_Notify Table

Notifications that are queued due to workshifts are saved here.

- **SQL Name** -- not_que
- **Object** -- notque

Field	Data Type	Reference	Remarks
cmth_over ride	INTEGER		method over ride
	INTEGER 30		

Field	Data Type	Reference	Remarks
context_instance			Contains the persistent ID of the associated Activity Log for the notifications
context_persid	STRING 30		Contains the persistent ID of object for notification
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
internal	INTEGER		internal notification
msg_ack	STRING 40		message acknowledgment
msg_body	STRING 1000		message text
msg_body_html	STRING 32768		message text
msg_title	STRING 40		Msg header text
notify_level	INTEGER		notification level
persid	STRING 30		Persistent ID (SystemObjectName:id)
transition_pt	INTEGER		transition point

Quick_Template_Types Table

Quick_Template_Types - Reference table for quick template types.

- **SQL Name** -- quick_tpl_types
- **Object** -- quick_tpl_types

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
enum	INTEGER UNIQUE NOT_NULL		Enumerated value for this entry - specifies ordering in lists and relative values
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
nx_desc	STRING 40		Descriptive Info
persid	STRING 30		Persistent ID (SystemObjectName:id)
sym	STRING 30		Symbolic name of level

Remote_Ref Table

Remote References. Used for smart hooks. Determines what command to execute. Different command for UNIX and pc's using the same smart hook. Can apply security to smart hook.

- **SQL Name** -- rem_ref
- **Object** -- rrf

Field	Data Type	Reference	Remarks
description	STRING 500		Specifies the description of the command.
arch_type	STRING 12		Specifies the architecture to exec this on UNIX or PC. If empty, then all.
code	STRING 12 UNIQUE NOT_NULL S_KEY		Specifies the noneditable key for command.
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1 --** Inactive/marked as deleted
exec_str	STRING 500		Specifies the string to execute on UNIX.
function_group	STRING 30		Specifies the function group for security.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
pcexec_str	STRING 500		Specifies the string to execute on pc.
sym	STRING 30 NOT_NULL		Specifies the name of command.

Response Table

Personalized response text used to simplify data entry when using the CA SDM applications.

- **SQL Name** -- response
- **Object** -- response

Field	Data Type	Reference	Remarks
chg_flag	INTEGER S_KEY		
cr_flag	INTEGER S_KEY		
del	INTEGER NOT_NULL		

Field	Data Type	Reference	Remarks
		Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
in_flag	INTEGER S_KEY		
iss_flag	INTEGER S_KEY		
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
persid	STRING 30		Persistent ID (SystemObjectName:id)
pr_flag	INTEGER S_KEY		
response	STRING 1000		response text
response_owner	UUID S_KEY	ca_contact::uuid	response owner
sym	STRING 50 NOT_NULL S_KEY		symbol

Rootcause Table

Reference table to denote the rootcause type used when resolving or closing a request, change order, or issue.

- **SQL Name** -- rootcause
- **Object** -- rc

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag as follows:**0** -- Active**1** -- Inactive/marked as deleted
description	nvarchar(240)		Provides a textual description of this root cause.
id	INTEGER		Primary key of this table.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
persid	nvarchar(30)		Persistent ID (SystemObjectName:id).
sym	nvarchar(60)		Identifies the symbolic value for this Rootcause.

Rpt_Meth Table

Reporting methods used to display information within the CA SDM applications.

- **SQL Name** -- rptmth
- **Object** -- rptm

Field	Data Type	Reference	Remarks
description	STRING 80		Specifies the textual description of this reporting method.
def_pg_len	STRING 80		Specifies the page length default.
default_out	STRING 80		Specifies the output default.
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
is_default	INTEGER		If set, this specifies the default reporting method.
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
script	STRING 1000		
sym	STRING 30 NOT_NULL		

Reporting_Method Table

Reference table to denote how the contact with the customer occurred. Example: email, phone.

- **SQL Name** -- repmeth
- **Object** -- rptmeth

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag as follows:**0** -- Active**1** -- Inactive/marked as deleted
id	INTEGER		Primary key of this table.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.

Field	Data Type	Reference	Remarks
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
sym	nvarchar (60)		Identifies the symbolic value for this Reporting Method.

Note_Board Table

Message board (announcements) on the main menu.

- **SQL Name** -- cnote
- **Object** -- cnote

Field	Data Type	Reference	Remarks
active_flag	INTEGER NOT_NULL	Boolean_Table:: enum	**0** -- Inactive **1** -- Active
close_date	LOCAL_TIME		Indicates when closed
cnote_type	INTEGER		Indicates the announcement type
control_group	UUID		Specifies the group to display to
del	INTEGER		Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
internal	INTEGER		Internal Flag
loc_id	UUID	ca_location:: location_uuid	Indicates a pointer to location
organization	UUID	ca_organization :: organization_ uuid	Indicates a pointer to Organization
persid	STRING 30		Persistent ID (SystemObjectName:id)
posted_by	UUID	ca_contact::uuid	Specifies who posted the announcement
posted_date	LOCAL_TIME		Indicates the last modify time
text	STRING 4000		Indicates the message text

Prob_Category Table

Call Request call areas. Category of the issue that the customer is calling about. Can be hierarchical.

- **SQL Name** -- prob_ctg
- **Object** -- pcat

Field	Data Type	Reference	Remarks
id	INTEGER	UNIQUE NOT_NULL KEY	Unique (to the table) numeric ID.
persid	STRING (30)		Persistent ID (SystemObjectName:id)
del	INTEGER	NOT_NULL	Delete flag that indicates the following: **0** -- Active **1** -- Inactive/marked as deleted
sym	STRING (1000)	NOT_NULL S_KEY	Specifies the symbolic name of the request area.
last_mod_dt	LOCAL_TIME		Identifies the timestamp of when this record was last modified.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
description	STRING (500)		Identifies the textual description of the call area.
organization	UUID	ca_organization	Foreign key to the id field of the ca_organization table, this is the Organization.
assignee	UUID	ca_contact	Foreign key to the contact_uuid field of the ca_contact table, this is the Assignee.
group_id	UUID	ca_contact	Foreign key to the contact_uuid field of the ca_contact table, this is the Group.
tcode	INTEGER		Deprecated
service_type	STRING (30)	Service_Desc	Foreign key to the code field of the srv_desc table, this is the Classic Service Type.
survey	INTEGER	Survey_Template	Foreign key of the id field of the survey_tpl table, this is the Survey.
schedule	INTEGER	Bop_Workshift	Deprecated
auto_assign	INTEGER		Represents the flag that enables auto assignment.

Field	Data Type	Reference	Remarks
owning_contract	INTEGER	Service_Contract	Foreign key to the id field of the svc_contract table.This is the Service Contract.
cr_flag	INTEGER		Represents the cr_flag status. When set to 1, this status is valid for requests.
in_flag	INTEGER		Specifies the Incident flag. When set to 1, the status is valid for Incidents.
pr_flag	INTEGER		Specifies the Problem flag. When set to 1, the status is valid for Problems.
suggest_knowledge	INTEGER		Specifies whether or not to suggest knowledge to users. **1** -- Suggest knowledge. **2** -- Do not suggest knowledge.
assignable_ci_attr	STRING (60)		Identifies the name of the attribute on a CI object that contains the grp contact that should be used to perform Category/CI auto group assignment.
flow_flag	INTEGER		Specifies the type of workflow:**0** -- Classic Workflow or none (default) **2** -- CA IT PAM
caextwf_start_id	INTEGER	caextwf_start_forms	Identifies the CA IT PAM process definition information to use when the user selects this category on a change order, issue, request.
tenant	UUID	ca_contact	
ss_include	INTEGER		Required. On new default: 0
ss_sym	STRING (128)		
category_urgency	INTEGER	Urgency	
sap_prop	INTEGER		

Product Table

Reference table to denote the product that the complaint relates to.

- **SQL Name** -- product
- **Object** -- prod

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Delete flag that indicates the following:**0** -- Active**1** -- Inactive/marked as deleted
id	INTEGER		Primary key of this table.
	byte(16)	ca_contact::uuid	

Field	Data Type	Reference	Remarks
last_mod_by			Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
sym	nvarchar (60)		Specifies the symbolic value for this Product.

sa_agent_availability Table

Program control table used by Support Automation.

- **SQL Name** -- sa_agent_availability
- **Object** -- sa_agent_availability

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
agentID	UUID	ca_contact	NOT_NULL
queueID	INTEGER	sa_queue	NOT_NULL
status	INTEGER		
availEpoch	LOCAL_TIME		
clientSessionID	INTEGER	sa_login_session	
matchEpoch	LOCAL_TIME		
groupID	INTEGER	sa_group	
incidentCount	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

Table_Name Table

Table name list used by CA SDM applications.

- **SQL Name** -- tn

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL		Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
tn_desc	STRING 240		description or table
tn_dflt	STRING 30		default external name
tn_name	STRING 30		user name for table
tn_sys	STRING 30 S_KEY		system name

usp_special_handling Table

The usp_special_handling table defines the characteristics of each special handling classification.

Attribute	Data Type	SREL References	Flags
alert_icon_url	STRING 1000		
alert_text	STRING 60		
autodisplay_notes	INTEGER		
del	INTEGER		NOT_NULL
description	STRING 4000		
escalate_urgency	INTEGER		
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	
last_mod_dt	LOCAL_TIME		
sym	STRING 60		NOT_NULL
tenant	UUID	ca_tenant	

usp_symptom_code Table

The usp_symptom_code table associates codes with a special handling classification.

Attribute	Data Type	SREL References	Flags
del	INTEGER		NOT_NULL
description	STRING 4000		
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	
last_mod_dt	LOCAL_TIME		
sym	STRING 60		NOT NULL
tenant	UUID	ca_tenant	

usp_tab Table

Information on Tabs used in the Role Based UI.

- **SQL Name** -- usp_tab
- **Object** -- tab

Field	Data Type	Reference	Remarks
id	INTEGER		Specifies the unique (to the table) numeric ID.
name	STRING (80)		Tab Name
display_name	STRING (80)		Text displayed on tab
code	STRING 30		Code
del	INTEGER	Active_ Boolean_ Table::enum	
description	STRING (255)		Description
menu_bar_obj	INTEGER	usp_menu_bar::id	Foreign key to the menu bar id field of the usp_menu_bar table.
web_form_obj	INTEGER	web_form::id	Foreign key to the web form id field of the usp_web_form table.

usp_ticket_type Table

The usp_ticket_type table lists the ticket types referenced by Action Object drop-down list (action_object) in the usp_mailbox_rule table.

Field	Data Type	Description
id	INTEGER UNIQUE KEY	Specifies the primary key of this table.
allow_mailbox	INTEGER	
code	STRING 30 UNIQUES_KEY	Specifies the REL_ATTR value of the table, and the distinct keyword for each ticket type that is recognized by some components
del	INTEGER	
sym	STRING 60	Specifies the symbolic value for the ticket type.
ticket_object	STRING 30	Specifies the Majic object for the ticket (cr, chg, or iss).
ticket_object_type	STRING 1	Specifies the Call_Request_Type field (R, I or P) for the cr object.

The following values are the defaults for the usp_ticket_type table:

id	code	sym	ticket_obj	ticket_obj_type
100	REQUEST	Request	cr	R
200	INCIDENT	Incident	cr	I
300	PROBLEM	Problem	cr	P
400	CHANGE	Change	chg	
500	ISSUE	Issue	iss	

usp_web_form Table

Information on Web Forms used in the Role Based UI.

- **SQL Name** -- usp_web_form
- **Object** -- web_form

Field	Data Type	Reference	Remarks
id	INTEGER		Specifies the unique (to the table) numeric ID.
name	STRING (80)		Tab Name
code	STRING 30		Code
del	INTEGER	Active_Boolean_Table::enum	
description	STRING (255)		Description
wf_resource	STRING (1024)		The URL to display the HTMPL form, Report, Go button resource or third party form.
wf_type	INTEGER		The type of the web form: **0** -- HTMPL **1** -- Report **2** -- Go Resource **3** -- Other
dflt_for_obj	STRING 30		For Go Resource type web forms only. Indicates that this Go Resource will override the role's default when displaying objects of this type (such as "Request", "Issue", "Change Order"). Only one Go Resource can be assigned a dflt_for_obj for each type.

usp_attr_control Table

A dependent_control object specifies the attribute name and locked or required value that activates dependent control.

- **SQL Name** -- usp_attr_control
- **Object** -- att_control

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
control	control	INTEGER REF	usp_dependent_control	
attrname	attrname	STRING 64		Identifies attribute name.
locked	locked	INTEGER		Identifies locked attribute.
required	required	INTEGER		Identifies required attribute.
last_mod_dt	last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
last_mod_by	last_mod_by	UUID REF	ca_contact	Specifies the UUID of the contact who last modified this record.
del		INTEGER	nn	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
tenant		UUID REF	ca_tenant	

usp_auto_close Table

The auto close object controls the automatic closure of a ticket (request, incident, problem, change order, issue). The usp_auto_close table lists the automatic closure settings. For each ticket type, you can define the number of business hours before the closure takes place. By definition, zero hours means that automatic closure is not implemented for the ticket type.

In an untenanted system only one active row is allowed in this table.

In a tenanted system, each tenant can have its own row and only one row is permitted. In addition, one active Public row is permitted for tenants that do not have a tenanted row. If a tenant does not have its own row of auto-close settings, and there is not an active Public row, the automatic closure feature is disabled for that tenant.

- **SQL Name** -- usp_auto_close
- **Object** -- auto_close

Label	Field	Description
id	INTEGER	Unique key

Label	Field	Description
sym	STRING 80	
cr_ach	INTEGER	
in_ach	INTEGER	
pr_ach	INTEGER	
chg_ach	INTEGER	
iss_ach	INTEGER	
description	STRING 255	
last_mod_dt	LOCAL_TIME	
last_mod_by	UUID REF	ca_tenant
del	INTEGER	nn
tenant	UUID REF	ca_tenant

usp_ci_window Table

The usp_ci_window table stores the associations between windows and configuration items.

- **SQL Name** -- usp_ci_window
- **Object** -- ci_window

Attribute	Data Type	SREL References
id		
nr_uuid	UUID	nr (object)
Window_id	ID	window (object)
producer_id	STRING	
persistent_id	STRING	
last_mod_by	SREL	cnt.id (http://cnt.id/)
last_mod_dt	DATE	

usp_email_type Table

The usp_email_type table lists the email types that are available for the Email Type drop-down list (email_type) in the usp_mailbox table.

Field	Data Type	Description
id	INTEGER UNIQUE KEY	Specifies the primary key of this table.
code	STRING 30 UNIQUE S_KEY	Specifies the code value for the email type.
del	INTEGER	
incoming	INTEGER	Specifies whether the email type is incoming or outgoing.
sym	STRING 60	Specifies the symbolic value for the email type.

The following values are the defaults for the usp_email_type table:

id	code	incoming	sym
100	NONE	1	NONE
200	IMAP	1	IMAP
300	POP3	1	POP3
400	SMTP	0	SMTP

usp_export_list_format Table

The usp_export_list_format table lists the file format that is used to export list results outside of CA Service Desk Manager.

- **SQL Name** -- usp_export_list_format
- **Object** -- usp_exlist_format

Label	Field	Description
id	INTEGER	Unique (to the table) Numeric ID.
file_extention	STRING	Specifies the active file format to export search list results. Excel (.xls) is currently supported.
mime_type	STRING	Specifies the internet media type.
xslt_name	STRING	Specifies the XSL file name on the server.
sym	STRING	Specifies the export file format.
delete_flag	INTEGER	Delete indicator.

usp_ical_alarm Table

- **SQL Name** -- usp_ical_alarm
- **Object** -- ical_alarm

Field	Data Type	Reference	Remarks
id	**INTEGER**		**Unique key**
del	INTEGER		
alarm_value	STRING 120		
sym	STRING 60		
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID REF	ca_contact	

usp_ical_event_template Table

- **SQL Name** -- usp_ical_event_template
- **Object** -- ical_event_template

Field	Data Type	Reference	
id	INTEGER		Unique key
del	INTEGER		NOT_NULL
obj_type	STRING 30		NOT_NULL
code	STRING 60		NOT_NULL
sym	STRING 60		NOT_NULL
start_date	STRING 30		NOT_NULL
end_date	STRING 30		
alarm	INTEGER	usp_ical_alarm	
categories	STRING 128		
summary	STRING 240		
description	STRING 4000		
url	STRING 4000		
extra_entries	STRING 4000		
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	

usp_owned_resource Table

Holds information about the owned resource.

- **SQL Name** -- usp_owned_resource
- **Object** -- usp_owned_resource

Attribute	DB Field	Data Type	SREL References	Flags
argis_id	nr_argis_id	STRING		
assoc_projex	assoc_projex	BREL	projex.id (http://projex.id/)	
audit_userid	audit_userid	LOCAL SREL	cnt	
assoc_in	assoc_in	QREL	cr	
assoc_pr	assoc_pr	QREL	cr	
bm_rep	nr_bm_rep	INTEGER	busrep id	
bm_label	nr_bmlabel	STRING		
bm_macro_smag	bm_macro_smag			

Attribute	DB Field	Data Type	SREL References	Flags
		LOCAL STRING 0		
bm_status	nr_bms	INTEGER	busstat status_no	
expiration_date	nr_exp_dt	LOCAL_TIME		
financial_num	nr_financial_id	STRING		
nsm_id	nsm_id	STRING 40		
contact_1	nr_nx_ref_1	UUID	ca_contact uuid	
contact_2	nr_nx_ref_2	UUID	ca_contact uuid	
contact_3	nr_nx_ref_3	UUID	ca_contact uuid	
linked_id_usp_ owned_resource	linked_id_usp_ owned_resource	UUID		
smag_1	nr_nx_string1	STRING		
smag_2	nr_nx_string2	STRING		
smag_3	nr_nx_string3	STRING		
smag_4	nr_nx_string4	STRING		
smag_5	nr_nx_string5	STRING		
smag_6	nr_nx_string6	STRING		
priority	nr_pr_id	INTEGER	pri enum	
name_type	nr_prim_skt_id	INTEGER		
service_type	nr_service_type	STRING	srv_desc code	
sla	nr_sla_id	INTEGER		
warranty_end	nr_wrty_end_dt	LOCAL_TIME		
warranty_start	nr_wrty_st_dt	LOCAL_TIME		
id	owned_resource_uuid	UUID		

USP_Preferences Table

Holds information about the CA SDM and Knowledge Management application preferences.

- **SQL Name** -- usp_preferences
- **Object** -- usp_preferences

Field	Data Type	Reference Remarks
ANALYST_ID	UUID	ca_contac t ::uuid
ARC_DOCS_TO_ DISPLAY	INTEGER	
ASSIGNEE	INTEGER	
AUTHOR	INTEGER	

Field	Data Type	Reference	Remarks
BU_RESULT	INTEGER		
CLASSIC_ RESULTSET_ CONTEXT	INTEGER		Specifies the Classic resultset context menu activation.
CREATED_VIA	INTEGER		
CREATION_DATE	INTEGER		Indicates the timestamp indicating when this record was created.
CURRENT_ACTION	INTEGER		
CUSTOM1	INTEGER		
CUSTOM2	INTEGER		
CUSTOM3	INTEGER		
CUSTOM4	INTEGER		
CUSTOM5	INTEGER		
CUSTOM_NUM1	INTEGER		
CUSTOM_NUM2	INTEGER		
DOC_ID	INTEGER		
DOC_TEMPLATE	INTEGER		
DOC_TYPE	INTEGER		
DOC_VERSION	INTEGER		
EXPIRATION_DATE	INTEGER		
GLOBALSD_ ACTIVE_ZONE	INTEGER		Specifies the status of the Global Service Desk Active Zone log reader:**0x01** -- Reduce popups**0x02** -- Close log reader
HITS	INTEGER		
ID	INTEGER NOT_NULL KEY		Specifies the numeric ID that is unique to this table.
INBOX_COUNTER	INTEGER		
INITIATOR	INTEGER		
ITEM	INTEGER		
KT_REPORT_ CARD_PAST_ DAYS	INTEGER		Indicates the Knowledge report card past_days status. This is a user-defined preference.
KT_REPORT_ CARD_SCREEN_ DEFAULT	INTEGER		Indicates the Knowledge report card screen default. this is a user-defined preference.
LAST_ACCEPTED_D ATE	INTEGER		
LAST_MOD_DT	LOCAL_TIM E		Indicates the timestamp for when this record was last modified.
MODIFY_DATE	INTEGER		

Field	Data Type	Reference	Remarks
ONE_B_DOC_ VIEW_MODE	INTEGER		
ONE_B_DOCS_TO_ DISPLAY	INTEGER		
ONE_B_HIDE_ DETAILS	INTEGER		
ONE_B_MATCH_ TYPE	INTEGER		
ONE_B_SEARCH_FI ELDS	INTEGER		
ONE_B_SEARCH_O RDER	STRING 255		
ONE_B_SEARCH_TY PE	INTEGER		
ONE_B_WORD_ PARTS	INTEGER		
OWNER	INTEGER		
PRIMARY_INDEX	INTEGER		
PRIORITY	INTEGER		
PRODUCT	INTEGER		
PUBLISHED_DATE	INTEGER		
REVIEW_DATE	INTEGER		
SD_ACCEPTED_ HITS	INTEGER		
SD_IMPACT	INTEGER		
SD_PRIORITY	INTEGER		
SD_ROOTCAUSE	INTEGER		
SD_SEARCH_ FIELDS_CR	INTEGER		Specifies the CA SDM and Knowledge Management search fields for requests.
SD_SEARCH_ FIELDS_ISS	INTEGER		Specifies the CA SDM and Knowledge Management search fields for issues.
SD_SEVERITY	INTEGER		
SD_URGENCY	INTEGER		
START_DATE	INTEGER		
STATUS	INTEGER		
SUBJECT_EXPERT	INTEGER		
USER_DEF_ID	INTEGER		
WEB_LAST_LOGIN	LOCAL_TIM E		Indicates the time of the last web login.
	INTEGER		Specifies the maximum height for pop-up1.

Field	Data Type	Reference	Remarks
WEB_POPUP1_ HEIGHT			
WEB_POPUP1_ WIDTH	INTEGER		Specifies the maximum width for the Web pop-up1.
WEB_POPUP2_ HEIGHT	INTEGER		Specifies the medium Web pop-up2 height.
WEB_POPUP2_ WIDTH	INTEGER		Specifies the Medium Web pop-up2 width.
WEB_POPUP3_ HEIGHT	INTEGER		Specifies the Small Web pop-up3 height.
WEB_POPUP3_ WIDTH	INTEGER		Specifies the Small Web pop-up3 width.
WEB_POPUP4_ HEIGHT	INTEGER		Specifies the extra Small Web pop-up height.
WEB_POPUP4_ WIDTH	INTEGER		Specifies the extra Small Web pop-up4 width.
WEB_ PREFERENCES	INTEGER		Indicates Web Preferences Flags.
WEB_SUPPRESS_T OUR	INTEGER		Specifies the Web suppressor tour flag: **1** -- Do not Suppress**2** -- Suppress tour page
WEB_TOOLBAR_ TAB	INTEGER		Indicates the initial toolbar tab.
WF_TEMPLATE	INTEGER		

usp_pri_cal Table

Stores priority calculation data.

- **SQL Name** -- usp_pri_cal
- **Object** -- pri_cal

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
name	STRING 80		NOT_NULL UNIQUE NOT_NULL S_KEY
description	STRING 1024		
del	INTEGER		NOT_NULL
in_flag	INTEGER	Boolean_Table	
pr_flag	INTEGER	Boolean_Table	
imp_def	INTEGER	Impact	
urg_def	INTEGER	Urgency	

Field	Data Type	Reference	Remarks
ci_imp	INTEGER	Boolean_Table	
cat_urg	INTEGER	Boolean_Table	
bk_window	INTEGER		
cnt_vip	INTEGER		
pri_5_4	INTEGER	Priority	
pri_5_3	INTEGER	Priority	
pri_5_2	INTEGER	Priority	
pri_5_1	INTEGER	Priority	
pri_5_0	INTEGER	Priority	
pri_4_4	INTEGER	Priority	
pri_4_3	INTEGER	Priority	
pri_4_2	INTEGER	Priority	
pri_4_1	INTEGER	Priority	
pri_4_0	INTEGER	Priority	
pri_3_4	INTEGER	Priority	
pri_3_3	INTEGER	Priority	
pri_3_2	INTEGER	Priority	
pri_3_1	INTEGER	Priority	
pri_3_0	INTEGER	Priority	
pri_2_4	INTEGER	Priority	
pri_2_3	INTEGER	Priority	
pri_2_2	INTEGER	Priority	
pri_2_1	INTEGER	Priority	
pri_2_0	INTEGER	Priority	
pri_1_4	INTEGER	Priority	
pri_1_3	INTEGER	Priority	
pri_1_2	INTEGER	Priority	
pri_1_1	INTEGER	Priority	
pri_1_0	INTEGER	Priority	
pri_0_4	INTEGER	Priority	
pri_0_3	INTEGER	Priority	
pri_0_2	INTEGER	Priority	
pri_0_1	INTEGER	Priority	
pri_0_0	INTEGER	Priority	
cap_reason	INTEGER	Boolean_Table	
last_mod_dt	LOCAL_TIME		

Field	Data Type	Reference	Remarks
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_tenant	

usp_properties Table

Provides a list of property/value pairs for CA SDM and Knowledge Management applications.

- **SQL Name** -- usp_properties
- **Object** -- usp_properties

The maximum number of characters (HTML or pure text) allowed in the document's resolution field is 32768 bytes by default. The system Administrator can set this limit based on the type of data being stored. The limit can be set from the Administration tab, Knowledge, Documents, Document Settings.

There is also a built-in limit of 32768 bytes for the document's pure text that will be indexed. If the resolution of a document is larger than the set limit, only the first 32768 bytes of the document will be indexed and the rest will be ignored.

Field	Data Type	Reference	Remarks
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID.
auto_policies_last	Date		Displays the *last* date and time when automated policies were run on the server; stored in seconds, in UNIX time format.
auto_policies_next_ interval	Number		Identifies the number of days between automated calculation batches.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
notify_days_bef_doc_ exp	Number		Defines the number of days before the document expires and a notification is sent.
property_default	STRING 32768		Identifies the property default.
property_description	STRING 255		Identifies the property description.
property_name	STRING 100 S_KEY		Identifies the property name.
property_type	STRING 100		Identifies the property type.
property_value	STRING 32768		Identifies the property value.
suggest_knowledge_ for _issue_cats	INTEGER		Flag that determines whether or not to suggest knowledge to customers. **1** -- Suggest knowledge by default for all issue categories. **0** -- Do not suggest knowledge.

usp_notification_phrase Table

The usp_notification_phrase table lists common phrases that notification message templates can use.

- **S QL Name** -- usp_notification_phrase
- **Object** -- notification_phrase

Field	Data Type	References	Description
id	INTEGER UNIQUE KEY		Specifies the primary key of this table.
del	INTEGER REF		
last_mod_dt	LOCAL_TIME		Specifies the time stamp of when this record was last modified.
last_mod_by	UUID REF	ca_contact	Specifies the UUID of the contact who last modified this record.
code	STRING UNIQUES_KEY		Specifies the code name for the notification phrase that identifies the specific phrase when referenced in other text.
sym	STRING		Specifies the display name for the notification phrase.
description	STRING		Describes the notification phrase.
phrase	STRING		Specifies the phrase text to use for notification.

usp_organization Table

This table provides extensions to the ca_organization table that are used only by CA SDM products.

- **SQL Name** -- usp_organization
- **Object** -- org

Field	Data Type	Reference	Remarks
iorg_assigned_svr	INTEGER		Deprecated.
iorg_service_type	nvarchar(30)	Service_Desc::code	Foreign key to the code field of the srv_desc table, this is the Classic Service Type.
last_mod	INTEGER		Indicates the timestamp of when this record was last modified.
organization_uuid	byte(16)		Primary key. Unique identifier.
owning_contract	INTEGER	Service_Contract::id	Identifies the unique (to the table) numeric ID.

Form_Group Table

Listing of defined form groups.

- **SQL Name** -- fmgrp
- **Object** -- fmgrp

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive/marked as deleted
description	nvarchar (100)		Specifies the textual description of this form group.
id	INTEGER		Primary key of this table, it is a unique, numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
sym	nvarchar (30)		Specifies the symbolic value for this Form_Group.

True_False_Table Table

Contains localized True or False strings that display on the UI.

- **SQL Name** -- True_False_Table
- **Object** -- true_false

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY Unique to the table Numeric ID.
del	INTEGER		NOT_NULL Deleted flag: **0** -- Active **1** -- Inactive/marked as deleted
enum	INTEGER		NOT_NULL Enumerated value for this entry **0** -- False **1** -- True
sym	STRING 60		UNIQUE NOT_NULL S_KEY Identifies the symbolic value for this target
desc	STRING 40		Describes the enum

Access Level and Type

This article contains the following information:

Access_Levels Table

Access level definitions for CA SDM applications.

- **SQL Name** -- acc_lvls
- **Object** -- acc_lvls

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Deleted flag:**0** -- Active **1 --** Inactive/marked as deleted)
enum	INTEGER		Indicates the enumerated value for this entry, it specifies ordering in lists and relative values **Note:** This is a primary key.
id	INTEGER		Unique (to the table) Numeric ID.
nx_desc	nvarchar (40)		Specifies the description or access level.
persid	nvarchar (30)		Specifies the Persistent ID (SystemObjectName:id).
sym	nvarchar (12)		Specifies the symbolic name of the level.

Access_Type_v2 Table

Access type information for the CA SDM applications.

- **SQL Name** -- acctyp_v2
- **Object** -- acctyp

Field	Data Type	Reference	Remarks
access_level	INTEGER	Access_Levels::enum	Enumerated value for this entry, it specifies ordering in lists and relative values. **Note:** This is a foreign key.
config	INTEGER		Indicates that it is authorized for the configuration interface.
default_flag	INTEGER		Specifies the default flag value for this Access Type.

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_ Table::enum	Indicates the Deleted flag, as follows:**0** -- Active**1** -- Inactive/marked as deleted)
description	nvarchar (100)		Describes the textual description of this Access Type
external_auth	INTEGER		Allows external authorization for this Access Type.
grant_level	INTEGER	Access_Levels:: enum	Enumerated value for this entry, this specifies ordering in lists and relative values. **Note:** This is a foreign key.
id	INTEGER		Specifies the primary key of this table.
last_mod_by	Byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
ldap_access_ group	nvarchar (512)		Identifies the ldap access group value for this Access Type.
pin_field	nvarchar (50)		Specifies the field that contains the user's pin for pin type authentication.
sym	nvarchar (30)		Indicates the symbolic value for this Access Type.
user_auth	INTEGER		Identifies the user authentication type for this Access Type.
view_internal	INTEGER		Controls access to internal logs.
wsp	INTEGER		Indicates the Web Screen Painter authorization level.
cmdline_role	INTEGER	role::id	Specifies the id of the role that is used for command line utilities.
reporting_role	INTEGER	role::id	Specifies the id of the role that is used for reporting.
web_service_ role	INTEGER	role::id	Specifies the id of the role that is used for web services.
rest_web_servi ce_role	INTEGER	usp_role	

Activities

This article contains the following topics:

Act_Log Table

Act_Log is a history of activities associated with a call request. The types of activities are listed in the Act_Type table.

- **SQL Name** -- act_log
- **Object** -- alg

Field	Data Type	Reference	Remarks
action_desc	nvarchar (4000)		Provides the textual description of the activity log entry.
analyst	byte(16)	ca_contact::uuid	Foreign key to the Contact that created this activity log entry.
call_req_id	nvarchar (30)	Call_Req::persid	This is the Persistent ID (SystemObjectName:id).
description	nvarchar (4000)		Indicates the textual description of this Activity Log.
id	INTEGER		Identifies the unique (to the table) numeric ID.
internal	INTEGER		Marks this as Internal log.
knowledge_session	nvarchar (80)		Indicates the reference to a knowledge tool session.
knowledge_tool	nvarchar (12)		Specifies the Knowledge tool used for this activity.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
persid	STRING 30		Persistent ID (SystemObjectName:id).
system_time	INTEGER		Indicates the Date and Time of record creation.
time_spent	INTEGER		Specifies the time spent on this activity by the user.
time_stamp	INTEGER		Specifies the Date and Time of the user activity.
type	nvarchar (12)	Act_Type::code	(Not Used) Specifies the acknowledgement, which is a noneditable string enum.**Note:** This is a foreign key.

Act_Type Table

Identifies the activities which may be used to create a history of a ticket. Controls the creation of the activity automatically, generates a notification to those contacts specified on the call request, and controls the notification level and message.

- **SQL Name** -- act_type
- **Object** -- aty

Note: Adding an activity type requires customization to allow the activity to be part of a ticket history.

Field	Data Type	Reference	Remarks
id	INTEGER		Indicates the numeric ID that is unique to this table.
persid	nvarchar (30)		Specifies the Persistent ID: (SystemObjectName:id).
code	nvarchar (12)		This is the primary key of this table.
del	INTEGER	Active_Boolean_Table::enum	Specifies the status of the Deleted flag:**0** -- Active**1** -- Inactive/marked as deleted
sym	nvarchar (60)		Describes the name of the activity.
description	nvarchar (500)		Specifies the textual description of this Activity Type.
flag1	INTEGER	Boolean_Table:: enum	Specifies the flag1 value: **1** -- Used by call requests.
flag2	INTEGER	Boolean_Table:: enum	Specifies the flag2 value: **1** -- Used by change requests.
flag3	INTEGER	Boolean_Table:: enum	Specifies the flag3 value: **1** -- Used by issues
flag4	INTEGER	Boolean_Table:: enum	Specifies the flag4 value: **1** -- Used by messages
flag5	INTEGER	Boolean_Table:: enum	Specifies the flag5 value: **1** -- Used by Knowledge Management
flag6	INTEGER	Boolean_Table :: enum	Specifies the flag6 value: **1** -- Used by Support Automation
krc_flag	INTEGER	Boolean_Table :: enum	Specifies the flag7 value: **1** -- Used by the Knowledge Report Card
sa_notif_flag	INTEGER	Boolean_Table :: enum	Specifies the flag8 value: **1** -- Used by Support Automation assistance sessions
cr_notifiy_info	nvarchar (30)		Specifies the request information link to macros for notify.
chg_notify_info	nvarchar (30)		Specifies the change order information link to macros for notify.
iss_notify_info	nvarchar (30)		Specifies the issue information link to macros for notify.
msg_notify_info	nvarchar (30)	Spell_Macro:: persid	Specifies the message information link to macros for notify.
kd_notify_info	nvarchar (30)		Specifies the knowledge document information link to macros for notify.

Field	Data Type	Reference	Remarks
kd_comment_ notify_info	nvarchar (30)		Specifies the knowledge document comment information link to macros for notify.
krc_notify_info	nvarchar (30)		Specifies the knowledge report card information link to macros for notify.
sa_notif_info	nvarchar (30)		Specifies the support automation information link to macros for notify.
cr_send_survey	INTEGER		Specifies the request information link to macros for notify.
cr_survey_ msgbody	Long Varchar		Specifies the body text of the survey.
cr_default_ survey	INTEGER	Survey_ Template	Specifies the default template used for the survey.
cr_survey_ msgtitle	nvarchar (80)		Specifies the title of the survey.
cr_survey_ method	INTEGER	Contact_ Method	Specifies the contact method used in the survey.
chg_send_ survey	INTEGER		
chg_survey_ msgbody	Long Varchar		Specifies the body text of the survey.
chg_default_sur vey	INTEGER	Survey_ Template	Specifies the default template used for the survey.
chg_survey_msg titl	nvarchar (80)		Specifies the title of the survey.
chg_survey_met hod	INTEGER	Contact_ Method	Specifies the contact method used in the survey.
iss_send_survey	INTEGER		
iss_survey_msgb ody	Long Varchar		Specifies the body text of the survey.
iss_default_surv ey	INTEGER	Survey_ Template	Specifies the default template used for the survey.
iss_survey_msgti tl	nvarchar (80)		Specifies the title of the survey.
iss_survey_meth od	INTEGER	Contact_ Method	Specifies the contact method used in the survey.
krc_send_survey	INTEGER		
krc_survey_ msgbody	Long Varchar		Specifies the body text of the survey.
krc_default_surv ey	SREL	svy_tpl	Specifies the default template used for the survey.
krc_survey_msgt itle	nvarchar (80)		Specifies the title of the survey.

Field	Data Type	Reference	Remarks
krc_survey_method	SREL	cmth	Specifies the contact method used in the survey.
sa_send_survey	INTEGER		
sa_survey_msgbody	Long Varchar		Specifies the body text of the survey.
sa_default_survey	SREL	svy_tpl	Specifies the default template used for the survey.
sa_survey_msgtitle	nvarchar (80)		Specifies the title of the survey.
sa_survey_method	SREL	cmth	Specifies the contact method used in the survey.
internal	INTEGER		Specifies the activity type:**0** -- User activity**1** -- Internal
last_mod_dt	DATE		Indicates the timestamp of when this record was last modified.
notify	INTEGER		Specifies whether to generate notifications:**0** -- No**1** -- Yes
notify_level	INTEGER	Notification_Urgency	Indicates the Notification level.
notify_ack	nvarchar (240)		Indicates the Notification message.
notify_body	Long nvarchar		Indicates the Notification message body.
notify_body_html	Long nvarchar		Specifies the Notification message body html.
notify_title	nvarchar (80)		Specifies the Notification message title.
ci_flag	INTEGER		Specifies the CI flag value.
cnt_flag	INTEGER		Specifies the contact flag value.
ci_notify_info	nvarchar (30)		
cnt_notify_info	nvarchar (30)		
rel_ticket	INTEGER		Specifies the related ticket of the activity.
single_tenant	UUID	ca_tenant	Specifies the UUID of the single tenant.
tenant_group	UUID	ca_tenant	Specifies the UUID of the tenant group.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

Act_Type_Assoc Table

Maps a field of an object we want to do activity logging for to an Activity Type (Assignee field on a request is mapped to 'Transfer' Act_Type. All _rsrved fields are reserved for CA and NOT FOR CLIENT USE)

- **SQL Name** -- atyp_asc
- **Object** -- act_type_assoc

Field	Data Type	Reference	Remarks
act_type	STRING 30	Act_Type::code	Associated activity type
code	STRING 12		UNIQUE NOT_NULL S_KEY
description	STRING 80		Textual description of this Act Type Association
id	INTEGER		Unique (to the table) Numeric ID UNIQUE NOT_NULL KEY
int1_rsrved	INTEGER		Flex field
int2_rsrved	INTEGER		Flex field
int3_rsrved	INTEGER		Flex field
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified
log_me_f	INTEGER		Logging on/off flag
ob_type	STRING 30		Associated object type
ob_type_attr	STRING 50		Attribute name within associated object
persid	STRING 30		Persistent ID (SystemObjectName:id)
str1_rsrved	STRING 30		Flex fields - reserved for CA
str2_rsrved	STRING 30		Flex field
str3_rsrved	STRING 30		Flex field
sym	STRING 30 NOT_NULL		

Boolean

This article contains the following topics:

Active_Boolean_Table Table

Table to translate 0 and 1 for the del field on records.

- **SQL Name** -- actbool
- **Object** -- actbool

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL		**0** -- Active **1** -- Inactive/marked as deleted
description	STRING 240		Textual description of this boolean value
enum	INTEGER NOT_NULL		Enumerated value for this entry
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified
sym	STRING 12 S_KEY		

Active_Reverse_Boolean_Table Table

Table to translate 0 and 1 for the del field on records.

- **SQL Name** -- acrtbool
- **Object** -- actrbool

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL		**0** -- Active **1** -- Inactive/marked as deleted
description	STRING 240		Specifies the textual description of this boolean value
enum	INTEGER NOT_NULL		Enumerated value for this entry
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified
sym	STRING 12 S_KEY		

Boolean_Table Table

Table of boolean values that allows the customer to define the text associated with true and false.

- **SQL Name** -- bool_tab
- **Object** -- bool

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL		Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
enum	INTEGER NOT_NULL		

Field	Data Type	Reference	Remarks
			Enumerated value for this entry - specifies ordering in lists and relative values
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
nx_desc	STRING 40		
sym	STRING 12 UNIQUE NOT_NULL S_KEY		

Reverse_Boolean_Table Table

Reverse boolean lookup table.

- **SQL Name** -- rbooltab
- **Object** -- rev_bool

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL		Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
enum	INTEGER NOT_NULL		Enumerated value for this entry - specifies ordering in lists and relative values
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
nx_desc	STRING 40		
sym	STRING 12 UNIQUE NOT_NULL S_KEY		

Asset

This article contains the following topics:

Am_Asset_Map Table

Maps a CA Asset Management asset to an internal object am_domain_id and am_unit_id to form a unique AM asset identifier. NOT FOR CLIENT USE.

- **SQL Name** -- am_map
- **Object** -- am_asset_map

Field	Data Type	Reference	Remarks
am_dmuuid	STRING 64		AM DMUUID of asset
am_domain_id	INTEGER		AM asset domain identifier which created asset
am_server	STRING 64		AM name of UAM domain server
am_type	INTEGER		AM asset type **1** -- Computer **2** -- User
am_unit_domain_id	INTEGER		AM asset domain identifier of asset
am_unit_id	INTEGER		AM asset unit id
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
int1_rsrved	INTEGER		Reserved for CA
int2_rsrved	INTEGER		Reserved for CA
ob_persid	STRING 30		
ob_type	STRING 30		
persid	STRING 30		Persistent ID: SystemObjectName:id
str1_rsrved	STRING 80		Reserved for CA
str2_rsrved	STRING 80		Reserved for CA
version	INTEGER NOT_NULL		Internal version

Asset_Assignment Table

Describes a relationship between two assets. Each instance of this table is one parent-child arrangement.

- **SQL Name** -- hier
- **Object** -- hier

Field	Data Type	Reference	Remarks
hier_child	UUID NOT_NULL S_KEY	ca_owned_resource:: uuid	Specifies the child.
hier_license_num	STRING 40		Specifies the license serial number.
hier_log_date	LOCAL_TIME NOT_NULL		Specifies the time of assignment.
hier_parent	UUID NOT_NULL S_KEY	ca_owned_resource:: uuid	Specifies the parent.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
	UUID	ca_contact::uuid	

Field	Data Type	Reference	Remarks
last_mod_by			Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
persid	STRING 30		Persistent ID (SystemObjectName:id)

Archive and Purge

This article contains the following topics:

Archive_Purge_History Table

Historic information about archive/purge activities completed.

- **SQL Name** -- arcpur_hist
- **Object** -- arcpur_hist

Field	Data Type	Reference	Remarks
chd_obj_deleted	INTEGER		
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
end_time	LOCAL_TIME		
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified
obj_deleted	INTEGER		
persid	STRING 30		Persistent ID (SystemObjectName:id)
rule_name	STRING 30 NOT_NULL	Archive_Purge_Rule::persid	
start_time	LOCAL_TIME		

Archive_Purge_Rule Table

Rule definitions for the archive/purge engine.

- **SQL Name** -- arcpur_rule

- **Object** -- arcpur_rule

Field	Data Type	Reference	Remarks
add_query	STRING 240		
arc_file_name	STRING 240		
conf_obj_name	STRING 64		
days_inactive	INTEGER NOT_NULL		
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
name	STRING 30 NOT_NULL UNIQUE NOT_NULL S_KEY		Specifies the text name of this item.
oper_type	INTEGER NOT_NULL		
persid	STRING 30		Persistent ID (SystemObjectName:id)
reoccur_interv	DURATION		
sched	STRING 30	Bop_Workshift :: persid	

Attached_Events Table

This article contains the following topics:

This table lists the actual attached events and their information.

- **SQL Name** -- att_evt
- **Object** -- atev

Field	Data Type	Reference	Remarks
	LOCAL_TIME		Time canceled

Field	Data Type	Reference	Remarks
cancel_time			
event_tmpl	STRING 30 NOT_NULL S_KEY	Events::persid	Specifies the persid for the attached event.
fire_time	LOCAL_TIME		Datetime event will fire.
first_fire_time	LOCAL_TIME		Datetime event first fired.
group_name	STRING 30		Group smag field.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
num_fire	INTEGER		Number of times the event fired.
obj_id	STRING 30 NOT_NULL		The persid of the object.
owning_ast	INTEGER	Attached_SLA::id	Owning ast object (CA Service Desk Manager Version 11.0).
persid	STRING 30		Persistent ID (SystemObjectName:id).
start_time	LOCAL_TIME		Datetime when the event was attached.
status_flag	INTEGER		
user_smag	STRING 200		User smag field
wait_time	DURATION		Time to wait before firing

Attached_SLA Table

Service Level Agreements associated to a ticket.

- **SQL Name** -- attached_sla
- **Object** -- attached_sla

Field	Data Type	Reference	Remarks
_mapped_chg	INTEGER	chg id	
_mapped_cr	STRING 30	Call_Req::persid	These are mostly required for advanced runtime queries.
_mapped_iss	STRING 30	issue persistent_id	
_mapped_iss_wf	INTEGER	isswf::id	
_mapped_wf	INTEGER	wf::id	
del	INTEGER NOT_NULL		

Field	Data Type	Reference	Remarks
		Active_Boolean_ Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
last_ttv_upd	LOCAL_TIME		
map_sdsc	STRING 30 NOT_NULL	Service_Desc:: code	
persid	STRING 30		Persistent ID (SystemObjectName:id)
sla_viol_status	INTEGER		
ticket_id	INTEGER NOT_NULL S_KEY		
ticket_type	STRING 30 NOT_NULL		
time_to_ violation	LOCAL_TIME		
ttv_event	STRING 30	Attached_Events:: persid	

Attachment Table

Object Attachments. (5.0 version)

- **SQL Name** -- attmnt
- **Object** -- attmnt

Field	Data Type	Reference	Remarks
attmnt_name	STRING 240		Specifies the attachment name.
created_by	UUID	ca_contact::uuid	Specifies who created this attachment.
created_dt	LOCAL_TIME		Specifies when the attachments was created.
del	INTEGER NOT_NULL	Active_Boolean_ Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
description	STRING 500		Specifies the textual description of this attachment.
exec_cmd	STRING 12	Remote_Ref:: code	Specifies the unix exec string (not currently used).
file_date	LOCAL_TIME		Specifies the date of the file.

Field	Data Type	Reference	Remarks
file_name	STRING 240		Specifies the server attachment filename.
file_size	INTEGER		Specifies the size of the file.
file_type	STRING 12		Specifies the file extension (not currently used).
folder_id	INTEGER	attmnt_folder::id	Specifies the folder id.
folder_path_ids	STRING 255		Specifies the folder path ids.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
inherit_permission_id	INTEGER		Specifies the folder ID where pgroup permissions come from.
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
link_only	INTEGER	Boolean_Table :: enum	
link_type	String		If embedded image = EMBD_IMG, otherwise NULL
orig_file_name	STRING 240		original file name, URL or UNC
persid	STRING 30		Persistent ID (SystemObjectName:id)
read_pgroup	INTEGER	P_GROUPS::id	Specifies the group of groups eligible to read the document.
rel_file_path	STRING 512		Specifies the relative path to the file.
repository	SREL	Document_Repository::persid	Specifies the repository.
status	STRING 12		Specifies the attachment status (INSTALLED, INSTALL_FAILED, LINK_ONLY).
write_pgroup	INTEGER	P_GROUPS::id	Specifies the group of groups eligible to update the document.
zip_flag	INTEGER		Specifies if the file is zipped.

attmnt_folder Table

List of attachment repository locations.

- **SQL Name** -- attmnt_folder
- **Object** -- attmnt_folder

Field	Data Type	Reference	Remarks
description	STRING 500		Textual description of this attachment folder
folder_name	STRING 255		Specifies the folder name
folder_path_ ids	STRING 255		Specifies the folder path ids
folder_type	INTEGER		Specifies the folder type
has_children	INTEGER		Specifies if the folder has children
id	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
inherit_ permission_ id	INTEGER	attmnt_folder::id	Specifies the id of folder to inherit from
last_mod_ date	LOCAL_TIME		Specifies the last modify date
parent_id	SREL	attmnt_folder::id	Specifies the parent folder id
read_pgroup	INTEGER	P_GROUPS::id	Read p Group permissions of the attachment
repository	SREL	Document_ Repository:: persid	Specifies the repository pers id
write_pgroup	INTEGER	P_GROUPS::id	Write p Group permissions of the attachment
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

Attachment

This article contains the following topics:

Attachment Table

Object Attachments. (5.0 version)

- **SQL Name** -- attmnt
- **Object** -- attmnt

Field	Data Type	Reference	Remarks
attmnt_name	STRING 240		Specifies the attachment name.
created_by	UUID	ca_contact::uuid	Specifies who created this attachment.
created_dt	LOCAL_TIME		Specifies when the attachment was created.

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL	Active_Boolean_ Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
description	STRING 500		Specifies the textual description of this attachment.
exec_cmd	STRING 12	Remote_Ref:: code	Specifies the unix exec string (not currently used).
file_date	LOCAL_TIME		Specifies the date of the file.
file_name	STRING 240		Specifies the server attachment filename.
file_size	INTEGER		Specifies the size of the file.
file_type	STRING 12		Specifies the file extension (not currently used).
folder_id	INTEGER	attmnt_folder::id	Specifies the folder id.
folder_path_ids	STRING 255		Specifies the folder path ids.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
inherit_ permission_id	INTEGER		Specifies the folder ID where pgroup permissions come from.
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
link_only	INTEGER	Boolean_Table :: enum	
link_type	String		If embedded image = EMBD_IMG, otherwise NULL
orig_file_name	STRING 240		Original file name, URL or UNC
persid	STRING 30		Persistent ID (SystemObjectName:id)
read_pgroup	INTEGER	P_GROUPS::id	Specifies the group of groups eligible to read the document.
rel_file_path	STRING 512		Specifies the relative path to the file.
repository	SREL	Document_ Repository::persid	Specifies the repository.
status	STRING 12		Specifies the attachment status (INSTALLED, INSTALL_FAILED, LINK_ONLY).
write_pgroup	INTEGER	P_GROUPS::id	Specifies the group of groups eligible to update the document.
zip_flag	INTEGER		Specifies if the file is zipped.

attmnt_folder Table

List of attachment repository locations.

- **SQL Name** -- attmnt_folder
- **Object** -- attmnt_folder

Field	Data Type	Reference	Remarks
description	STRING 500		Textual description of this attachment folder
folder_name	STRING 255		Specifies the folder name
folder_path_ ids	STRING 255		Specifies the folder path ids
folder_type	INTEGER		Specifies the folder type
has_children	INTEGER		Specifies if the folder has children
id	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
inherit_ permission_ id	INTEGER	attmnt_folder::id	Specifies the id of folder to inherit from
last_mod_ date	LOCAL_TIME		Specifies the last modify date
parent_id	SREL	attmnt_folder::id	Specifies the parent folder id
read_pgroup	INTEGER	P_GROUPS::id	Read p Group permissions of the attachment
repository	SREL	Document_ Repository:: persid	Specifies the repository pers id
write_pgroup	INTEGER	P_GROUPS::id	Write p Group permissions of the attachment
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

usp_lrel_attachments_changes Table

Relates attachments to change orders.

- **SQL Name** -- usp_lrel_attachments_changes
- **Object** -- lrel_attachments_changes

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
chg	INTEGER	Change_Request	
attmnt	INTEGER	Attachment	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_attachments_issues Table

Relates attachments to issues.

- **SQL Name** -- usp_lrel_attachments_issues
- **Object** -- lrel_attachments_issues

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
iss	STRING 30	Issue	
attmnt	INTEGER	Attachment	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_attachments_requests Table

Relates attachments to requests, problems, or incidents.

- **SQL Name** -- usp_lrel_attachments_requests
- **Object** -- lrel_attachments_requests

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
cr	STRING 30	Call_Req	
attmnt	INTEGER	Attachment	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

Document_Repository Table

Contains Information on document repositories, which are used to store attachments.

- **SQL Name** -- doc_rep
- **Object** -- doc_rep

Field	Data Type	Reference	Remarks
description	STRING 500		Specifies the description.
archive_path	STRING 255		

Field	Data Type	Reference	Remarks
archive_type	INTEGER		
cgi_path	STRING 255		Specifies the location and name of CGI.
default_rep	INTEGER		
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
file_limit_size	INTEGER		Specifies the file limit size.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
persid	STRING 30		Persistent ID (SystemObjectName:id)
prohibited_ext	STRING 500		Specifies the prohibited file extensions.
protocol	STRING 12		HTTP or SHARE
repository_type	INTEGER		Specifies the type of repository (attachments, knowledge).
retrieve_path	STRING 255		Specifies how to get back to upload_path via protocol.
server	STRING 30		Specifies the name of Doc Server.
servlet_path	STRING 255		Specifies the servlet URL.
sym	STRING 30 NOT_NULL S_KEY		Specifies the name of document repository.
upload_path	STRING 255		Specifies the server location of doc repository.

Company (CA MDB)

This article contains the following topics:

ca_company Table

Company information (CA-MDB).

- **SQL Name** -- ca_company

- **Object** -- ca_cmpny

Field	Data Type	Reference	Remarks
alias	nvarchar(30)		Identifies the Company alias or "also known as" name. For example, CA.
authentication_ password	nvarchar(20)		Specifies the authentication password.
authentication_ user_name	nvarchar(64)		Specifies the authentication user name.
bbs	nvarchar(30)		Identifies bulletin board system information.
company_name	nvarchar (100)		Identifies the company name.
company_type	INTEGER	ca_company_type::id	Identifies the Company Type or Vendor Provider. **Note:** This is the Foreign key to the id field of the ca_company_type table.
company_uuid	Byte (16)		The Primary key of this table.
creation_date	INTEGER		Indicates the date this record was created.
creation_user	nvarchar(64)		Identifies the user or process that created the record.
delete_time	INTEGER		Specifies the delete time.
description	nvarchar (400)		Shows the textual description of this entry.
exclude_registration	INTEGER		Indicates to exclude registration.
inactive	INTEGER	Active_Boolean_Table:: enum	Flag representing whether this record is active or inactive.**0** -- False (Active)**1** -- True (Inactive)
last_update_date	INTEGER		Indicates the date that this record was last updated.
last_update_user	nvarchar(64)		Identifies the user or process that last updated the record.
location_uuid	Byte (16)	ca_location:: location_uuid	Identifies the location.**Note:** This is the Foreign key to the ca_location table entry.
month_fiscal_year_ends	INTEGER		Specifies the Integer value (1-12) representing the month the company's fiscal year ends.
parent_company_ uuid	Byte (16)	ca_company:: company_uuid	This is the Foreign key to the company_uuid field of the ca_company table for the company's parent company.

Field	Data Type	Reference	Remarks
primary_contact_ uuid	Byte (16)	ca_contact::uuid	Specifies the Primary contact. **Note:** This is the Primary foreign key to the ca_contact table.
source_type_id	INTEGER		Represents the Source type id.**Note:** This is the Foreign key to the ca_source_type table.
version_number	INTEGER		Specifies the version number for transaction integrity.
web_address	nvarchar(50)		Identifies the company web address.

ca_company_type Table

Company type information (CA-MDB).

- **SQL Name** -- ca_company_type
- **Object** -- vpt

Field	Data Type	Reference	Remarks
creation_date	INTEGER		Specifies the date this record was created.
creation_user	nvarchar (64)		Identifies the user or process that created the record.
description	nvarchar (255)		Provides the textual company type description of this entry.
id	INTEGER		Specifies the Primary key, this also identifies the unique company type numeric ID.
inactive	INTEGER	Active_Boolean_ Table::enum	Specifies Active flag, as follows:**0** -- False (Active)**1** -- True (Inactive)
last_update_date	INTEGER		Specifies the date when this record was last updated.
last_update_user	nvarchar (64)		Specifies the user or process that updated the record.
name	nvarchar (100)		Identifies the unique, company type name.
version_ number	INTEGER		Specifies the version number for transaction integrity

Contact (CA MDB)

This article contains the following topics:

ca_contact Table

Table of persons that interact with the system in some manner (CA-MDB).

- **SQL Name** -- ca_contact
- **Object** -- cnt

Field	Data Type	Reference	Remarks
admin_organization_uuid	Byte (16)	ca_organization :: organization_uuid	Identifies the Administrative Organization.**Note:** This is the Foreign key to the ca_organization table.
alias	nvarchar (30)		Identifies the Contact alias or "known as" name.
alt_phone_number	nvarchar (40)		Specifies the alternate phone number.
alternate_identifier	nvarchar (30)		Identifies the alternate contact (for example, the social security number).
comment	nvarchar (255)		Shows the text of the comment.
company_uuid	Byte (16)	ca_company::company_uuid	Identifies the Company.**Note:** This is the Foreign key to the ca_company table.
contact_type	INTEGER	ca_contact_type::id	Specifies the Contact type, such as: Customer, Analyst, and so on.**Note:** This is the Foreign key to the id field of the ca_contact_type table.
contact_uuid	Byte (16)		This is the Primary key, and is a unique identifier.
cost_center	INTEGER	ca_resource_cost_ center::id	Identifies the cost center.**Note:** This is the Foreign key to the id field of the ca_resource_cost_center table.
creation_date	INTEGER		Identifies the date that the record was created.
creation_user	nvarchar (64)		Specifies the user or process that created this record.
delete_time	INTEGER		Shows the time of deletion.
department	INTEGER	ca_resource_department::id	Identifies the department.**Note:** This is the Foreign key to the id field of the ca_resource_department table.

Field	Data Type	Reference	Remarks
email_address	nvarchar (120)		Identifies the email address.
exclude_registration	INTEGER		Indicates to exclude registration.
fax_number	nvarchar (40)		Identifies the fax number.
first_name	nvarchar (100)		Identifies the first name.
floor_location	nvarchar (30)		Identifies the floor location. (for example, the employee works on the first floor).
inactive	INTEGER	Active_Boolean_ Table::enum	Specifies the Active flag, as follows:**0** -- Active**1** -- Inactive
inrdid	INTEGER		Identifies the role ID.
job_function	INTEGER		Specifies the job function.**Note:** This is the Foreign key to ca_job_function table.
job_title	INTEGER	ca_job_title::id	Specifies the job title.**Note:** This is a Foreign key.
last_name	nvarchar (100)		(Required) Identifies the last name.
last_update_date	INTEGER		Shows the date this record was last updated.
last_update_user	nvarchar (64)		Specifies the user or process that last updated the record.
location_uuid	Byte (16)	ca_location::location_uuid	Specifies the location.**Note:** This is the Foreign key to the ca_location table entry.
mail_stop	nvarchar (30)		Identifies the mail stop.
middle_name	nvarchar (100)		Identifies the middle name.
mobile_phone_number	nvarchar (40)		Specifies the mobile phone number.

Field	Data Type	Reference	Remarks
organization_uuid	Byte (16)	ca_organization::organization_uuid	Specifies the Organization.**Note:** This is a Foreign key to the id field of the ca_organization table.
pager_email_address	nvarchar (120)		Identifies the pager email address.
pager_number	nvarchar (40)		Identifies the pager number.
pri_phone_number	nvarchar (40)		Identifies the primary phone number.
room_location	nvarchar (30)		Identifies the Room location (for example, the employee works in Cube 123).
supervisor_contact_uuid	Byte (16)	ca_contact::uuid	Identifies the Supervisor.**Note:** This is a Foreign key to the ca_contact table.
userid	nvarchar (100)		Specifies the User account id (for example, a company employee ID). This ID is unique for active records in order to prevent a user from retrieving the security settings of another user.
version_number	INTEGER		Version number for transaction integrity.

ca_contact_type Table

Definitions of type/classifications of personal information stored in the ca_contact table (CA-MDB).

- **SQL Name** -- ca_contact_type
- **Object** -- ctp

Field	Data Type	Reference	Remarks
creation_date	INTEGER		Specifies the date when this record was created.
creation_user	nvarchar (64)		Identifies the user or process that created this record.
delete_time	INTEGER		Specifies the delete time.
description	nvarchar (255)		Specifies the textual, contact type description.
exclude_registration	INTEGER		Indicates to exclude registration.
hourly_cost	Money		Specifies the hourly cost.

id	INTEGER		Unique (to the table), numeric contact type ID.**Note:** This is a Primary key.
inactive	INTEGER	Active_Boolean_Table::enum	Identifies the Active flag, as follows:**0** -- False (Active)**1** -- True (Inactive)
last_update_date	INTEGER		Specifies the date of when this record was last updated.
last_update_user	nvarchar (64)		Identifies the user or process that last updated the record.
name	nvarchar (100)		Identifies the unique,contact type name.
user_uuid	UUID	ca_contact:: uuid	This is a unique identifier.**Note:** This is also the Primary key.
version_number	INTEGER		Version number for transaction integrity.
view_internal	INTEGER		Flag to represent whether this contact type is allowed to view internal data.

Job (CA MDB)

This article contains the following topics:

ca_job_function Table

Job function descriptions (CA-MDB).

- **SQL Name** -- ca_job_function
- **Object** -- job_func

Field	Data Type	Reference	Remarks
creation_date	INTEGER		Specifies the date when this record was created.
creation_user	nvarchar (64)		Specifies the user or process that created the record.
delete_time	INTEGER		Identifies the delete time.
description	nvarchar (255)		Specifies the Job function description.
exclude_registration	INTEGER		Indicates to exclude registration.
id	INTEGER		Identifies the unique (to the table) numeric job function ID.**Note:** This is a Primary key.

Field	Data Type	Reference	Remarks
inactive	INTEGER	Active_Boolean_Table::enum	Sets the Active flag, as follows:**0** -- False (Active)**1** -- True (Inactive)
last_update_date	INTEGER		Specifies the date of when this record was last updated.
last_update_user	varchar (64)		Identifies the user or process that last updated the record.
name	varchar (100)		Identifies the job function name.
version_number	INTEGER		Specifies the version number for transaction integrity.

ca_job_title Table

Job title descriptions (CA-MDB).

- **SQL Name** -- ca_job_title
- **Object** -- position

Field	Data Type	Reference	Remarks
creation_date	INTEGER		Specifies the date of when this record was created.
creation_user	nvarchar(64)		Identifies the user or process that created the record.
delete_time	INTEGER		Indicates the time of deletion.
exclude_registration	INTEGER		Indicates to exclude registration.
id	INTEGER		Identifies the unique (to the table) numeric job title ID.**Note:** This is a Primary key.
inactive	INTEGER	Active_Boolean_Table::enum	Specifies the Active flag, as follows:**0** -- False (Active)**1** -- True (Inactive)
last_update_date	INTEGER		Indicates the date of when this record was last updated.
last_update_user	varchar (64)		Specifies the user or process that last updated the record.
name	varchar (100)		Specifies the job title name.
version_number	INTEGER		Specifies the version number for transaction integrity.

Organization

ca_organization Table

Used to describe a business, or associate businesses with smaller business units, or contacts to businesses.

- **SQL Name** -- ca_organization
- **Object** -- org

Field	Data Type	Reference	Remarks
abbreviation	nvarchar(30)		Identifies the abbreviation of the organization.
alt_phone_cc	INTEGER		Identifies the alternate phone number country code.
alt_phone_number	nvarchar(32)		Specifies the alternate phone number.
comment	nvarchar (255)		Shows the comment.
company_uuid	byte (16)	ca_company::company_uuid	Foreign key to the company_uuid field of the ca_company table representing the organization's company.
contact_uuid	byte (16)	ca_contact::uuid	Foreign key to the contact_uuid field of the ca_contact table representing the organization's primary contact.
cost_center	INTEGER	ca_resource_cost_center::id	Foreign key to the id field of ca_resource_cost_center table which represent this cost center.
creation_date	INTEGER		Identifies the date of when this record was created.
creation_user	nvarchar(64)		Identifies the user or process that created the record.
delete_time	INTEGER		Specifies the time of deletion.
description	nvarchar (255)		Indicates the description of the organization.
email_address	nvarchar (120)		Specifies the email address.
exclude_registration	INTEGER		Indicates to exclude registration.
fax_cc	INTEGER		Specifies the fax number's country code.
fax_number	nvarchar(32)		Identifies the fax number.

inactive	INTEGER	Active_Boolean_Table::enum	Specifies the Active flag, as follows:**0** -- False (Active)**1** -- True (Inactive)
last_update_date	INTEGER		Specifies the date of when this record was last updated.
last_update_user	nvarchar(64)		Specifies the user or process that last updated this record.
location_uuid	byte (16)	ca_location::location_uuid	Foreign key to the location_uuid field of the ca_location table for the organization's parent location.
org_name	nvarchar (100)		Identifies the name of the organization.
organization_uuid	byte (16)		This is the Primary key for Organization.
pager_email_address	nvarchar (120)		Identifies the pager email address.
parent_org_uuid	byte (16)		Foreign key to the organization_uuid field of the ca_organization table for the organization's parent organization.
pri_phone_cc	INTEGER		Identifies the country code for the primary phone number.
pri_phone_number	nvarchar(32)		Identifies the primary phone number.
version_number	INTEGER		Specifies the version number for transaction integrity.

Model Definitions

ca_model_def Table

Model definitions for specific manufacturer/model combinations (CA-MDB).

- **SQL Name** -- ca_model_def
- **Object** -- mfrmod

Field	Data Type	Reference	Remarks
abbreviation	nvarchar(30)		Specifies the model abbreviation.
capacity	float		Defines the capacity.
capacity_unit	INTEGER		Defines the capacity unit.**Note:** This is the Foreign key to the id field of the ca_capacity_unit table.

Field	Data Type	Reference	Remarks
class_id	INTEGER	ca_resource_class::id	Foreign key to the id field of the ca_resource_class table for the class to which this model belongs.
creation_date	INTEGER		Specifies the date of when this record was created.
creation_user	nvarchar(64)		Identifies the user or process that created the record.
current_as_of_ date	INTEGER		Specifies the date which represents the point at which the model information is considered current.
delete_time	INTEGER		Indicates the time of deletion.
description	nvarchar (255)		Identifies the model description.
exclude_registration	INTEGER		Indicates to exclude registration.
family_id	INTEGER		Foreign key to the id field of the ca_resource_family table for the family to which this model belongs.
gl_code	INTEGER		Specifies the GL code.**Note:** This is the Foreign key to the id field of the ca_resource_gl_code table.
inactive	INTEGER	Active_Boolean_Table::enum	Specifies the Active flag, as follows:**0** -- False (Active)**1 --** True (Inactive)
last_update_date	INTEGER		Specifies the date of when this record was last updated.
last_update_user	nvarchar(64)		Specifies the user or process that last updated this record.
manufacturer_uuid	byte (16)	ca_company::company_uuid	Foreign key to the company_uuid field of the ca_company table for the record that represents the manufacturer.
model_uuid	byte (16)		Specifies the model ID.**Note:** This is a Primary key.
name	nvarchar (100)		Identifies the unique Model name.
operating_system	INTEGER		Operating system.**Note:** It is a Foreign key to the id field of the ca_resource_operating_system table.
preferred_seller_uuid	byte (16)		Foreign key to the company_uuid field of the ca_company table for the record that represents the preferred seller company of this model.
subclass_id	INTEGER		Foreign key to the id field of the ca_resource_class table for the subclass to which this model belongs.
version_number	INTEGER		Indicates the version number for transaction integrity.

Resource

This article contains the following topics:

ca_resource_class Table

Definitions of the classifications that may be applied to an asset/resource.

- **SQL Name** -- ca_resource_class
- **Object** -- grc

Field	Data Type	Reference	Remarks
creation_date	INTEGER		Specifies the date the of when this record was created.
creation_user	nvarchar(64)		Identifies the user or process that created the record.
delete_time	INTEGER		Indicates the date of deletion.
description	nvarchar (255)		Specifies the class description.
exclude_registration	INTEGER		Indicates to exclude registration.
family_id	INTEGER	ca_resource_family::id	Primary key that is also the resource family id.
id	INTEGER		Primary key that is also the class id.
inactive	INTEGER	Active_Boolean_Table::enum	Sets the Active flag, as follows:**0** -- False (Active)**1** -- True (Inactive)
last_update_date	INTEGER		Indicates the date the record was last updated.
last_update_user	nvarchar(64)		Specifies the user or process that last updated the record.
name	nvarchar (100)		Identifies the unique class name within family.

Field	Data Type	Reference	Remarks
parent_id	SREL		Foreign key back to the id field of the ca_resource_class table to allow for hierarchical class groupings (for example, subclass).
usp_nsm_class	INTEGER	buscls id	Represents the CA NSM class.**Note:** This is the Foreign key to the id field of the buscls table.
version_number	INTEGER		Specifies the version number for transaction integrity.

ca_resource_cost_center Table

An asset is associated with.

- **SQL Name** -- ca_resource_cost_center
- **Object** -- cost_cntr

Field	Data Type	Reference	Remarks
creation_date	INTEGER		Identifies the date of when this record was created.
creation_user	nvarchar (64)		User or process that created the record.
delete_time	INTEGER		Specifies the time of deletion.
description	nvarchar (255)		Indicates the cost center description.
exclude_registration	INTEGER		Specifies to exclude registration.
id	INTEGER		Primary key that is also the cost center id.
inactive	INTEGER	Active_Boolean_Table::enum	Sets the Active flag, as follows:**0** -- False (Active)**1** -- True (Inactive)
last_update_date	INTEGER		Specifies the date of when this record was last updated.
last_update_user	nvarchar (64)		Specifies the user or process that last updated this record.
name	nvarchar (100)		Identifies the unique cost center name.
version_number	INTEGER		Specifies the version number for transaction integrity.

ca_resource_department Table

Department that a resource is assigned to and associated with.

- **SQL Name** -- ca_resource_department

- **Object** -- dept

Field	Data Type	Reference	Remarks
creation_date	INTEGER		Specifies the date of when this record was created.
creation_user	nvarchar (64)		Indicates the user or process that created this record.
delete_time	INTEGER		Indicates the time of deletion.
description	nvarchar (255)		Specifies the department description.
exclude_registration	INTEGER		Specifies to exclude registration.
id	INTEGER		Primary key that is also the resource department id.
inactive	INTEGER	Active_Boolean_Table ::enum	Sets the Active flag, as follows:**0** -- False (Active)**1** -- True (Inactive)
last_update_date	INTEGER		Specifies the date of when this record was last updated.
last_update_user	nvarchar (64)		Specifies the user or process that last updated the record.
name	nvarchar (100)		Identifies the unique department name.
version_number	INTEGER		Specifies the version number for transaction integrity.

ca_resource_family Table

High level classification of a resource items, such as Computer, furniture, phone, software and so on.

- **SQL Name** -- ca_resource_family
- **Object** -- nrf

Field	Data Type	Reference	Remarks
creation_date	INTEGER		Specifies the date of when this record was created.
creation_user	nvarchar (64)		Indicates the user or process that created this record.
delete_time	INTEGER		Indicates the time of deletion.
description	nvarchar (255)		Specifies the family description.
exclude_ registration	INTEGER		Specifies to exclude registration.
id	INTEGER		Primary key that is also the resource family id.

Field	Data Type	Reference	Remarks
inactive	INTEGER	Active_Boolean_Table::enum	Specifies the Active flag, as follows:**0** -- False (Active)**1** -- True (Inactive)
include_reconciliation	INTEGER		Specifies the flag that indicates whether to include this family in reconciliation.
last_update_date	INTEGER		Specifies the date of when this record was last updated.
last_update_user	nvarchar (64)		Specifies the user or process that last updated the record.
name	nvarchar (100)		Identifies the unique family name.
table_extension_ name	nvarchar (30)		Identifies the name of the associated table to hold extended data for this family.
version_number	INTEGER		Indicates the version number for transaction integrity.

ca_resource_gl_code Table

General ledger entry a resource is assigned to/associated with.

- **SQL Name** -- ca_resource_gl_code
- **Object** -- gl_code

Field	Data Type	Reference	Remarks
creation_date	INTEGER		Specifies the date of when this record was created.
creation_user	nvarchar (64)		Indicates the user or process that created this record.
delete_time	INTEGER		Indicates the time of deletion.
description	nvarchar (255)		Specifies the GL code description.
exclude_registration	INTEGER		Specifies to exclude registration.
id	INTEGER		Primary key that is also the resource GL code id.
inactive	INTEGER	Active_Boolean_Table::enum	Specifies the Active flag, as follows:**0** -- False (Active) **1** -- True (Inactive)
last_update_date	INTEGER		Specifies the date of when this record was last updated.
last_update_user	nvarchar (64)		Specifies the user or process that last updated the record.
name	nvarchar (100)		Identifies the unique GL code name.
	INTEGER		

Field	Data Type Reference		Remarks
version_number			Indicates the version number for transaction integrity.

ca_resource_operating_system Table

Operating system a resource is assigned to/associated with.

- **SQL Name** -- ca_resource_operating_system
- **Object** -- opsys

Field	Data Type Reference		Remarks
creation_date	INTEGER		Specifies the date of when this record was created.
creation_user	nvarchar (64)		Indicates the user or process that created this record.
delete_time	INTEGER		Indicates the time of deletion.
description	nvarchar (255)		Specifies the operating system description.
exclude_registration	INTEGER		Indicates to exclude registration.
id	INTEGER		Primary key that is also the resource operating system id.
inactive	INTEGER	Active_Boolean_Table::enum	Specifies the Active flag, as follows:**0 --** False (Active) **1 --** True (Inactive)
last_update_date	INTEGER		Specifies the date of when this record was last updated.
last_update_user	nvarchar (64)		Specifies the user or process that last updated the record.
name	nvarchar (100)		Identifies the unique operating system name.
version_number	INTEGER		Specifies the version number for transaction integrity.

ca_resource_status Table

Status of a resource/asset.

- **SQL Name** -- ca_resource_status
- **Object** -- rss

Field	Data Type Reference		Remarks
creation_date	INTEGER		Specifies the date of when this record was created.
creation_user	nvarchar (64)		Indicates the user or process that created this record.

Field	Data Type	Reference	Remarks
delete_time	INTEGER		Indicates the time of deletion.
description	nvarchar (255)		Specifies the operating system description.
exclude_ registration	INTEGER		Specifies to exclude registration.
id	INTEGER		Primary key that is also the resource status id.
inactive	INTEGER	Active_Boolean_ Table::enum	Specifies the Active flag, as follows:**0** -- False (Active) **1** -- True (Inactive)
last_update_d ate	INTEGER		Specifies the date of when this record was last updated.
last_update_us er	nvarchar (64)		Specifies the user or process that last updated the record.
name	nvarchar (100)		Identifies the unique status name.
version_numb er	INTEGER		Indicates the version number for transaction integrity.

Tenant

This article contains the following topics:

ca_tenant Table

This table lists information about a tenant.

- **SQL Name** -- ca_tenant
- **Object** -- tenant

Column	Type	Remarks
id	UUID	ID
name	STRING 255	Specifies the tenant name.
tenant _numb er	STRING 30	Specifies the alternate tenant identification (customer comment; no OTB use)
service _provid er	INTEGER	**1** -- Service Provider tenant
contact	SREL cnt	Specifies the primary contact for the tenant .

Column	Type	Remarks
logo	STRING 255	Specifies the URL of the tenant logo.
description	STRING 1024	
phone_number	STRING 255	
fax_phone	STRING 255	
alt_phone	STRING 255	
location	SREL loc	Specifies the location of the tenant .
inactive	INTEGER	**1** -- tenant deleted
version number	INTEGER	Specifies the update version of this tenant (incremented whenever tenant is saved).
tenant	UUID (SREL tenant)	Always specifies the same value as the ID
ldap_tenant_group	STRING 512	Specifies the name of the LDAP group that corresponds to this tenant.
subtenants_ok	INTEGER	**1** -- tenant is allowed to have subtenants
fkey_group	UUID (SREL tenant_group)	Specifies the tenant group to which objects that belong to this tenant can reference. Same as the supertenant group. System-maintained (cannot be edited).
supertenant_group	UUID (SREL tenant_group)	Specifies the tenant group that includes the tenant and higher tenants in this hierarchy. Can include the service provider (if in the same hierarchy). System-maintained (cannot be edited).
subtenant_group	UUID (SREL tenant_group)	Specifies the tenant group that includes the tenant and lower tenants in this hierarchy. System-maintained (cannot be edited).
related tenant_group	UUID (SREL tenant_group)	Specifies the tenant group that includes all tenants in this hierarchy (includes the subtenant and supertenant groups). Can include the service provider (if in the same hierarchy). System-maintained (cannot be edited).
tenant_depth	INTEGER	Specifies the number of levels above the tenant in this hierarchy. System-maintained (cannot be edited).
parent	UUID	Specifies the tenant immediately above this tenant in the hierarchy.

Column	Type	Remarks
creation_user	STRING 64	Specifies the user ID of contact who created this tenant.
creation_date	INTEGER	Specifies the date of tenant creation (number of seconds after 0000 hours on 01/01/1970).
last_update_user	STRING 64	Specifies the user ID of contact who last updated this tenant.
last_update_date	INTEGER	Specifies the date of last update (number of seconds after 0000 hours on 01/01/1970).
terms_of_usage	UUID REF ca_tou	Specifies the terms of usage associated with the tenant.

ca_tenant_group Table

This table lists information about a tenant group.

- **SQL Name** -- ca_tenant_group
- **Object** -- tenant_group

Column	Type
id	UUID
name	STRING 255
description	STRING 1024

ca_tenant_group_member Table

This table lists information about a tenant group member.

- **SQL Name** -- ca_tenant_group_member
- **Object** -- tenant_group_member

Column	Type
id	UUID
tenant	SREL tenant
tenant_group	SREL tenant_group

g_tenant Table

Column	Type	Remarks
id	integer	
remote_sys_id	SREL Global_Servers	Required (NOT NULL)

Column	Type	Remarks
remote_id	UUID	Regional tenant id
tenant_name	STRING 255	

Call Request

This article contains the following topics:

Call_Req Table

Integration with call manager.

- **SQL Name** -- call_req
- **Object** -- cr

Field	Data Type	Reference	Remarks
active_flag	INTEGER	Boolean_Table ::enum	Sets the Active flag, as follows:**0** -- Inactive**1** -- Active
affected_rc	byte (16)	ca_owned_resource::uuid	Foreign key to the id field of the ca_owned_resource table. It identifies the asset.
assignee	byte (16)		Foreign key to the contact_uuid field of the ca_contact table. It identifies the assignee.
call_back_date	INTEGER		Specifies the call back timestamp for this request.
call_back_flag	INTEGER		Specifies the call back flag value for this request.
category	nvarchar(30)	Prob_Category ::persid	Foreign key to the persistent_id field of the prob_ctg table. This identifies the category.
change	INTEGER	chg ID	Foreign key to the ID field of the chg table. This is the associated change order.
caused_by_chg	INTEGER	Change_Request	Indicates the change request was caused by another change order.
charge_back_id	nvarchar(12)		Indicates the user-defined string field.

Field	Data Type	Reference	Remarks
close_date	INTEGER		Represents the timestamp of when this request was closed.
cr_tticket	INTEGER		Not used.
created_via	INTEGER	Interface::id	Foreign key to the id field of the interface table. Based on site-defined conditions, this reflects which interface created the request.
customer	byte (16)	ca_contact::uuid	Foreign key to the contact_uuid field of the ca_contact table. This identifies the Affected End User.
description	nvarchar (4000)		This is the textual description of this call request.
event_token	nvarchar(30)		Used by TNGeh_writer for message matching.
external_system_ticket	STRING 4000		
extern_ref	nvarchar(30)		(Deprecated) Specifies the trouble ticket associated with the call request.
group_id	byte (16)		Foreign key to the contact_uuid field of the ca_contact table, this represents the Assigned to Group ID.
id	INTEGER		Specifies the unique (to the table) numeric ID.
impact	INTEGER	Impact::enum	Foreign key to the enum field of the impact table, this identifies the impact of the request.
incident_priority	INTEGER		Specifies the computed incident priority if this is an ITIL incident.
incorrectly_assigned	INTEGER		Indicates that the incident is assigned incorrectly.
last_act_id	nvarchar(12)		Identifies the persid of the last activity.
last_mod_by	byte (16)		Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
log_agent	byte (16)	ca_contact::uuid	Foreign key to the contact_uuid field of the ca_contact table. This identifies who the request was reported by.
macro_predict_viol	INTEGER		Indicates that it is likely to violate its sla (boolean) for action macros to predict sla violations.
major_incident	INTEGER		Identifies the incident as a major incident.
open_date	INTEGER		Identifies the timestamp of when the request was created.

orig_user_admin_org	UUID	ca_organization	
orig_user_cost_center	INTEGER	ca_resource_cost_center	
orig_user_dept	INTEGER	ca_resource_department	
orig_user_organization	UUID	ca_organization	
outage_detail_ what	STRING 4000		Describes the outage details.
outage_detail_ who	STRING 4000		
outage_detail_ why	STRING 4000		Describes why the outage occurred.
outage_reason	INTEGER	Outage_Reason	Identifies the reason for the outage.
outage_type	INTEGER	Outage_Type	Identifies the type of outage.
parent	nvarchar(30)	Call_Req::persid	Foreign key to the persistent_id field of the call_req table to allow for hierarchical request groupings (for example, "parent/child").
pct_service_restored	INTEGER		Represents the percentage of service restored.
persid	nvarchar(30)		Identifies the Persistent ID (SystemObjectName:id).
predicted_sla_viol	INTEGER		Indicates that an sla violation has been predicted by Neugents: **1** -- Request
priority	INTEGER	Priority::enum	Foreign key to the enum field of the pri table, this indicates the priority of the call request.
problem	nvarchar(30)		Foreign key to the persistent_id field of the call_req table to allow for linking this incident to a problem.
ref_num	nvarchar(30)		Shows a visible reference number to the user.
requested_by	UUID	ca_contact	Identifies who requested the ticket.
remote_control_used	INTEGER		Indicates that remote control was used.

Field	Data Type	Reference	Remarks
resolvable_at_lower	INTEGER		Indicates that the ticket was resolved at a lower level.
resolve_date	INTEGER		Indicates the timestamp of when this request was resolved.
return_to_service	INTEGER		Indicates whether service is fully restored.
rootcause	INTEGER	Rootcause::id	Foreign key to the id field of the rootcause table. Specifies the root cause of the request.
sched_token	nvarchar (128)		Specifies the job scheduling token.
severity	INTEGER	Severity:: enum	Foreign key to the enum field of the Severity table, this identifies the severity of the Request.
sla_violation	INTEGER		If defined, this flags the request as follows:Template **1** -- Request has violated its sla
solution	nvarchar(30)	Call_Req:: persid	(Decrecated) Foreign key to the persistent_id field of the crsol table for old request solutions.
status	nvarchar(12)	Cr_Status:: code	Foreign key to the code field of the cr_stat table, this is the status of the problem.
string1	nvarchar(40)		Identifies the user defined string field.
string2	nvarchar(40)		Identifies the user defined string field.
string3	nvarchar(40)		Identifies the user defined string field.
string4	nvarchar(40)		Identifies the user defined string field.
string5	nvarchar(40)		Identifies the user defined string field.
string6	nvarchar(40)		Identifies the user defined string field.
summary	nvarchar (240)		Identifies the summary text.
support_lev	nvarchar(30)	Service_Desc ::code	Foreign key to the code field of the srv_desc table, this defines the Classic Service Type.
symptom_code	INTEGER	Symptom_Code	
template_name	nvarchar(30)	Cr_Template:: template_name	Foreign key to the template_name field of the cr_tpl table, this specifies the name of the request template.
caextwf_instance_id	INTEGER	caextwf_instances	

Field	Data Type	Reference	Remarks
			Indicates the CA Process Automation process instance id and process definition name and reference path launched by this Service Desk object.
tenant	UUID	ca_tenant	
outage_start_ time	LOCAL_TIME		
outage_end_time	LOCAL_TIME		
ticket_ avoided	INTEGER		**0** -- Do not search **10** -- Perform search **20** -- Open knowledge document **30** -- Ticket avoided by self-service
time_spent_sum	INTEGER		Specifies the sum of activity time spent.
type	nvarchar(10)	crt code	Foreign key to the crt table, this is the Request type.
urgency	INTEGER	Urgency:: enum	Foreign key to the enum field of the urgency table, this indicates the call request urgency.
target_start_last	LOCAL_TIME		Time when target timer started or restarted.
target_hold_last	LOCAL_TIME		Time of most recent ticket hold
target_hold_count	INTEGER		Number of times ticket went into a Hold status
target_resolved_last	LOCAL_TIME		Time of most recent ticket resolution
target_resolved_ count	INTEGER		Number of times ticket went into a Resolved status
target_closed_last	LOCAL_TIME		Time ticket was last closed
target_closed_count	INTEGER		Number of times that ticket was closed
affected_service	UUID	ca_owned_ resource	UNIQUE NOT_NULL KEY

Call_Req_Type Table

Stores codes used in Call_Req.type and the detail form names that should be displayed. This is used by the ITIL vertical market customizations to display alternative forms for cr_detail based on the value of Call_Req.type

- **SQL Name** -- crt

- **Object** -- crt

Field	Data Type	Reference	Remarks
code	nvarchar (10)Y		Primary key of this table.
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive/marked as deleted
display_name	nvarchar (30)		The display name value for this Request type.
id	INTEGER		Specifies the unique (to the table) numeric ID.
nx_desc	nvarchar (30)		The description value for this Request type.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
sym	nvarchar (30)		The symbolic value for this Request type.

Call_Solution Table

This table exists in the schema for backward compatibility only. Although there is an interface to it, you should not use this table at all; however, it is important that you not delete it from the schema.

- **SQL Name** -- crsol
- **Object** -- crsol

Field	Data Type	Reference	Remarks
description	STRING 500		Specifies the problem description.
cr_count	INTEGER		Specifies the call request usage count:**0** -- Yes**1** -- No call request usage count
cr_flag	INTEGER		Indicates the call request manager flag used by ITIL code.
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Specifies the status of the Deleted flag:**0** -- Active**1** -- Inactive/marked as deleted.
id	INTEGER UNIQUE NOT_NULL KEY		Indicates the numeric ID that is unique to the table.
in_flag	INTEGER		Specifies the in_flag used by ITIL code.
last_mod_dt	LOCAL_TIME		Indicates the timestamp for when this record was last modified.
nx_desc	STRING 40		Specifies the name for prob_mgr cbox table.
persid	STRING 30		Indicates the Persistent ID:SystemObjectName:id
pr_flag	INTEGER		Specifies the pr_flag used by ITIL code.
	INTEGER		Indicates the status of solution approved.

Field	Data Type	Reference	Remarks
sapproved		Boolean_Table::enum	
sname	STRING 40		Specifies the solution name.
solution	STRING 1000		Specifies the solution description.
sym	STRING 60 NOT_NULL S_KEY		Specifies the symbol for the solution.
tcode	INTEGER		This field is no longer used.

Cr_Call_Timers Table

Call Request call timers. A stop watch with various thresholds that gives the help desk analyst a visual and audio indication of elapsed time.

- **SQL Name** -- crctmr
- **Object** -- ctimer

Field	Data Type	Reference	Remarks
beep	INTEGER		A beep indicator for then the threshold is reached:**0** -- No beep**1** -- Beep
color	STRING 12		Indicates the color of the timer at the start time.
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Specifies the status of the Delete flag: **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		The ID unique (to the table) Numeric ID.
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp for when this record was last modified.
persid	STRING 30		Identifies the Persistent ID (SystemObjectName:id).
text	STRING 240		Identifies the threshold text to display when the timer indicates elapsed time.
threshold	DURATION NOT_NULL		Identifies the threshold elapsed time.

Cr_Status Table

Call Request Status. Lists the states of the call request. May be added to at will. Allows the user to control whether the call request is active or inactive when it is changed to this status.

- **SQL Name** -- cr_stats

- **Object** -- crs

Field	Data Type	Reference	Remarks
active	INTEGER		Sets the Active flag, as follows:**0** -- Inactive**1** -- Active
code	nvarchar (12)		Primary key of this table.
cr_flag	INTEGER		When this flag is set to 1, this status is valid for Requests.
del	INTEGER	Active_Boolean_Table::enum	The Delete flag that indicates the following:**0** -- Active**1** -- Inactive/marked as deleted
description	nvarchar (500)		Identifies the textual description of the status.
hold	INTEGER		Sets the Hold flag, as follows:**0** -- Start events**1** -- Stop events
id	INTEGER		Unique (to the table) numeric ID.
in_flag	INTEGER		When this flag is set to 1, the status is valid for Incidents.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
pr_flag	INTEGER		When this flag set to 1, the status is valid for Problems.
resolved	INTEGER		Flag that indicates the following:**0** -- Not yet resolved**1** -- Resolved
sym	nvarchar (30)		Identifies the symbol of the Request status name.

Cr_Stored_Queries Table

Custom bin stored queries. System administrators may add to this table at will. Determines which queries may be used by help desk analysts to customize their scoreboard.

- **SQL Name** -- crsq
- **Object** -- crsq

Field	Data Type	Reference	Remarks
description	STRING 240		Specifies the textual description of this stored query.
code	STRING 12 UNIQUE NOT_NULL S_KEY		Specifies the non-editable handle for the query.

Field	Data Type	Reference	Remarks
count_url	STRING 240		Specifies the URL for counts, if obj_type=url.
criteria	STRING 240		Specifies the where clause for querying.
del	INTEGER NOT_NULL	Active_Boolean_ Table::enum	The deleted flag **0** -- active **1** -- inactive/marked as deleted)
id	INTEGER UNIQUE NOT_NULL KEY		Specifies the key (to the table) Numeric ID.
label	STRING 80		Specifies the label to display on the scoreboard.
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp for when this record was last modified.
obj_type	STRING 30		Indicates the scoreboard, with the capability of having enough space to allow for expansions to accommodate the cr, tt, ir, and chg types.
persid	STRING 30		The Persistent ID (SystemObjectName:id).

Cr_Template Table

Request Template Table maps a template name to a Call_Req that will be used as a template.

- **SQL Name** -- cr_template
- **Object** -- cr_tpl

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_ Table::enum	The Delete flag that indicates the following:**0** -- Active**1** -- Inactive/marked as deleted
description	nvarchar (1000)		Shows the description of the template.
id	INTEGER		Identifies the nique (to the table) numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
quick_tmpl_type	INTEGER	Quick_Template_ Types::enum	Flag that indicates the following:**1** -- Quick tmpl**2** -- Quick tmpl+review
template		Call_Req::persid	Persistent ID (SystemObjectName:id).

Field	Data Type Reference	Remarks
	nvarchar (30)	
template_class	nvarchar (12)	Indicates to allow subclassing templates.
template_name	nvarchar (30)	Identifies the unique name of the template.

cr_trans Table

A transition object controls the current and next ticket status. The cr_trans table lists the status, new status, and actions that need to occur for a default transition.

- **SQL Name** -- cr_trans
- **Object** -- cr_trans

Label	Field	Description
id	INTEGER	Unique key.
status	SYMBOL	Specifies the current ticket status.
new_status	SYMBOL	Specifies the new ticket status
must_comment	INTEGER	Comment required when using a transition. On new default: 0
is_default	INTEGER	Default transition that appears when the Status field is empty. On new default: 0
condition	BOP_REF_STR_REF Macro	Site condition macro to approve transition.
condition error	STRING 255	Error message for site condition.
description	STRING 255	Description of this transition.
last_mod_dt	LOCAL_TIME	Timestamp of last update to this record.
last_mod_by	UUID REF ca_contact	User who last updated this.
del	INTEGER nn	Logical database delete status.
tenant	UUID REF ca_tenant	Reference to Tenant information.

Knowledge Management Tables

This article contains the following topics:

CI_ACTIONS Table

Program control table used by Knowledge Management.

- **SQL Name** -- CI_ACTIONS
- **Object** -- CI_ACTIONS

Field	Data Type	Reference	Remarks
ACTION_ORDER	INTEGER		
ACTION_TITLE	STRING 100		
ANALYST_ID	UUID	ca_contact::uuid	
GROUP_ID	UUID	ca_contact::uuid	
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
PREDEFINED	INTEGER		
STATUS_CURRENT_ID	INTEGER	CI_STATUSES::id	
UNPUBLISH	INTEGER		
UNRETIRE	INTEGER		
WF_TEMPLATE_ID	INTEGER	CI_WF_TEMPLATES ::id	

CI_ACTIONS_ALTERNATE Table

Program control table used by Knowledge Management.

- **SQL Name** -- CI_ACTIONS_ALTERNATE
- **Object** -- CI_ACTIONS_ALTERNATE

Field	Data Type	Reference	Remarks
ACTION_ID	INTEGER	CI_ACTIONS::id	
CONTACT_ID	UUID	ca_contact::uuid	
CONTACT_TYPE	INTEGER		
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.

CI_BOOKMARKS Table

Program control table used by Knowledge Management.

- **SQL Name** -- CI_BOOKMARKS
- **Object** -- CI_BOOKMARKS

Field	Data Type	Reference	Remarks
BOOKMARK_TITLE	STRING 100		
DOCUMENT_ID	INTEGER	SKELETONS::id	
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
USER_ID	UUID	ca_contact::uuid	

CI_DOC_LINKS Table

Program control table used by Knowledge Management.

- **SQL Name** -- CI_DOC_LINKS
- **Object** -- CI_DOC_LINKS

Field	Data Type	Reference	Remarks
DOC_ID1	INTEGER	SKELETONS::id	Specifies the parent ID.
DOC_ID2	INTEGER	SKELETONS::id	Specifies the child ID.
id	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
parent_child	INTEGER		Indicates the document has one of the following relationships with another document: **0** -- See also link **1** -- Parent Child Link
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

CI_DOC_TEMPLATES Table

Program control table used by Knowledge Management.

- **SQL Name** -- CI_DOC_TEMPLATES
- **Object** -- CI_DOC_TEMPLATES

Field	Data Type	Remarks
ID	INTEGER NOT_NULL KEY	Unique (to the table) Numeric ID
IS_DEFAULT	INTEGER	
IS_PREDEFINED	INTEGER	
KD ID	Long	Knowledge Document id that is used as a template for default values.
LAST_MOD_DT	LOCAL_TIME	Indicates the timestamp of when this record was last modified.
PAGE_HTML	STRING 32768	
TEMPLATE_NAME	STRING 255	

CI_DOC_TYPES Table

Program control table used by Knowledge Management.

- **SQL Name** -- CI_DOC_TYPES
- **Object** -- CI_DOC_TYPES

Field	Data Type	Reference	Remarks
DOC_TYPE_TXT	STRING 50		
ID	INTEGER KEY		Unique (to the table) Numeric ID
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.

CI_PRIORITIES Table

Program control table used by Knowledge Management.

- **SQL Name** -- CI_PRIORITIES
- **Object** -- CI_PRIORITIES

Field	Data Type	Reference	Remarks
ID	INTEGER KEY		Unique (to the table) Numeric ID
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
PRIORITY	STRING 50		

CI_STATUSES Table

Program control table used by Knowledge Management.

- **SQL Name** -- CI_STATUSES
- **Object** -- CI_STATUSES

Field	Data Type	Reference	Remarks
ID	INTEGER KEY		Unique (to the table) Numeric ID
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
PREDEFINED	INTEGER		
STATUS	STRING 50		
STATUS_DESCRIPTION	STRING 255		
STATUS_ORDER	INTEGER		

CI_WF_TEMPLATES Table

Program control table used by Knowledge Management.

- **SQL Name** -- CI_WF_TEMPLATES
- **Object** -- CI_WF_TEMPLATES

Field	Data Type	Reference	Remarks
ID	INTEGER KEY		Unique (to the table) Numeric ID
IS_DEFAULT	INTEGER		
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
WF_DESCRIPTION	STRING 255		
WF_NAME	STRING 255		

Doc_Versions Table

Program control table used by CA SDM Knowledge Management.

- **SQL Name** -- DOC_VERSIONS
- **Object** -- DOC_VERSIONS

Field	Data Type	Reference	Remarks
ID	INTEGER		Specifies the primary key.
doc_ID	INTEGER	skeletons::id	Specifies the SREL to the knowledge document object.
ver_count	INTEGER		Specifies the internal version ID that indicates the number of versions created (1, 2, 3, 4...)
ver_comment	STRING (2000)		Specifies the comment text.
start_date	DATE		Specifies the date when this version started.
end_date	DATE		Specifies the date when this version ended.
started_by	UUID		Specifies the user that created this version.
published_by	UUID		Specifies the user that published this version.
status_ID	INTEGER		Specifies the document version status.
ver_status	INTEGER		Specifies the previous version's status: **0** -- Existed **1** -- Archived **2** -- Deleted (this only relates to the resolution field)
title	STRING		Specifies the document version title.
summary	STRING		Specifies the document summary text.
problem	STRING		Specifies the problem description.
notes	STRING		Specifies the document notes.
doc_type_ID	INTEGER		Specifies the document type.
ext_doc_ID	INTEGER		Specifies the Tree ID when Decision Tree is used.
last_mod_by	Byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.

EBR_ACRONYMS Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_ACRONYMS
- **Object** -- EBR_ACRONYMS

Field	Data Type	Reference	Remarks
ACRONYM	STRING 50		

Field	Data Type	Reference	Remarks
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
LAST_MOD_ DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.

EBR_KEYWORDS Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_KEYWORDS
- **Object** -- EBR_KEYWORDS

Field	Data Type	Reference	Remarks
ENTITY_ID	INTEGER		
EXT_TABLE_ID	INTEGER		
FULL_WORD	STRING 50		
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID

EBR_LOG Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_LOG
- **Object** -- EBR_LOG

Field	Data Type	Reference	Remarks
ASKED_DATE	LOCAL_TIME		
BEST_IDS	STRING 110		
EXTERNAL_ID	STRING 50		
FILTER_DATA	STRING 32768		
FUZZINESS	INTEGER		
ID	INTEGER KEY		Unique (to the table) Numeric ID
KEYWORDS	STRING 32768		
MATCH_TYPE	INTEGER		
METHOD_ PERFORMANCE	INTEGER		
METHOD_TYPE	INTEGER		
NUM_MATCHES	INTEGER		
ORDER_DIRECTION	INTEGER		
PRIMARY_ORDER	STRING 50		
ROWS_FOUND	INTEGER		

Field	Data Type	Reference	Remarks
ROWS_TO_FETCH	INTEGER		
SEARCH_IN	INTEGER		
SEARCH_QUALITY	INTEGER		
SEARCH_TEXT	STRING 255		
SEARCH_TYPE	INTEGER		
SECONDARY_ORDER	INTEGER		
SESSION_ID	INTEGER		
SQL_TEXT	STRING 32768		
TOP_MATCH_ID	INTEGER		
UNIQUE_WORD_COUNT	INTEGER		
USER_ID	STRING 100		
WORD_COUNT	INTEGER		

EBR_METRICS Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_METRICS
- **Object** -- EBR_METRICS

Field	Data Type	Reference	Remarks
COMMENTS	STRING 255		
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
METRIC	STRING 50		
WEIGHT	REAL		

EBR_NOISE_WORDS Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_NOISE_WORDS
- **Object** -- EBR_NOISE_WORDS

Field	Data Type	Reference	Remarks
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
NOISE_WORD	STRING 50		

EBR_PATTERNS Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_PATTERNS
- **Object** -- EBR_PATTERNS

Field	Data Type	Reference	Remarks
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
PATTERN_DEFAULT	STRING 255		
PATTERN_NAME	STRING 50		
PATTERN_VALUE	STRING 255		
PATTERN_VALUE_ADM	STRING 255		

EBR_PREFIXES Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_PREFIXES
- **Object** -- EBR_PREFIXES

Field	Data Type	Reference	Remarks
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
PREFIX	STRING 50		

EBR_PROPERTIES Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_PROPERTIES
- **Object** -- EBR_PROPERTIES

Field	Data Type	Reference	Remarks
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
PROPERTY_ADMIN	INTEGER		
PROPERTY_DEFAULT	STRING 50		
PROPERTY_NAME	STRING 50 S_KEY		
PROPERTY_TYPE	STRING 50		
PROPERTY_VALUE	STRING 32768		
PROPERTY_VALUE_ADM	STRING 32768		

EBR_SUBSTITS Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_SUBSTITS
- **Object** -- EBR_SUBSTITS

Field	Data Type	Reference	Remarks
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
SYMBOL1	STRING 50		
SYMBOL2	STRING 50		

ES_CONSTANTS Table

Program control table used by Knowledge Management.

- **SQL Name** -- ES_CONSTANTS
- **Object** -- ES_CONSTANTS

Field	Data Type	Reference	Remarks
COMMENTS	STRING 255		
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
LAST_MOD_ DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
NAME	STRING 50		Specifies the text name of this item.
PROPERTYID	INTEGER		
PROPVALUE	INTEGER		

ES_NODES Table

Program control table used by CA SDM Knowledge Management.

- **SQL Name** -- ES_NODES
- **Object** -- ES_NODES

Field	Data Type	Reference	Remarks
DISPLAYED_ TEXT	STRING 32768		
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
LAST_MOD_ DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
LINK_ID	INTEGER		

Field	Data Type	Reference	Remarks
		ES_NODES: :id	
NODE_ID	INTEGER		
NODE_SHORT_DESC	STRING 150		
NODE_TYPE	INTEGER		
PARENT_ NODE_ID	INTEGER		
QUERY_RESP_NUMBER	INTEGER		
QUERY_RESP_TYPE	STRING 50		
RESPLINKID1	INTEGER		
RESPLINKID2	INTEGER		
RESPLINKID3	INTEGER		
RESPLINKID4	INTEGER		
RESPLINKID5	INTEGER		
RESPLINKID6	INTEGER		
RESPLINKID7	INTEGER		
RESPONSE1	STRING 100		
RESPONSE2	STRING 100		
RESPONSE3	STRING 100		
RESPONSE4	STRING 100		
RESPONSE5	STRING 100		
RESPONSE6	STRING 100		
RESPONSE7	STRING 100		
ROOT_ID	INTEGER	ES_NODES: :id	
TREE_ID	INTEGER	SKELETONS ::id	

ES_RESPONSES Table

Program control table used by Knowledge Management.

- **SQL Name** -- ES_RESPONSES
- **Object** -- ES_RESPONSES

Field	Data Type	Reference	Remarks
ID			Unique (to the table) Numeric ID

Field	Data Type	Reference	Remarks
	INTEGER NOT_NULL KEY		
LAST_MOD_ DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
PARENT_ NODE_ID	INTEGER	ES_NODES ::id	
RESPONSE_ LINK_ID	INTEGER	ES_NODES ::id	
RESPONSE_ LINK_ORDER	INTEGER		
RESPONSE_ LINK_TEXT	STRING 100		

ES_SESSIONS Table

Program control table used by Knowledge Management.

- **SQL Name** -- ES_SESSIONS
- **Object** -- ES_SESSIONS

Field	Data Type	Reference	Remarks
COMMENT_T EXT	STRING 50		
EVALUATION	INTEGER		
EXTERNAL_ID	STRING 50		
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
LAST_MOD_D T	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
PATH_IDS	STRING 50		
PATH_QAS	STRING 32768		
SESSION_ID	INTEGER		
TREE_ID	INTEGER	ES_NODES: :id	

Index_Doc_Links Table

Program control table used by Knowledge Management.

- **SQL Name** -- index_doc_links
- **Object** -- index_doc_links

Field	Data Type	Reference	Remarks
DOC_ID	INTEGER	SKELETONS::id	
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
INDEX_ID	INTEGER	O_INDEXES::id	
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
RELATIONAL_ID	STRING 255		

KD_Atmnt Table

Program control table used by Knowledge Management.

- **SQL Name** -- kd_attmnt
- **Object** -- kd_attmn

Field	Data Type	Reference	Remarks
ATTMNT_ID	INTEGER	Attachment::id	
DOC_ID	INTEGER	SKELETONS::id	
ID	INTEGER KEY		Unique (to the table) Numeric ID
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
RES_ID	Long		If there is an embedded image, the RES_ID points to the resource file id in the attmnt table.

Knowledge_Keywords Table

Knowledge Base key words for associating trouble codes and call areas to solutions.

- **SQL Name** -- km_kword
- **Object** -- kwrd

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.

Field	Data Type	Reference	Remarks
persid	STRING 30		Persistent ID (SystemObjectName:id)
sym	STRING 30 NOT_NULL S_KEY		keyword

kdlinks Table

Each record indicates a link between a KD and request or issues link_type field represented by the following enum value:

1 = KD is a solution to the ticket

2 = Ticket created is based on the document last_mod_by the person that links the document and the ticket

- **SQL Name** -- kdlinks
- **Object** -- kdlinks

Field	Data Type	Reference	Remarks
cr	STRING 30	Call_Req:: persid	
ID	INTEGER KEY		Specifies the Numeric ID that is unique to this table.
iss	STRING 30	Issue	
kd	INTEGER	SKELETONS::id	
last_mod_by	UUID	ca_contact:: uuid	Specifies the UUID of the contact who last modified this record.
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp for when this record was last modified.
link_type	INTEGER		
sd_obj_id	INTEGER		
sd_obj_type	STRING 5		

KEIT_TEMPLATES Table

Field Name	Type	Index	Comment
ID	Int	Primary Key	
TEMPLATE_NAME	Text (50)		
EXP_SUB_CAT	int		Indicates a flag to export sub categories: **0** -- No **1** -- Yes
EXP_SEC_CAT	int		

Field Name	Type	Index	Comment
			Indicates a flag to export secondary categories **0** -- No **1** -- Yes
EXP_ALL_DOCS	int		Indicates a flag to export all documents linked to the selected category **0** -- No **1** -- Yes
EXP_FILTER	Text (2048)		Additional Filter for export
EXP_ATTMNT	int		Indicates a flag to export attachments **0** -- No **1** -- Yes
EXP_INDEX_DOC	int		Indicates a flag to Index documents after import **0** -- No **1** -- Yes
OVERRIDE_PUB	int		Indicates a flag to override published documents **0** -- No **1** -- Yes
OVERRIDE_UNPUB			Indicates a flag to override unpublished documents **0** -- No **1** -- Yes
OVERRIDE_DEFAULTS			Use the default values when overriding documents
ERR_THRESHOLD	int		Error threshold for stopping the process
FIELD_LIST	Text		List of fields to export
CAT_LIST	Text		List of categories to export
DEFAULT_LIST	Text		List of fields, their types and values used as defaults on import
STATUS_ID and following fields			Used internally to fulfill the DEFAULT_LIST field
last_mod_by	UUID		
last_mod_dt	Long		

KT_act_content Table

The kt_act_content table is used for action content links.

Field	Data Type	Remarks
Id	Long	id
Name	String	Name of the action content.
Code	String (10)	Action content code - Rel_attr
Description	String	Description of the action content
URL	String	URL of the action content
HTMPL	String	Parameters for the HTMPL URL

KT_Blc Table

Program control table used by Knowledge Management to store the best link conditions data for the Recommended Documents feature.

- **SQL Name** -- kt_blc
- **Object** -- kt_blc

Field	Data Type	Reference	Remarks
ID	INTEGER		Primary key.
KD	INTEGER		SREL to the knowledge document object.
Kcat	INTEGER		SREL to knowledge category for recommended document condition type of 4.
BLC_Type	INTEGER		SREL to recommended document condition type.
BLC_Text	STRING 255		The recommended document condition term.
Author_ID	UUID		SREL to cnt
Del	INTEGER	Active_Boolean _Table:: enum	Specifies the status of the Deleted flag: **0** -- Active **1** -- Inactive/marked as deleted
Last_mod_dt	DATE		Shows the date of when this record was last updated.

KT_Blc_Type Table

Program control table used by Knowledge Management to store the Best Link Condition types for the Recommended Documents feature.

- **SQL Name** -- kt_blc_type
- **Object** -- kt_blc_type

Field	Data Type	Reference	Remarks
ID	INTEGER		Primary key.
SYM	STRING 50		**1** -- Full Match **2** -- Exact Match **3** -- Keyword List **4** -- Knowledge Category
BLC_Condition	STRING 255		Category path if BLC type is category; otherwise, BLC text is used.
Last_mod_dt	DATE		Shows the date of when this record was last updated.

KT_Flg_Status Table

Identifies the different flag statuses used by the Automated Policies feature.

- **SQL Name** -- kt_flg_status
- **Object** -- kt_flg_status

Field	Data Type	Reference	Remarks
ID	INTEGER		Identifies the unique (to the table) numeric ID.
sym	STRING (50)		Flag type name.

KT_Flg_Type Table

Identifies the different flags types used by the Automated Policies feature to flag documents for correction.

- **SQL Name** -- kt_flg_type
- **Object** -- kt_flg_type

Field	Data Type	Reference	Remarks
ID	INTEGER		Identifies the unique (to the table) numeric ID.
sym	STRING (50)		Flag type name.
description	STRING (2000)		Flag type description.
init_by_users	INTEGER (1/0)		Specifies the flag type users select in the end user interface.
show_as_comment	INTEGER (1/0)		Displays the flag type as a comment when document is open for viewing.
follow_up	INTEGER (1/0)		Raises follow-up mechanism for the flag type.
time_to_complete	INTEGER		Specifies the time from which the argument is completed.
dev_assignee	UUID		For future use.
del	INTEGER		Specifies if the flag type is active or inactive.
last_mod_by	UUID	SREL to the Contacts table.	Displays the last date of when a user modified the record.
last_mod_dt	Long (date)		Displays the last modified date.

KT_Life_Cycle_Rep Table

Identifies the knowledge document life cycle data for the Automated Policies feature in Knowledge Management.

- **SQL Name** -- KT_Life_Cycle_Rep
- **Object** -- KT_Life_Cycle_Rep

Field	Data Type	Reference	Remarks
ID	Long	Primary index.	Identifies the unique (to the table) numeric ID of the primary index.
policy	Long	Required field. SREL to query_policy.	Identifies the Policy ID.
kd	Long	Required field. SREL to the knowledge document (Skeletons table).	Identifies the Document ID.
last_mod_dt	Long (date)		Displays the last modified date.

KT_REPORT_CARD Table

Program control table used by Knowledge Management.

- **SQL Name** -- kt_report_card
- **Object** -- kt_report_card

Field	Data Type	Reference	Remarks
ID	INTEGER		KEY Unique (to the table) Numeric ID
SUBJECT_ID	nvarchar(64)		
PAST_DAYS	INTEGER		
ORG_STATISTICS	INTEGER		
DOCUMENTS_SUBMITTED	INTEGER		
DOCUMENTS_PUBLISHED	INTEGER		
TOTAL_HITS	INTEGER		
AVERAGE_EFFECTIVENESS_RATING	INTEGER		

Field	Data Type	Reference	Remarks
TOTAL_SOLUTION_ COUNT	INTEGER		
USER_SLV_CNT	INTEGER		
TOTAL_VOTES	INTEGER		
AVG_RATING	REAL		
LINKED_ KNOWLEDGE_BY_ OTHERS	INTEGER		
LINKED_ KNOWLEDGE_BY_ME	INTEGER		
CLOSED_TICKETS	INTEGER		
TICKETS_WITH KNOWLEDGE	INTEGER		
TICKETS_HAD_ SEARCH_ ACTIVITES	INTEGER		
KNOWLEDGE_ SUBMIT_FROM_ TICKET	INTEGER		
TIME_TO_PUBLISH	INTEGER		
MY_COMMENTS	INTEGER		
DOCUMENTS_ RETIRED	INTEGER		
TIME_TO_FIX	INTEGER		
FLAGS_FIXED	INTEGER		
COMMENTS_ON_ MY_DOCUMENTS	INTEGER		
FIRST_CALL_RES_ WITH_KNOW	INTEGER		
FIRST_CALL_RES_ WITHOUT_KNOW	INTEGER		
creation_user	nvarchar(64)		Specifies the name of the person who created this record. Should be in form: LastName, FirstName
creation_date	INTEGER		Indicates the timestamp indicating when this record was created
last_update_user			

Field	Data Type	Reference	Remarks
	nvarchar(64)		Specifies the contact who last modified this record. Should be in form: LastName, FirstName
last_update_date	INTEGER		Indicates the timestamp of when this record was last modified
CONTRIBUTOR_ UUID	SREL	cnt	TENANCY_ UNRESTRICTED
IS_SUPERVISOR	INTEGER		
SUPERVISOR_ UUID	SREL	cnt	TENANCY_ UNRESTRICTED
MY_ORG_REF_ID	SREL	KT_REPORT_ CARD	
ALL_ORG_REF_ID	SREL	KT_REPORT_ CARD	
PAST_DAYS_TEXT	nvarchar(20)		Populates from the resource file.
LAST_MOD_DT_ TEXT	nvarchar(50)		Specifies the KRC calculation date.
DOCUMENTS_ PUBLISHED_ PERCENT	nvarchar(4)		
AVG_HITS	nvarchar(20)		
AVG_RATING_ TEXT	nvarchar(100)		
last_mod_by	SREL	cnt	
last_mod_dt	DATE		

O_INDEXES Table

Program control table used by Knowledge Management.

- **SQL Name** -- O_INDEXES
- **Object** -- KCAT

Field	Data Type	Reference	Remarks
DESCRIPTION	STRING 255		Textual description
AUTHOR_ID	UUID	ca_contact::uuid	
CAPTION	STRING 50		
CR_CAT	STRING 30	Prob_Category	
DOC_TEMPLATE	INTEGER		

Field	Data Type	Reference	Remarks
		CI_DOC_ TEMPLATES::id	
HAS_CHILDREN	INTEGER		
HAS_DOCS	INTEGER		
ID	INTEGER KEY		Unique (to the table) Numeric ID
iSS_CAT	STRING 30	Issue_Category	
KEYWORDS	STRING 255		
LAST_MOD_BY	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
LAST_MOD_DT	LOCAL_TI ME		Indicates the timestamp of when this record was last modified
OWNER_ID	UUID	ca_contact::uuid	
PARENT_ID	SREL	O_INDEXES::id	
PERMISSION_INDE X_ ID	INTEGER	O_INDEXES::id	
READ_PGROUP	INTEGER	P_GROUPS::id	
RELATIONAL_ID	STRING 255		
SUBJECT_EXPERT_ ID	UUID	ca_contact::uuid	
WF_TEMPLATE	INTEGER	CI_WF_ TEMPLATES::id	
WRITE_PGROUP	INTEGER	P_GROUPS::id	

Program control table used by CA SDM Knowledge Management.

- **SQL Name** -- KD
- **Object** -- Skeletons

Field	Data Type	Reference	Remarks
Active_st ate	INTEG ER		
Active_st ate_date	LOCAL _TIME		
assignee _ID	UUID	ca_contac t::uuid	
author_I D	UUID	ca_contac t::uuid	

Field	Data Type	Reference	Remarks
bu_result	REAL		
created_via	INTEGER		
creation_date	LOCAL_TIME		Indicates the timestamp when this record was created.
current_action_ID	INTEGER	ci_actions::id	
custom1	STRING 50		
custom2	STRING 50		
custom3	STRING 50		
custom4	STRING 255		
custom5	STRING 255		
custom_num1	REAL		
custom_num2	REAL		
doc_template_ID	INTEGER	ci_doc_templates :: id	
doc_type_ID	INTEGER	ci_doc_types::id	
doc_version	STRING 50		
expiration_date	LOCAL_TIME		
expire_notification_sent	INTEGER		
ext_doc_ID	INTEGER		
flg_cnt	INTEGER		Number of open flags in the KD.
fullwords	STRING 32768		
hits	INTEGER		

Field	Data Type	Reference	Remarks
ID	INTEGER KEY		Identifies the unique (to the table) numeric ID.
indexed	INTEGER		
inherit_permission	INTEGER		
initiator	STRING 100		
initiator_ID	UUID	ca_contact::uuid	
KD_permission_index_ID	INTEGER	o_indexes::id	
last_accepted_date	LOCAL_TIME		
last_hit_date	INTEGER (DATE)		Specifies the last hit date created.
last_mod_dt	LOCAL_TIME		Indicates the timestamp when this record was last modified.
last_vote_date	INTEGER (DATE)		Specifies the last vote date presented in the Knowledge Report Card interface.
locked_by_ID	UUID	ca_contact::uuid	
modify_date	LOCAL_TIME		
notes	STRING 32768		
owner_ID	UUID	ca_contact::uuid	
parent_cr	STRING 30	call_req::persid	
parent_iss	STRING 30	issue persistent_id	
primary_index	INTEGER	o_indexes::id	

Field	Data Type	Reference	Remarks
priority_ID	INTEGER	ci_properties::id	
PROBLEM	STRING 32768		
published_date	LOCAL_TIME		
read_pgroup	INTEGER	p_groups::id	
resolution	STRING 32768		
resolution_length	INTEGER		
resolution_short	STRING 255		
review_date	LOCAL_TIME		
rework_ver	INTEGER (1/0)		**0** -- Specifies all available knowledge document version records. **1** -- Specifies a rework version record.
sd_accepted_hits	INTEGER		
sd_asset_ID	UUID	ca_owned_resource::uuid	
sd_impact_ID	INTEGER	impact::enum	
sd_priority_ID	INTEGER	priority::enum	
sd_problem	STRING		Problem persid
sd_product_ID	INTEGER	Product::id	
sd_rootcause_ID	INTEGER	rootcause::id	
sd_severity_ID	INTEGER	severity::enum	
sd_urgency_ID	INTEGER	urgency::enum	
shortwords			

Field	Data Type	Reference	Remarks
	STRING 32768		
skip_auto_policies	INTEGER (4) (1/0)		Boolean (1/0) field to indicate if the automated policies should skip a knowledge document.
status_ID	INTEGER	ci_statuses::id	
subject_expert_ID	UUID	ca_contact::uuid	
summary	STRING 255		
ticket_avoided	INTEGER		Specifies the counter field to update in the Customer/Employee interface when the user accepts a document as a solution to a request /incident/problem during the self-service process.
title	STRING 255		
user_def_ID	STRING 40		
user_slv_cnt	INTEGER		
vote_count	INTEGER		
avg_rating	FLOAT		
faq_sym	INTEGER		
ver_comment	STRING 1000		Comment logged when the rework (new) version was created
ver_count	INTEGER		Specifies the version ID for the number of versions created (1, 2, 3, 4...).
ver_cross_ref_ID	INTEGER		Specifies a cross-reference between the published document record and the new version record.
wf_template	INTEGER	ci_wf_templates :: id	
word_count_total	INTEGER		
wordcount	INTEGER		
wordcounts			

Field	Data Type	Reference	Remarks
	STRING 32768		
wordorders	STRING 32768		
wordplace	STRING 32768		
wordspans	STRING 32768		
write_pgroup	INTEGER	p_groups::id	

LONG_TEXTS

Program control table used by CA SDM Knowledge Management.

- **SQL Name** -- long_texts
- **Object** -- long_texts

Field	Data Type	Reference	Remarks
ACTUAL_TEXT	STRING 32768		
CNT_ORDER	INTEGER		
ID	INTEGER KEY		Unique (to the table) Numeric ID
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
REF_PERSID	STRING 30		

P_Groups Table

Program control table used by Knowledge Management.

- **SQL Name** -- P_GROUPS
- **Object** -- P_GROUPS

Field	Data Type	Reference	Remarks
GRP_LIST	STRING 4096		
GRP_LIST_KEY	STRING 255		

Field	Data Type	Reference	Remarks
TYPE	INTEGER		Indicates if the P Groups is based on Roles or Groups: **1** -- Groups (Default) **2** -- Roles
ID	INTEGER KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

Doc_Versions

Program control table used by CA SDM Knowledge Management.

- **SQL Name** -- DOC_VERSIONS
- **Object** -- DOC_VERSIONS

Field	Data Type	Reference	Remarks
ID	INTEGER		Specifies the primary key.
doc_ID	INTEGER	skeletons::id	Specifies the SREL to the knowledge document object.
ver_count	INTEGER		Specifies the internal version ID that indicates the number of versions created (1, 2, 3, 4...)
ver_comment	STRING (2000)		Specifies the comment text.
start_date	DATE		Specifies the date when this version started.
end_date	DATE		Specifies the date when this version ended.
started_by	UUID		Specifies the user that created this version.
published_by	UUID		Specifies the user that published this version.
status_ID	INTEGER		Specifies the document version status.
ver_status	INTEGER		Specifies the previous version's status: **0** -- Existed **1** -- Archived **2** -- Deleted (this only relates to the resolution field)
title	STRING		Specifies the document version title.
summary	STRING		Specifies the document summary text.
problem	STRING		Specifies the problem description.
notes	STRING		Specifies the document notes.

Field	Data Type	Reference	Remarks
doc_type_ID	INTEGER		Specifies the document type.
ext_doc_ID	INTEGER		Specifies the Tree ID when Decision Tree is used.
last_mod_by	Byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.

KD_Atmnt Table

Program control table used by Knowledge Management.

- **SQL Name** -- kd_attmnt
- **Object** -- kd_attmn

Field	Data Type	Reference	Remarks
ATTMNT_ID	INTEGER	Attachment::id	
DOC_ID	INTEGER	SKELETONS::id	
ID	INTEGER KEY		Unique (to the table) Numeric ID
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
RES_ID	Long		If there is an embedded image, the RES_ID points to the resource file id in the attmnt table.

Change Request

This article contains the following topics:

Change_Act_Log Table

Change manager tables Change_Act_Log is a history of activities associated with a change request. The types of activities are listed in the Act_Type table.

- **SQL Name** -- chgalg

- **Object** -- chgalg

Field	Data Type	Reference	Remarks
action_desc	nvarchar (4000)		Shows the text description of the activity log entry.
analyst	byte(16)	ca_contact::uuid	Foreign key to the contact_uuid field of the ca_contact table. This is the Analyst who created this activity log.
change_id	INTEGER	chg id	Foreign key to the id field of the chg table to which the activity log belongs. This is a Change Order.
description	nvarchar (4000)		Textual description of this activity log
id	INTEGER		Unique numeric ID that is the Primary key of this table.
internal	INTEGER		Marks this as 'Internal' log.
knowledge_session	nvarchar (80)		The knowledge session value for this Change_Act_Log.
knowledge_tool	nvarchar (12)		The knowledge management tool value for this Change_Act_Log.
last_mod_dt	INTEGER		Specifies the date of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
system_time	INTEGER		Specifies the date and time of record creation.
time_spent	INTEGER		Specifies the time spent by the user on the activity.
time_stamp	INTEGER		Specifies the date and time time of activity by the user.
type	nvarchar (12)	Act_Type::code	Identifies the Activity log type.Note: This is the Foreign key to the code field of the act_type table.

Change_Category Table

Change Request categories can be hierarchical.

- **SQL Name** -- chgcat
- **Object** -- chgcat

Field	Data Type	Reference	Remarks
id	INTEGER		Specifies the unique (to the table) numeric ID.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id)

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Delete flag that indicates the following:**0** -- Active**1** -- Inactive /marked as deleted
sym	STRING (1000)	S_KEY	REQUIRED Change Category symbolic description.
code	STRING (12)	S_KEY	Primary key of this table.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
last_mod_by	byte (16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
description	nvarchar (500)		Identifies the textual description of this change category.
organization	byte (16)	ca_organization::organization_uuid	Foreign key to the id field of the ca_organization table, this is the Organization.
assignee	byte (16)	ca_contact	Foreign key to the contact_uuid field of the ca_contact table, this is the Assignee.
group_id	byte (16)	ca_contact	Foreign key to the contact_uuid field of the ca_contact table. This is the Group.
children_ok	INTEGER		Specifies the handling of the change category:**0** -- Children not allowed**1** -- Children are allowed
service_type	STRING (30)	Service_Desc	
survey	INTEGER	Survey_Template	
schedule	INTEGER	Bop_Workshift	Deprecated.
auto_assign	INTEGER		Flag that enables auto assignment.
owning_contract	INTEGER	Service_Contract	Foreign key to the id field of the svc_contract table.This is the Service Contract.
flow_flag	INTEGER		Specifies the type of workflow: **0** -- Classic Workflow or none (default) **2** -- CA Process Automation
caextwf_start_id	INTEGER	caextwf_start_forms	Identifies the CA Process Automation process definition information to use when the user selects this category on a change order, issue, request.
tenant	UUID	ca_tenant	
chgtype	INTEGER	usp_change_type	

Field	Data Type	Reference	Remarks
risk_survey	INTEGER	Risk_Survey_Template	
cab	UUID	ca_contact	Reference to Contact information.
ss_include	INTEGER		REQUIRED On new default: 0
ss_sym	STRING (128)		

Change_Request Table

Change requests.

- **SQL Name** -- chg
- **Object** -- chg

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE NOT_NULL KEY		Primary key of this table, this is a unique numeric ID.
persid	STRING 30		Specifies the Persistent ID (SystemObjectName:id).
chg_ref_num	STRING 30 UNIQUE NOT_NULL S_KEY;		Shows a User visible reference number.
summary	STRING 240		Identifies the Change Order summary text.
description	STRING 4000		Provides a textual description of this Change Order.
status	STRING 12	Change_Status	Foreign key to the code field of the chgstat table, this identifies the Status.
active_flag	INTEGER NOT_NULL	Boolean_Table::benum	Flag representing whether this record is active or inactive: **0** -- Inactive **1** -- Active
start_date	LOCAL_TIME		Indicates the timestamp of when processing started.
open_date	LOCAL_TIME		Shows the timestamp of when this Change Order was created.
last_mod_dt	LOCAL_TIME		Identifies the timestamp of when this record was last modified.
last_mod_by	UUID REF	ca_contact	Specifies the UUID of the contact who last modified this record.
close_date	LOCAL_TIME		Shows the timestamp of when the Change Order was closed.
	LOCAL_TIME		

Field	Data Type	Reference	Remarks
resolve_date			Indicates the timestamp of when the Change Order was resolved.
rootcause	INTEGER	Rootcause	Foreign key to the id field of the rootcause table, this identifies the Root Cause.
est_total_time	DURATION		Identifies the sum of estimated task time.
actual_total_time	DURATION		Specifies the sum of actual task time.
log_agent	UUID NOT_NULL	ca_contact	Foreign key to the contact_uuid field of the ca_contact table, this identifies who the change request was reported by.
assignee	UUID	ca_contact	Foreign key to the contact_uuid field of the ca_contact table, this identifies the Assignee.
organization	UUID	ca_organization	Foreign key to the id field of the ca_organization table, this identifies the Organization.
group_id	UUID	ca_contact	Foreign key to the contact_uuid field of the ca_contact table, this is the Group ID.
affected_contact	UUID NOT_NULL	ca_contact	Foreign key to the contact_uuid field of the ca_contact table, this specifies the Affected End User.
requestor	UUID NOT_NULL	ca_contact	Foreign key to the contact_uuid field of the ca_contact table, this identifies the Requestor.
category	STRING 12	Change_Category	Foreign key to the code field of the chgctg table, this identifies the Category.
priority	INTEGER NOT_NULL	Priority	Foreign key to the enum field of the pri table, this identifies the Priority.
need_by	LOCAL_TIME		Shows the Need By Date timestamp.
est_comp_date	LOCAL_TIME		Shows the timestamp for the estimated completion date.
actual_comp_ date	LOCAL_TIME		Specifies the actual completion date timestamp.
est_cost	INTEGER		Specifies the estimated cost of this Change Order.
actual_cost	INTEGER		Identifies the actual cost of this Change Order.
justification	STRING 4000		Identifies the justification value for this Change_Request.
backout_plan	STRING 4000		Identifies the backout plan value for this Change_Request.
risk	INTEGER	Risk_Level	
business_case	STRING 4000		
cab	UUID	ca_contact	
closure_code	INTEGER	Closure_Code	
impact	INTEGER	Impact	

Field	Data Type	Reference	Remarks
			Foreign key to the enum field of the impact table, this defines the impact.
parent	INTEGER	Change_Request	Foreign key to the id field of the chg table to allow for hierarchical Change Order groupings (for example, "parent /child").
effort	STRING 2000		Identifies the effort value for this Change_Request.
support_lev	STRING 30	Service_Desc	Foreign key to the code field of the srv_desc table, this identifies the Classic Service Type.
template_name	STRING 30		Foreign key to the template_name field of the chg_tpl table, this identifies the Template name.
sla_violation	INTEGER		Flag indicating the following: **1** -- change order has violated its sla.
predicted_sla_violation	INTEGER		Flag that indicates the following: **1** -- change order has been predicted by neugents.
macro_predicted_violation	INTEGER		Identifies that it is likely to violate its sla (boolean) for action macros to predict sla violations.
created_via	INTEGER	Interface	Foreign key to the id field of the interface table, this identifies which interface created the Change request.
call_back_date	LOCAL_TIME		Identifies the call back timestamp for this Change Order.
call_back_flag	INTEGER		Specifies the call back flag value for this Change Order.
string1	STRING 40		This is a user-defined string field.
string2	STRING 40		This is a user-defined string field.
string3	STRING 40		This is a user-defined string field.
string4	STRING 40		This is a user-defined string field.
string5	STRING 40		This is a user-defined string field.
string6	STRING 40		This is a user-defined string field.
service_date	LOCAL_TIME		Specifies the service date value for this Change_Request.
service_num	STRING 30		Specifies the service num value for this Change_Request.
product	INTEGER	Product	Foreign key to the id field of the product table, this identifies the Product.
actions	STRING 750		
type_of_contact	INTEGER	Type_Of_Contact	
reporting_method	INTEGER	Reporting_Method	Foreign key to the id field of the repmeth table, this identifies how this Change Order was reported.
	INTEGER		

Field	Data Type	Reference	Remarks
person_ contacting		Person_ Contacting	Foreign key to the id field of the person table, this identifies the person who made the contact.
flag1	INTEGER		This is a user-defined integer flag.
flag2	INTEGER		This is a user-defined integer flag.
flag3	INTEGER		This is a user-defined integer flag.
flag4	INTEGER		This is a user-defined integer flag.
flag5	INTEGER		This is a user-defined integer flag.
flag6	INTEGER		This is a user-defined integer flag.
user1	STRING 100		This is a user-defined string field.
user2	STRING 100		This is a user-defined string field.
user3	STRING 100		This is a user-defined string field.
caextwf_ins tance_id	INTEGER	caextwf_in stances	Indicates the CA Process Automation process instance id and process definition name and reference path launched by this Service Desk object.
project	UUID	ca_owned _ resource	
tenant	UUID	ca_tenant	
sched_start _ date	LOCAL_TIME		
sched_end _ date	LOCAL_TIME		
sched_dura tion	DURATION		
actual_start _date	LOCAL_TIME		
actual_end _ date	LOCAL_TIME		
chgtype	INTEGER	usp_chang e_ type	
cab_approv al	INTEGER	Boolean_T able	
requested_ by	UUID REF	ca_contact	
external_ system_tick et	STRING 4000		
orig_user_d ept	INTEGER	ca_resourc e_ departme nt	
	UUID		

Field	Data Type	Reference	Remarks
orig_user_ organizatio n		ca_organiz ation	
orig_user_ admin_ org	UUID	ca_organiz ation	
orig_user_c ost_ center	INTEGER	ca_resourc e_ cost_cente r	
target_start _ last	LOCAL_TIME		
target_hold _ ast	LOCAL_TIME		
target_hold _ count	INTEGER		
target_reso lved_ last	LOCAL_TIME		
target_reso lved_ count	INTEGER		
target_clos ed_ last	LOCAL_TIME		
target_clos ed_ count	INTEGER		
target_start _ last	LOCAL_TIME		Time when target timer started or restarted.
target_hold _ last	LOCAL_TIME		Time of most recent ticket hold
target_hold _ count	INTEGER		Number of times ticket went into a Hold status
target_reso lved_ last	LOCAL_TIME		Time of most recent ticket resolution
target_reso lved_count	INTEGER		Number of times ticket was resolved
target_clos ed_ last	LOCAL_TIME		Time ticket was last closed
target_clos ed_ count	INTEGER		Number of times that ticket was closed

Change_Status Table

Lists the states of the change request, which you can add to at will. This table allows you to control whether the change request is active or inactive when it is changed to this status. Possible statuses include: Open, approval in process, implementation in progress, verification in progress, cancelled, suspended, and closed.

- **SQL Name** -- chgstat
- **Object** -- chgstat

Field	Data Type	Reference	Remarks
active	INTEGER		Flag that indicates the following:**0** -- Inactive**1** -- Active
code	nvarchar (12)		Primary key of this table.
del	INTEGER	Active_Boolean_Table::enum	Delete flag that indicates the following:**0** -- Active**1** -- Inactive/marked as deleted
description	nvarchar (500)		Identifies the textual description of this status.
hold	INTEGER		Flag that specifies the following:**0** -- Start events**1** -- Stop events
id	INTEGER		Unique (to the table) numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
resolved	INTEGER		Flag that indicates the following:**0** -- Not yet resolved**1** -- Resolved
sym	nvarchar (30)		Identifies the Change Request status name.

Chg_Template Table

Maps a template name to a Change_Request that will be used as a template.

- **SQL Name** -- chg_template
- **Object** -- chg_tpl

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Delete flag that represents the following:**0** -- Active**1** -- Inactive/marked as deleted

Field	Data Type	Reference	Remarks
description	nvarchar (1000)		Describes the template.
id	INTEGER		Unique (to the table) numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id)
quick_tmpl_type	INTEGER	Quick_Template_Types::enum	Flag that indicates the following:**1** -- Quick tmpl**2** -- Quick tmpl+review
template	INTEGER	chg id	Unique (to the table) numeric ID.
template_class	nvarchar (12)		Allows subclassing templates.
template_name	nvarchar (30)		Unique name of the template.

chg_trans Table

A transition object controls the current and next ticket status. The chg_trans table lists the status, new status, and actions that need to occur for a default transition.

- **SQL Name** -- chg_trans
- **Object** -- chg_trans

Label	Field	Description
id	INTEGER	Unique key.
status	SYMBOL	Specifies the current ticket status.
new_status	SYMBOL	Specifies the new ticket status
must_comment	INTEGER	Comment required when using a transition. On new default: 0
is_default	INTEGER	Default transition that appears when the Status field is empty. On new default: 0
condition	BOP_REF_STR_REF Macro	Site condition macro to approve transition.
condition error	STRING 255	Error message for site condition.
description	STRING 255	Description of this transition.
last_mod_dt	LOCAL_TIME	Timestamp of last update to this record.
last_mod_by	UUID REF ca_contact	User who last updated this.

Label	Field	Description
del	INTEGER nn	Logical database delete status.
tenant	UUID REF ca_tenant	Reference to Tenant information.

CI Attributes

ci_managed_attribute Table

The following table lists CI attributes that CACF manages for change verification:

- **SQL Name** -- ci_managed_attribute
- **Object** -- ci_managed_attribute

Field	Data Type	Reference	Remarks
id	INTEGER		Primary key to this table, it is a unique numeric ID.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.
del	INTEGER	Active_Boolean_Table::enum	Indicates the Deleted flag, as follows:**0** -- Active **1** -- Inactive/marked as deleted
attribute_name	STRING 128		Specifies the name of the CI attribute.
attribute_label	STRING 50		Specifies the label for the attribute.
description	STRING 255		Specifies a description for the attribute.
initial_status	STRING 32	ci_planned_change_status	Specifies the initial status of the attribute.
case_sensitive	INTEGER		Specifies if the managed attribute is case sensitive.
attribute_type	INTEGER		Specifies the data type.
attribute_length	INTEGER		Specifies the maximum length of the attribute.
srel_factory	STRING 26		Specifies the factory associated with a SREL attribute.
srel_rel_attr	STRING 26		Specifies the factory attribute used as a foreign key.
srel_common_name_attr	STRING 26		Specifies the factory attribute that stores the human-readable value.
srel_show_dropdown	INTEGER	Boolean_Table	Specifies the factory to show in the drop-down list.

Change States

ci_managed_chgstat Table

The following table lists details about managed change states:

- **SQL Name** -- ci_managed_chgstat
- **Object** -- ci_managed_chgstat

Field	Data Type	Reference	Remarks
id	INTEGER		Primary key to this table, it is a unique numeric ID.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
del	INTEGER	Boolean_Table	Indicates the Deleted flag, as follows:**0** -- Active **1** -- Inactive/marked as deleted
code	STRING 12	chgstat	Specifies the Change Order status managed by change verification.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.
can_edit_criteria	INTEGER	Boolean_Table	Specifies if the change status lets you edit criteria.
verification_active	INTEGER	Boolean_Table	Specifies if change verification is active in this state.
autopromote_chg	INTEGER	Boolean_Table	Specifies if autopromote is active for the state.
show_override_buttons	INTEGER	Boolean_Table	Specifies if the override buttons appear for the state.
is_implementation	INTEGER	Boolean_Table	Specifies if the state is an implementation state.

Change Verification

ci_verification_policy Table

The following table lists details about verification policies:

- **SQL Name** -- ci_verification_policy
- **Object** -- ci_verification_policy

Field	Data Type	Reference	Remarks
id	INTEGER		Primary key to this table, it is a unique numeric ID.

Field	Data Type	Reference	Remarks
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.
del	INTEGER	Active_Boolean_Table::enum	Indicates the Deleted flag, as follows:**0** -- Active **1** -- Inactive/marked as deleted
attribute_name	STRING 128	ci_managed_attribute	Specifies the name of the attribute.
ci_name_pattern	STRING 255		Specifies the name of the CI pattern.
class_pattern	STRING 255		Specifies the name of the CI class pattern.
description	STRING 255		Specifies the name of the description of the policy.
mdr_name_pattern	STRING 255		Specifies the name of the MDR pattern.
mdr_class_pattern	STRING 255		Specifies the name of the MDR class pattern.
rolename_pattern	STRING 255		Specifies the name of the role pattern.
name	STRING 100		Specifies the name of the policy.
sequence	INTEGER		Specifies the order that CACF processes the policy.
location_pattern	STRING 255		Specifies the name of the location pattern.
isvariance	INTEGER	Boolean_Table	Specifies if the policy activates for a variance.
isnotverifiable	INTEGER	Boolean_Table	Specifies if the policy is not verifiable.
isrogue_insert	INTEGER	Boolean_Table	Specifies if the policy activates for rogue inserts.
isrogue_update	INTEGER	Boolean_Table	Specifies if the policy activates for rogue updates.
action	STRING 32	ci_verification_policy_act	Specifies the policy action.
write_twa	INTEGER	Boolean_Table	Specifies if you want the policy to write CI and relationship data to the TWA.
write_incident	INTEGER	Boolean_Table	Specifies if you want the policy to create an Incident.
		cr_template	Specifies the Incident template.

Field	Data Type	Reference	Remarks
incident_template	STRING 30		
autoclose_incident	INTEGER	Boolean_Table	Specifies if you want the policy to close the Incident automatically.
log_only_mode	INTEGER	Boolean_Table	Specifies if you want the policy to write to the log instead of modifying a Change Order, CI, or relationship.
start_date	LOCAL_TIME		Specifies the date to start the policy.
end_date	LOCAL_TIME		Specifies the date to end the policy.
service_type	STRING 30	Service_Desc	Specifies the service type of the policy.
priority	INTEGER	Priority	Specifies the priority of the policy.

ci_verification_policy_act Table

The following table lists information about verification policy actions:

- **SQL Name** -- ci_verification_policy_act
- **Object** -- ci_verification_policy_action

Field	Data Type	Reference	Remarks
id	INTEGER		Primary key to this table, it is a unique numeric ID.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.
description	STRING 255		Specifies the long description of the policy action.
name	STRING 100		Specifies the short name of the policy action.
sym	STRING 30		Specifies the constant symbol for this action.

ci_verification_policy_log Table

The following table lists CI attributes that CACF manages for change verification:

- **SQL Name** -- ci_verification_policy_log

Field	Data Type	Reference	Remarks
id	INTEGER		Primary key to this table, it is a unique numeric ID.

Field	Data Type	Reference	Remarks
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.
del	INTEGER	Active_Boolean_Table::enum	Indicates the Deleted flag, as follows:**0** -- Active **1** -- Inactive/marked as deleted
ci_planned_change	INTEGER	ci_planned_change	Specifies the change specification.
nr	UUID	ca_owned_resource	
ci_verification_policy	INTEGER	ci_verification_policy	Specifies the verification policy.
ci_managed_attribute	INTEGER	ci_managed_attribute	Specifies the managed attribute.
oldvalue	STRING 2000		Specifies the old attribute value.
discoveredvalue	STRING 2000		Specifies the discovered attribute value.
newvalue	STRING 2000		Specifies the new attribute value.
status	STRING 32	ci_planned_change_status	Specifies the change verification state.
ci_twa_ci	INTEGER	ci_twa_ci	Specifies the CI in the TWA.
ci_twa_relation	INTEGER	ci_twa_relation	Specifies the relationship in the TWA.
ci_mdr_provider	INTEGER	ci_mdr_provider	Specifies the provider of the MDR.
is_unverifiable	INTEGER	Boolean_Table	Specifies if the change is verifiable.
is_rogueinsert	INTEGER	Boolean_Table	Specifies if the change is a rogue insert.
is_variance	INTEGER	Boolean_Table	Specifies if the change is a variance.
is_rogueupdate	INTEGER	Boolean_Table	Specifies if the change is a rogue update.
ci_verification_policy_act	STRING 32	ci_verification_policy_act	Specifies the verification policy action.
incident	STRING 30	Call_Req	Specifies the incident associated with the verification policy.
role	INTEGER	usp_role	Specifies the role associated with the verification policy.
error_message	STRING 2000		Specifies the error message.

ci_verification_twa_act Table

The following table lists CI attributes that CACF manages for change verification:

- **SQL Name** -- ci_verification_twa_act
- **Object** -- ci_verification_twa_act

Field	Data Type	Reference	Remarks
id	INTEGER		Primary key to this table, it is a unique numeric ID.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
del	INTEGER	Active_Boolean_ Table::enum	Indicates the Deleted flag, as follows:**0** -- Active **1** -- Inactive/marked as deleted
description	STRING 255		Specifies a description for the attribute.
name	STRING 50		Specifies the name of the TWA action.
sym	STRING 32		Specifies the constant symbol for this action.

Change Specifications

This article contains the following topics:

ci_planned_change Table

The following table lists details about change specifications:

- **SQL Name** -- ci_planned_change
- **Object** -- ci_planned_change

Field	Data Type	Reference	Remarks
id	INTEGER		Primary key to this table, it is a unique numeric ID.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.
del	INTEGER	Active_Boolean_ Table::enum	Indicates the Deleted flag, as follows:**0** -- Active **1** -- Inactive/marked as deleted
attribute_name	STRING 128		Specifies the name of the CI or relationship attribute.

Field	Data Type	Reference	Remarks
attribute_value_original	STRING 2000		Specifies the original attribute value.
attribute_value_planned	STRING 2000		Specifies the planned attribute value.
attribute_value_discovered	STRING 2000		Specifies the discovered attribute value.
chg	INTEGER	Change_Request	Specifies the Change Order associated with the planned change.
ci	UUID	ca_owned_resource	Specifies the CI associated with the change specification.
description	STRING 255		Specifies a description of the change specification.
status	STRING 32	ci_planned_change_status	Specifies the status of the change.
incident	STRING 30	Call_Req	Specifies the Incident that the change specification created.
attribute_value_disc_internal	STRING 255		Specifies the internal discovered attribute value.
attribute_value_orig_internal	STRING 255		Specifies the internal original attribute value.
attribute_value_internal	STRING 255		Specifies the internal attribute value.
last_verification_policy	INTEGER	ci_verification_policy	Specifies the last verification policy associated with the change specification.
ci_twa_ci	INTEGER	ci_twa_ci	Specifies the CI in the TWA.
ci_twa_relation	INTEGER	ci_twa_relation	Specifies the CI relationship in the TWA.
verification_msg	STRING 255		Specifies the verification message.

ci_planned_change_status Table

The following table lists details about change specification states:

- **SQL Name** -- ci_planned_change_status
- **Object** -- ci_planned_change_status

Field	Data Type	Reference	Remarks
id	INTEGER		Primary key to this table, it is a unique numeric ID.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.

Field	Data Type	Reference	Remarks
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.
del	INTEGER	Boolean_Table	Indicates the Deleted flag, as follows:**0** -- Active **1** -- Inactive/marked as deleted
description	STRING 255		Specifies the long description of the policy action.
name	STRING 128		Specifies the short name of the policy action.
sym	STRING 10		Specifies the constant symbol for this action.
isinitial	INTEGER	Boolean_Table	Specifies the initial state of the state.
isfinal	INTEGER	Boolean_Table	Specifies the final state of the state.
isselectable	INTEGER	Boolean_Table	Specifies the selectable state.

Events

This article contains the following topics:

Event_Delay Table

This table lists the times that events were delayed.

- **SQL Name** -- evt_dly
- **Object** -- evtdly

Field	Data Type	Reference	Remarks
description	STRING 80		Specifies the user description of delay,
act_delay	DURATION		Specifies the actual duration of delay.
cancel_time	LOCAL_TIME		Specifies when the time delay was cancelled.
create_time	LOCAL_TIME		Specifies when the time delay was created.
delay_type	INTEGER	Event_Delay_Type: enum	Event_Delay_Type : enum

Field	Data Type	Reference	Remarks
eff_delay	DURATION		Specifies the effective duration of delay.
group_name	STRING 30		Specifies the group Name of attevt (currently only SLA).
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
obj_id	STRING 30 NOT_NULL S_KEY		Specifies the persid of the object.
persid	STRING 30		Persistent ID (SystemObjectName:id)
start_time	LOCAL_TIME		Specifies when the time delay was started.
start_userid	UUID	ca_contact::uuid	Specifies the user that created and started delay.
status_flag	INTEGER		Specifies a flag for indicating an event delay status.
stop_time	LOCAL_TIME		Specifies when the time delay was stopped
stop_userid	UUID	ca_contact::uuid	Specifies the user that stopped and cancelled delay.
support_lev	STRING 30	Service_Desc::code	Specifies the service type in effect.

Event_Delay_Type Table

User-defined code for the type of event delay.

- **SQL Name** -- evtdlytp
- **Object** -- evtdlytp

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
enum	INTEGER NOT_NULL		Enumerated value for this entry - specifies ordering in lists and relative values
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
nx_desc	STRING 40		
sym	STRING 12 UNIQUE NOT_NULL S_KEY		

event_log Table

USP event log.

- **SQL Name** -- event_log
- **Object** -- event_log

Field	Data Type	Reference	Remarks
event	INTEGER	event_type::id	Event type
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
kd_id	INTEGER	SKELETONS::id	Assoc knowledge doc
log_time	LOCAL_TIME		Server log date
millitime	INTEGER		Log date millisec
numdata1	INTEGER		Smag number
numdata2	INTEGER		Smag number
sd_obj_id	INTEGER		Assoc SD id
sd_obj_type	STRING 30		Assoc SD object
session	INTEGER	session_log::id	Session with event
textdata1	STRING 500		Smag string
textdata2	STRING 500		Smag string

event_type Table

Event type.

- **SQL Name** -- event_type
- **Object** -- event_type

Field	Data Type	Reference	Remarks
description	STRING 500		Specifies the description.
code	STRING 12 UNIQUE NOT_NULL S_KEY		Specifies the noneditable string enum.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
persid	STRING 30		Persistent ID (SystemObjectName:id)

Events Table

Tables for Event stuff. Events attached to objects.

- **SQL Name** -- evt
- **Object** -- evt

Field	Data Type	Reference	Remarks
description	STRING 80		Specifies the event description.
condition	STRING 30	Spell_Macro:: persid	Specifies the macro function for condition.
del	INTEGER NOT_NULL	Active_Boolean_Table:: enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
delay_time	DURATION NOT_NULL		Specifies the time until condition check.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
modulo_time	DURATION NOT_NULL		Specifies the time increment to adjust.
obj_type	STRING 30		Specifies the object type for this event.
on_done_flag	INTEGER NOT_NULL		Sets the *fire_time* time directly on the attached event to indicate when the event is done.
persid	STRING 30		Persistent ID (SystemObjectName:id)
sym			Specifies the event name.

Field	Data Type	Reference	Remarks
	STRING 30 NOT_NULL unique S_KEY		
urgency	INTEGER		Specifies the urgency of the event.
user_settime	INTEGER NOT_NULL		The user_settime allows the user (or system) to override the fire time (delay time) that is defined for an event. For example, when users add an event to a Service Type, they can redefine the fire time for the event only if the user_settime flag is set. Otherwise, the fire time defined in the event is used.
user_smag	STRING 200		Specifies the user smag field.
violate_on_false	INTEGER		
violate_on_true	INTEGER		
work_shift	STRING 30	Bop_Workshift::persid	

O_EVENTS Table

Program control table used by CA SDM Knowledge Management.

- **SQL Name** -- O_EVENTS
- **Object** -- o_events

Field	Data Type	Reference	Remarks
ACTION	STRING 32768		
ENTITY_ID	INTEGER	SKELETONS::id	
EVENT_NAME	STRING 50		
EVENT_TIMESTAMP	LOCAL_TIME		
ID			Unique (to the table) Numeric ID

Field	Data Type	Reference	Remarks
	INTEGER KEY		
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
VER_COUNT	INTEGER		Version ID indicates the number of versions created (1, 2, 3, 4...)
WF_ACTION_ID	INTEGER		
WF_USER_ID	UUID	ca_contact::uuid	

Data Partition Constraints and Controlled Table

This article contains the following topics:

Domain Table

Lists the names and descriptions of the data partitions themselves.

- **SQL Name** -- dmn
- **Object** -- dmn

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive /marked as deleted
id	INTEGER		Primary key of this table, it is a unique numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
nx_desc	nvarchar (40)		Identifies the data partition description.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
sym	nvarchar (30)		Identifies the data partition name.

Domain_Constraint Table

Lists the constraints associated with a particular data partition and controlled table.

- **SQL Name** -- dcon
- **Object** -- dcon

Field	Data Type	Reference	Remarks
alias	INTEGER		Identifies the alias value for this Domain_Constraint.
constraint_majic	nvarchar (4000)		Specifies Constraint (Majic).
constraint_ SQL	nvarchar (4000)		Specifies Constraint (SQL).
del	INTEGER	Active_Boolean_Table::enum	Indicates the Delete flag, as follows:**0** -- Active**1** -- inactive/marked as deleted)
dom_id	INTEGER	Domain::id	Identifies the unique (to the table) numeric ID.
error_msg	nvarchar (150)		Specifies the message on violation.
id	INTEGER		Primary key to this table, it is a unique numeric ID.
last_mod_ by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_ dt	INTEGER		Indicates the timestamp of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
tbl_id	INTEGER	ctab::id	Indicates the unique (to the table) numeric ID.
type	INTEGER	Domain_ Constraint_Type :: enum	Enumerated value for this entry, this specifies ordering in lists and relative values.

Domain_Constraint_Type Table

Lists the types of constraints that can be associated with a particular data partition and controlled table.

- **SQL Name** -- dcon_typ
- **Object** -- dcon_typ

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table ::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive /marked as deleted
enum	INTEGER		Enumerated value for this entry, this specifies ordering in lists and relative values.
id	INTEGER		Indicates the unique (to the table) numeric ID.
nx_de sc	nvarchar (40)		Specifies the description of the domain contraint type.

Field	Data Type	Reference	Remarks
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
sym	nvarchar (12)		Identifies the symbolic name of this constraint type.

External Entity

External_Entity_Map Table

NOT FOR CLIENT USE. Maps an external entity to an internal object where the external entity is uniquely defined in its own namespace by the xentity_id. The namspace is uniquely defined for our use by the xschema_code and xschema_ver. The semantics of the xentity_id, and parameters (*_rsrved fields) depends upon the namespace.

- **SQL Name** -- xent_map
- **Object** -- ext_entity_map

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
int1_rsrved	INTEGER		reserved for CA - do not use
int2_rsrved	INTEGER		reserved for CA - do not use
int3_rsrved	INTEGER		reserved for CA - do not use
int4_rsrved	INTEGER		reserved for CA - do not use
int5_rsrved	INTEGER		reserved for CA - do not use
int6_rsrved	INTEGER		reserved for CA - do not use
lstr1_rsrved	STRING 255		reserved for CA - do not use
lstr2_rsrved	STRING 255		reserved for CA - do not use
ob_persid	STRING 30		the "mapped to" object
ob_type	STRING 30		the "mapped to" object type
persid	STRING 30		Persistent ID (SystemObjectName:id)
str1_rsrved	STRING 80		reserved for CA - do not use
str2_rsrved	STRING 80		reserved for CA - do not use
xentity_id	STRING 180 NOT_NULL		Specifies the uniq. external entity reference.
xschema_code	STRING 12 NOT_NULL		Specifies the internal code for the namespace of the entity.
xschema_ver	INTEGER NOT_NULL		Specifies the internal ver for the namespace of the entity.

Form Group

Form_Group Table

Listing of defined form groups.

- **SQL Name** -- fmgrp
- **Object** -- fmgrp

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive/marked as deleted
description	nvarchar (100)		Specifies the textual description of this form group.
id	INTEGER		Primary key of this table, it is a unique, numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
sym	nvarchar (30)		Specifies the symbolic value for this Form_Group.

Interface Definitions

intfc Object

Interface definitions used for creating requests and change orders.

- **SQL Name** -- interface
- **Object** -- intfc

Field	Data Type	Reference	Remarks
code	nvarchar (10)		Specifies the code value for this interface.
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive/marked as deleted
id	INTEGER		Primary key of this table, it is a unique numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
nx_desc	nvarchar (240)		The desc value for this interface.

Field	Data Type Reference	Remarks
persid	nvarchar (30)	Persistent ID (SystemObjectName:id).
sym	nvarchar (30)	Identifies the symbolic value for this interface.

Document Repository

Document_Repository Table

Contains Information on document repositories, which are used to store attachments.

- **SQL Name** -- doc_rep
- **Object** -- doc_rep

Field	Data Type	Reference	Remarks
description	STRING 500		Specifies the description.
archive_path	STRING 255		
archive_type	INTEGER		
cgi_path	STRING 255		Specifies the location and name of CGI.
default_rep	INTEGER		
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
file_limit_size	INTEGER		Specifies the file limit size.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
persid	STRING 30		Persistent ID (SystemObjectName:id)
prohibited_ext	STRING 500		Specifies the prohibited file extensions.
protocol	STRING 12		HTTP or SHARE
repository_type	INTEGER		Specifies the type of repository (attachments, knowledge).
retrieve_path	STRING 255		Specifies how to get back to upload_path via protocol.

Field	Data Type	Reference	Remarks
server	STRING 30		Specifies the name of Doc Server.
servlet_path	STRING 255		Specifies the servlet URL.
sym	STRING 30 NOT_NULL S_KEY		Specifies the name of document repository.
upload_path	STRING 255		Specifies the server location of doc repository.

External Application

ext_appl Table

External application.

- **SQL Name** -- ext_appl

Field	Data Type	Reference	Remarks
description	STRING 500		Appl description
code	STRING 12 UNIQUE NOT_NULL S_KEY		Noneditable string enum
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID		Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
persid	STRING 30		Persistent ID (SystemObjectName:id)
sym	STRING 30 NOT_NULL S_KEY		Application name

Group Member

Group Members.

- **SQL Name** -- grpmem
- **Object** -- grpmem

Field	Data Type	Reference	Remarks
group_id	byte (16)		Foreign key to the contact_uuid field of the ca_contact table, this is the group.
id	INTEGER		Specifies the unique (to the table) numeric ID.
			Specifies the Manager flag, as follows:**0** -- No**1** -- Group manager.

Field	Data Type	Reference	Remarks
manager_flag	INTEGER		
member	byte (16)	ca_contact::uuid	Foreign key to the contact_uuid field of the ca_contact table, this is the Member.
notify_flag	INTEGER		Specifies the Notify flag, as follows:**0** -- No notification, **1** -- Notify.

Global Tables

This article contains the following topics:

Global_Change_Extension Table

Local copy of data that will be pushed to master's Global_Change_Queue table.

- **SQL Name** -- g_chg_ext
- **Object** -- g_chg_ext

Field	Data Type	Reference	Remarks
active_flag	INTEGER NOT_NULL	Active_Reverse_Boolean::enum	**1** -- Active **0** -- Inactive
affected_contact	UUID NOT_NULL	ca_contact::uuid	Specifies the Effected End User of CO.
assignee	UUID	ca_contact::uuid	Specifies the assignee of CO.
category	STRING 30		Specifies the category symbol of CO.
chg_ref_num	STRING 30 NOT_NULL		Specifies the change ref num.

Field	Data Type	Reference	Remarks
close_date	LOCAL_TIME		Specifies the close Date of CO.
global_queue_id	INTEGER	Global_Queue_Names::id	Specifies the pointer to global queue.
group_id	UUID		Specifies the group assigned to CO.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
impact	INTEGER	Impact::enum	Specifies the impact of change order.
last_mod_dt	LOCAL_TIME NOT_NULL		Indicates the timestamp of when this record was last modified.
open_date	LOCAL_TIME NOT_NULL		Specifies the open date of CO.
priority	INTEGER NOT_NULL	Priority::enum	Specifies the priority of CO.
remote_id	INTEGER NOT_NULL S_KEY		Specifies the regional request id.
requestor	UUID NOT_NULL	ca_contact::uuid	Specifies the requester of CO.
status	STRING 30 NOT_NULL	Change_Status:: code	Specifies the status symbol of CO.
summary	STRING 240		Specifies the summary of CO.

Global_Change_Queue Table

This table is an accumulation of all of the regional Global_Change_Extension tables.

- **SQL Name** -- g_chg_queue
- **Object** -- g_chg_queue

Field	Data Type	Reference	Remarks
active_flag	INTEGER NOT_NULL	Active_Reverse_Boolean::enum	**1** -- Active **0** -- Inactive
affected_contact	UUID NOT_NULL		Specifies the Affected End User of CO.
assignee	UUID		Specifies the assignee of CO.
category	STRING 30		Specifies the category symbol of CO.
chg_ref_num	STRING 30 NOT_NULL		Specifies the change ref num.
close_date	LOCAL_TIME		Specifies the close Date of CO.
global_queue_ id	INTEGER	Global_Queue_Names::id	Specifies the pointer to global queue.
group_id	UUID		Specifies the group assigned to CO.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
impact	INTEGER	Impact::enum	Specifies the impact of change order.

Field	Data Type	Reference	Remarks
last_mod_dt	LOCAL_TIME NOT_NULL		Indicates the timestamp of when this record was last modified.
open_date	LOCAL_TIME NOT_NULL		Specifies the open date of CO.
priority	INTEGER NOT_NULL	Priority::enum	Specifies the priority of CO.
remote_id	INTEGER NOT_NULL S_KEY		Specifies the regional change id.
remote_sys_id	INTEGER NOT_NULL S_KEY	Global_Servers:: remote_sys_id	Specifies the regional system id.
requestor	UUID NOT_NULL		Specifies the requestor of CO.
status	STRING 30 NOT_NULL	Change_Status:: code	Specifies the status sybmol of CO.
summary	STRING 240		Specifies the summary of CO.

Global_Contact Table

Contain all contacts across all systems participating in the Global Service Desk.

- **SQL Name** -- g_contact
- **Object** -- g_cnt

Field	Data Type	Reference	Remarks
contact_num	STRING 30		Specifies the contact number.
del	INTEGER NOT_NULL	Active_Boolean_ Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
email_address	STRING 120		Specifies the email address of the contact.
first_name	STRING 100		Specifies the first name of the contact.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
last_name	STRING 100		Specifies the last name of the contact.
loc_id	UUID		Specifies the location id.
middle_name	STRING 100		Specifies the middle name of the contact.
org_id	UUID		Specifies the organization id.
pri_phone_ number	STRING 32		Specifies the phone number of the contact.
remote_id	UUID NOT_NULL S_KEY		Specifies the regional contact id.
			Specifies the regional system id.

Field	Data Type	Reference	Remarks
remote_sys_id	INTEGER NOT_NULL S_KEY	Global_Servers :: remote_sys_id	
userid	STRING 100		Specifies the userid of the contact.

Global_Issue_Extension Table

Local copy of data that will be pushed to master's Global_Issue_Queue table.

- **SQL Name** -- g_iss_ext
- **Object** -- g_iss_ext

Field	Data Type	Reference	Remarks
active_flag	INTEGER NOT_NULL	Active_Reverse_ Boolean::enum	**1** -- Active **0** -- Inactive
assignee	UUID	ca_contact::uuid	Assignee of Issue
category	STRING 30		Category symbol of Issue
close_date	LOCAL_TIME		Close Date of Issue
global_queue_id	INTEGER	Global_Queue_Names::id	Pointer to global queue
group_id	UUID		Group assigned to Issue
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
impact	INTEGER	Impact::enum	Impact of Issue
last_mod_dt	LOCAL_TIME NOT_NULL		Indicates the timestamp of when this record was last modified.
open_date	LOCAL_TIME NOT_NULL		Open Date of Issue
priority	INTEGER NOT_NULL	Priority::enum	Priority of Issue
product	INTEGER	Product::id	Product of Issue
ref_num	STRING 30 NOT_NULL		Issue ref num
remote_id	INTEGER NOT_NULL S_KEY		Regional request id
requestor	UUID NOT_NULL	ca_contact::uuid	Affected End User of CO
status	STRING 30 NOT_NULL	Issue_Status::code	Status symbol of Issue
summary	STRING 240		Summary of Issue

Global_Issue_Queue Table

This table is an accumulation of all of the regional Global_Issue_Extension tables.

- **SQL Name** -- g_iss_queue

- **Object** -- g_iss_queue

Field	Data Type	Reference	Remarks
active_flag	INTEGER NOT_NULL	Active_Reverse_ Boolean::enum	**1** -- Active **0** -- Inactive
assignee	UUID		Assignee of Issue
category	STRING 30		Category symbol of Issue
close_date	LOCAL_TIME		Close Date of Issue
global_que ue_ id	INTEGER	Global_Queue_ Names::id	Pointer to global queue
group_id	UUID		Group assigned to Issue
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
impact	INTEGER	Impact::enum	Impact of Issue
last_mod_ dt	LOCAL_TIME NOT_NULL		Indicates the timestamp of when this record was last modified.
open_date	LOCAL_TIME NOT_NULL		Open Date of Issue
priority	INTEGER NOT_NULL	Priority::enum	Priority of Issue
product	INTEGER		Product of Issue
ref_num	STRING 30 NOT_NULL		Issue ref num
remote_id	INTEGER NOT_NULL S_KEY		Regional Issue id
remote_sys _id	INTEGER NOT_NULL S_KEY	Global_Servers:: remote_sys_id	Regional system id
requestor	UUID NOT_NULL		Affected User of Issue
status	STRING 30 NOT_NULL	Issue_Status::code	Status symbol of Issue
summary	STRING 240		Summary of Issue

Global_Location Table

Contains all Location names for all regions.

- **SQL Name** -- g_loc
- **Object** -- g_loc

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL	Active_Boolean_ Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
	LOCAL_TIME		

Field	Data Type	Reference	Remarks
last_mod_dt			Indicates the timestamp of when this record was last modified.
loc_name	STRING 100		Location Name
remote_id	UUID NOT_NULL S_KEY		Regional location id
remote_sys_id	INTEGER NOT_NULL S_KEY	Global_Servers:: remote_sys_id	Regional system id

Global_Organization Table

Contains all Organizations names for all regions.

- **SQL Name** -- g_org
- **Object** -- g_org

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL	Active_Boolean_ Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
org_name	STRING 100		Organization Name
remote_id	UUID NOT_NULL S_KEY		Regional organization id
remote_sys_id	INTEGER NOT_NULL S_KEY	Global_Servers:: remote_sys_id	Regional system id

Global_Product Table

Contains all Product names for all regions. Used by Global_Issue_Queue.

- **SQL Name** -- g_product
- **Object** -- g_prod

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL	Active_Boolean_ Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
	LOCAL_TIME		

Field	Data Type	Reference	Remarks
last_mod_dt			Indicates the timestamp of when this record was last modified.
remote_id	INTEGER NOT_NULL S_KEY		Regional product id
remote_sys_ id	INTEGER NOT_NULL S_KEY	Global_Servers:: remote_sys_id	Regional system id
sym	STRING 60		Symbol name of product

Global_Queue_Names Table

List of queues that are considered global.

- **SQL Name** -- g_queue_names
- **Object** -- g_qname

Field	Data Type	Reference	Remarks
description	STRING 100		comments field
del	INTEGER NOT_NULL	Active_Boolean_ Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
sym	STRING 30 UNIQUE NOT_NULL		Descriptive name

Global_Request_Extension Table

Local copy of data that will be pushed to master's Global_Request_Queue table.

- **SQL Name** -- g_req_ext
- **Object** -- g_cr_ext

Field	Data Type	Reference	Remarks
active_flag	INTEGER NOT_NULL	Active_Reverse_ Boolean::enum	**1** -- Active **0** -- Inactive
assignee	UUID	ca_contact::uuid	Assignee of Request
category	STRING 30		Category symbol of Request
close_date	LOCAL_TIME		Close Date of Request

Field	Data Type	Reference	Remarks
customer	UUID NOT_NULL	ca_contact::uuid	Affected User of Request
global_queue_id	INTEGER	Global_Queue_Names::id	Pointer to global queue
group_id	UUID		Group assigned to Request
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
impact	INTEGER	Impact::enum	Impact of Request
last_mod_dt	LOCAL_TIME NOT_NULL		Indicates the timestamp of when this record was last modified.
open_date	LOCAL_TIME NOT_NULL		Open Date of Request
priority	INTEGER NOT_NULL	Priority::enum	Priority of Request
ref_num	STRING 30 NOT_NULL		Request ref num
remote_id	INTEGER NOT_NULL S_KEY		Regional request id
status	STRING 30 NOT_NULL	Cr_Status::code	Status symbol of Request
summary	STRING 240		Summary of Request
type	STRING 10	crt code	ITIL record type

Global_Request_Queue Table

This table is an accumulation of all of the regional Global_Request_Extension tables.

- **SQL Name** -- g_req_queue
- **Object** -- g_cr_queue

Field	Data Type	Reference	Remarks
active_flag	INTEGER NOT_NULL	Active_Reverse_Boolean::enum	**1** -- Active **0 --** Inactive
assignee	UUID		Assignee of Request
category	STRING 30		Category symbol of Request
close_date	LOCAL_TIME		Close Date of Request
customer	UUID NOT_NULL		Affected User of Request
global_queue_id	INTEGER	Global_Queue_Names::id	Pointer to global queue
group_id	UUID		Group assigned to Request
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
impact	INTEGER	Impact::enum	Impact of Request

Field	Data Type	Reference	Remarks
last_mod_dt	LOCAL_TIME NOT_NULL		Indicates the timestamp of when this record was last modified.
open_date	LOCAL_TIME NOT_NULL		Open Date of Request
priority	INTEGER NOT_NULL	Priority::enum	Priority of Request
ref_num	STRING 30 NOT_NULL		Request ref num
remote_id	INTEGER NOT_NULL S_KEY		Regional request id
remote_sys_id	INTEGER NOT_NULL S_KEY	Global_Servers:: remote_sys_id	Regional system id
status	STRING 30 NOT_NULL	Cr_Status::code	Status symbol of Request
summary	STRING 240		Summary of Request
type	STRING 10	crt code	ITIL record type

Global_Servers Table

Maintains a list of CA SDM installations that comprise the Global Service Desk.

- **SQL Name** -- g_srvr
- **Object** -- g_srvrs

Field	Data Type	Reference	Remarks
description	STRING 100		Specifies the comments field.
chg_prefix	STRING 5		Specifies the prefix for changes for a region.
cr_prefix	STRING 5		Specifies the prefix for requests for a region.
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
global_name	STRING 30 UNIQUE NOT_NULL		Value of NX_GLOBAL_NAME on region
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID

Field	Data Type	Reference	Remarks
is_master	INTEGER	Boolean_Table::enum	Indicates if this server defined as master.
iss_prefix	STRING 5		Specifies the prefix for issues for a region.
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
remote_sys_id	INTEGER UNIQUE NOT_NULL		Regional system id
slump_addr	STRING 30		Specifies the CA SDM primary server hostname or IP address. A slump_addr is defined for each global region definition.
sym	STRING 30 UNIQUE NOT_NULL		Specifies the descriptive name.
web_protocol	STRING 10		Specifies the master region web access protocol (http https).
web_server	STRING 30		Specifies the web server name.
web_server_port	STRING 10		Specifies the web server port (can be blank).
web_url	STRING 100		Specifies the rest of URL to pdmweb.exe of remote system (or webdirector).

Usp_Servers Table

The usp_servers table lists all the servers in the CA SDM deployment.

Field	Data Type	Reference	Description
id	INTEGER UNIQUE		Unique key.
local_host	STRING 128 UNIQUE NOT_NULL S_KEY		Host name/Server name
timezone	STRING 30	Timezone	Timezone of server.
desc	STRING 1024		Textual description of the this host/server.
del	INTEGER NOT_NULL		Deleted flag 0 -- active 1 -- inactive/marked as deleted
server_id	INTEGER		Server ID or Slump ID

Field	Data Type	Reference	Description
slump_port	INTEGER		Slump port number for communication.
server_type	INTEGER	server_types	Type of Server 0 -- primary 1 -- Secondary 2 -- Background 3 -- Stand-By 4 -- Application Server
database_type	STRING 30		Currently unused. 0 -- SQL 1 -- Oracle
external_dns_name	STRING 30		Currently unused.
platform	STRING 30		Currently unused. 0 -- Unix/Linux 1 -- Windows
linked	INTEGER NOT_NULL		Specify whether the server is configured.
last_mod_dt	LOCAL_TIME		Timestamp of when the record was last modified.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified the record.

Global_Table_Map Table

Contains list of table maps (local to master) used in global data transport.

- **SQL Name** -- g_tbl_map
- **Object** -- g_tblmap

Field	Data Type	Reference	Remarks
description	STRING 100		Comments field
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
map_definition	STRING 64 NOT_NULL		Map Definition name in xml file
sym	STRING 30 UNIQUE NOT_NULL		Name of this table map

Global_Table_Rule Table

Contains list of extract rules for global data transport.

- **SQL Name** -- g_tbl_rule
- **Object** -- g_tblrule

Field	Data Type	Reference	Remarks
description	STRING 100		Comments field
addl_query	STRING 240		Additional query
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
last_sync_dt	LOCAL_TIME		What was the last sync date
reoccur_interv	DURATION		How often to re-query
sched	STRING 30	Bop_Workshift::persid	Valid run schedule
sym	STRING 30 UNIQUE NOT_NULL S_KEY		Name for rule
table_map	INTEGER	Global_Table_Map::id	Table map

Transition Object Control

This article contains the following information:

in_trans Table

A transition object controls the current and next ticket status. The in_trans table lists the status, new status, and actions that need to occur for a default transition.

- **SQL Name** -- in_trans
- **Object** -- in_trans

Label	Field	Description
id	INTEGER	Unique key.
status	SYMBOL	Specifies the current ticket status.
new_status	SYMBOL	Specifies the new ticket status
must_comment	INTEGER	Comment required when using a transition. On new default: 0
is_default	INTEGER	Default transition that appears when the Status field is empty. On new default: 0
condition	BOP_REF_STR_REF Macro	Site condition macro to approve transition.
condition error	STRING 255	Error message for site condition.
description	STRING 255	Description of this transition.
last_mod_dt	LOCAL_TIME	Timestamp of last update to this record.
last_mod_by	UUID REF ca_contact	User who last updated this.
del	INTEGER nn	Logical database delete status.
tenant	UUID REF ca_tenant	Reference to Tenant information.

iss_trans Table

A transition object controls the current and next ticket status. The iss_trans table lists the status, new status, and actions that need to occur for a default transition.

- **SQL Name** -- iss_trans
- **Object** -- iss_trans

Label	Field	Description
id	INTEGER	Unique key.
status	SYMBOL	Specifies the current ticket status.
new_status	SYMBOL	Specifies the new ticket status
must_comment	INTEGER	Comment required when using a transition. On new default: 0
is_default	INTEGER	Default transition that appears when the Status field is empty. On new default: 0
condition	BOP_REF_STR_REF Macro	Site condition macro to approve transition.
condition error	STRING 255	Error message for site condition.
description	STRING 255	Description of this transition.
last_mod_dt	LOCAL_TIME	Timestamp of last update to this record.

Label	Field	Description
last_mod_by	UUID REF ca_contact	User who last updated this.
del	INTEGER nn	Logical database delete status.
tenant	UUID REF ca_tenant	Reference to Tenant information.

Issue Template

iss_Template Table

Table to manage Issue templates. There is one entry for each Issue that is a template.

- **SQL Name** -- iss_template
- **Object** -- iss_tpl

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive/marked as deleted
description	nvarchar (1000)		Specifies the textual description of the template.
id	INTEGER		Specifies the unique (to the table) numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
quick_tmpl_type	INTEGER	Quick_Template_Types::enum	Specifies the quick template type, as follows:**1** -- Quick tmpl**2** -- Quick tmpl+review
template	nvarchar (30)	issue persistent_id	Persistent ID (SystemObjectName:id).
template_class	nvarchar (12)		This allow subclassing of the templates.
template_name	nvarchar (30)		Identifies the unique name of the template

Issue Table

This article contains the following topics:

Request management's analyst recording of an external user's ticket.

- **SQL Name** -- issue
- **Object** -- iss

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE NOT_NULL KEY		Specifies the unique (to the table) numeric ID.
persid	STRING 30		Specifies the Persistent ID (SystemObjectName:id).
ref_num	STRING 30 UNIQUE NOT_NULL S_KEY		Identifies the reference number.
summary	STRING 240		Identifies the Issue summary text.
description	STRING 4000		Provides a textual description of this Issue.
status	STRING 12	Issue_Status	
active_flag	INTEGER NOT_NULL		Flag representing whether this record is active or inactive: **0** -- Inactive **1** -- Active
start_date	LOCAL_TIME		Indicates the timestamp of when processing started.
open_date	LOCAL_TIME		Shows the timestamp of when this Issue was opened.
last_mod_dt	LOCAL_TIME		Identifies the timestamp of when this record was last modified.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
close_date	LOCAL_TIME		Shows the timestamp of when the Issue was closed.
resolve_date	LOCAL_TIME		Indicates the timestamp of when the Change Order was resolved.
rootcause	INTEGER	Rootcause	Foreign key to the id field of the rootcause table, this identifies the Root Cause.
est_total_time	DURATION		Identifies the sum of estimated task time.
actual_total_time	DURATION		Specifies the sum of actual task time.
log_agent	UUID NOT_NULL	ca_contact	Foreign key to the contact_uuid field of the ca_contact table, this identifies who the change request was reported by.
assignee	UUID	ca_contact	Foreign key to the contact_uuid field of the ca_contact table, this identifies the Assignee.
organization	UUID	ca_organization	Foreign key to the id field of the ca_organization table, this identifies the Organization.
group_id	UUID	ca_contact	Foreign key to the contact_uuid field of the ca_contact table, this is the Group ID.
	UUID	ca_contact	Foreign key to the contact_uuid field of the ca_contact table.

Field	Data Type	Reference	Remarks
affected_contact			
requestor	UUID NOT_NULL	ca_contact	Foreign key to the contact_uuid field of the ca_contact table, this specifies the Affected End User.
category	STRING 12	Issue_Category	Foreign key to the code field of the isscat table, this identifies the Category.
priority	INTEGER NOT_NULL	Priority	Foreign key to the enum field of the pri table, this identifies the Priority.
need_by	LOCAL_TIME		Shows the Need By Date timestamp for this Issue.
est_comp_date	LOCAL_TIME		Shows the estimated completion date for this Issue.
actual_comp_date	LOCAL_TIME		Specifies the actual completion date timestamp.
est_cost	INTEGER		Specifies the estimated cost value for this Issue.
actual_cost	INTEGER		Identifies the actual cost of this Issue.
justification	STRING 240		Identifies the justification value for this Issue.
backout_plan	STRING 240		Identifies the backout plan value for this Issue.
impact	INTEGER	Impact	Foreign key to the enum field of the impact table, this defines the impact.
parent	STRING 30	Issue	Foreign key to the persistent_id field of the iss table, this identifies the Parent.
effort	STRING 240		Identifies the effort value for this Issue.
support_lev	STRING 30	Service_Desc	Foreign key to the code field of the srv_desc table, this identifies the Classic Service Type.
template_name	STRING 30		Foreign key to the template_name field of the iss_tpl table, this identifies the Template name.
sla_violation	INTEGER		Flag indicating the following: **1** -- Issue has violated its sla.
predicted_sla_violation	INTEGER		Flag that indicates the following: **1** -- Has been predicted by neugents.
macro_predicted_violation	INTEGER		Identifies that it is likely to violate its sla (boolean) for action macros to predict sla violations.
created_via	INTEGER	Interface	Specifies the unique (to the table) numeric ID.
call_back_date	LOCAL_TIME		Identifies the call back timestamp for this Issue.
call_back_flag	INTEGER		Specifies the call back flag value for this Issue.
string1	STRING 40		This is a user-defined string field.
string2	STRING 40		This is a user-defined string field.

Field	Data Type	Reference	Remarks
string3	STRING 40		This is a user-defined string field.
string4	STRING 40		This is a user-defined string field.
string5	STRING 40		This is a user-defined string field.
string6	STRING 40		This is a user-defined string field.
service_date	LOCAL_TIME		Specifies the service date value for this Issue.
service_num	STRING 30		Specifies the service num value for this Issue.
product	INTEGER	Product	Foreign key to the id field of the product table, this identifies the Product.
actions	STRING 750		Identifies the actions value for this Issue.
type_of_contact	INTEGER	Type_Of_Contact	Foreign key to the id field of the toc table, this identifies the Type of Contact.
reporting_method	INTEGER	Reporting_Method	Foreign key to the id field of the repmeth table, this identifies how this Issue was reported.
person_contacting	INTEGER	Person_Contacting	Foreign key to the id field of the person table, this identifies the person who made the contact.
flag1	INTEGER		This is the flag1 value for this Issue.
flag2	INTEGER		This is the flag2 value for this Issue.
flag3	INTEGER		This is the flag3 value for this Issue.
flag4	INTEGER		This is the flag4 value for this Issue.
flag5	INTEGER		This is the flag5 value for this Issue.
flag6	INTEGER		This is the flag6 value for this Issue.
user1	STRING 100		This is a user-defined string field.
user2	STRING 100		This is a user-defined string field.
user3	STRING 100		This is a user-defined string field.
caextwf_instance_id	INTEGER	caextwf_instances	Indicates the CA Process Automation process instance id and process definition name and reference path launched by this Service Desk object.
ticket_avoided	INTEGER		
tenant	UUID	ca_tenant	
requested_by	UUID	ca_contact	
external_system_ticket	STRING 4000		
orig_user_dept	INTEGER	ca_resource_department	

Field	Data Type	Reference	Remarks
orig_user_organization	UUID	ca_organization	
orig_user_admin_org	UUID	ca_organization	
orig_user_cost_center	INTEGER	ca_resource_ cost_center	
target_start_last	LOCAL_TIME		
target_hold_last	LOCAL_TIME		
target_hold_count	INTEGER		
target_resolved_ last	LOCAL_TIME		
target_resolved_ count	INTEGER		
target_closed_last	LOCAL_TIME		
target_closed_ count	INTEGER		

Issue_Act_Log Table

History of activities associated with an issue. Types of activities are listed in the Act_Type table.

- **SQL Name** -- issalg
- **Object** -- issalg

Field	Data Type	Reference	Remarks
action_desc	nvarchar (4000)		Specifies the text description of the activity log entry.
analyst	byte (16)	ca_contact::uuid	Foreign key to the contact_uuid field of the ca_contact table, this represents the Analyst who created this activity log.
description	nvarchar (4000)		Specifies the text description of the activity log.
id	INTEGER		Primary key of this table, this is a unique numeric ID.
internal	INTEGER		Designates the log as an Internal log.
issue_id	nvarchar (30)		Foreign key to the persistent_id field of the iss table, this is the Issue for this activity.

Field	Data Type	Reference	Remarks
		issue persistent _id	
knowledge _session	nvarchar (80)		Specifies the reference to the Knowledge Management session.
knowledge _tool	nvarchar (12)		Identifies the Knowledge Management Tool used for this activity.
last_mod_ dt	INTEGER		Identifies the timestamp of when this record was last modified.
persid	nvarchar (30)		Specifies the Persistent ID (SystemObjectName:id).
system_ti me	INTEGER		Represents the date and time of the record creation.
time_spen t	INTEGER		Identifies the time spent on the activity by the user.
time_stam p	INTEGER		Specifies the time spent on the activity by the user.
type	nvarchar (12)	Act_Type:: code	(Not Used) This is an acknowledgement that is also a non-editable string enum.

Issue_Category Table

Issue categories. Can be hierarchical.

- **SQL Name** -- isscat
- **Object** -- isscat

Field	Data Type	Reference	Remarks
id	INTEG ER		Unique (to the table) numeric ID.
persid	STRIN G(30)		Persistent ID (SystemObjectName:id)
del	INTEG ER	Active_Boolean_ Table::enum	Delete flag that indicates the following:**0** -- Active**1** -- Inactive /marked as deleted
sym	STRIN G (1000)		Identifies the Issue Category symbolic description.
code	STRIN G (12)		Primary key of this table.
last_mo d_dt	LOCAL _TIME		Identifies the timestamp of when this record was last modified.
	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.

Field	Data Type	Reference	Remarks
last_mod_by			
description	STRING (500)		Identifies the textual description of this issue category.
organization	UUID	ca_organization::organization_uuid	Foreign key to the id field of the ca_organization table, this is the Organization.
assignee	UUID		Foreign key to the contact_uuid field of the ca_contact table, this is also the Assignee.
group_id	UUID		Foreign key to the contact_uuid field of the ca_contact table. This is the Group.
children_ok	INTEGER		Specifies the handling of the issue category:**0** -- Children not allowed**1** -- Children are allowed
service_type	STRING (30)	Service_Desc	
survey	INTEGER	Survey_Template::id	Foreign key of the id field of the survey_tpl table, this is the Survey.
schedule	INTEGER	Bop_Workshift	Deprecated.
auto_assign	INTEGER		Flag that enables auto assignment.
owning_contract	INTEGER	Service_Contract::id	Foreign key to the id field of the svc_contract table.This is the Service Contract.
flow_flag	INTEGER		Specifies the type of workflow:**0** -- Classic Workflow or none (default) **2** -- CA IT PAM
caextwf_start_id	INTEGER	caextwf_start_forms	Identifies the CA IT PAM process definition information to use when the user selects this category on a change order, issue, request.
tenant	UUID	ca_tenant	
chgtype	INTEGER	usp_change_type	
risk_survey	INTEGER	Risk_Survey_Template	
cab	UUID	ca_contact	
ss_include	INTEGER	bool	REQUIRED On new default: 0
ss_sym	STRING (128)		

Issue_Property Table

Property value pairs for an object.

- **SQL Name** -- issprp
- **Object** -- iss_prp

Field	Data Type	Reference	Remarks
description	nvarchar(240)		Specifies the textual description of this property.
error_msg	STRING 240		Specifies the error message produced if validation fails.
id	INTEGER		Primary key of this table, it is also a unique, numeric ID.
label	nvarchar(80)		Specifies the label value for this Issue property.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
owning_iss	nvarchar(30)	Issue	Foreign key to the persistent_id field of the iss table, this is also the Issue.
owning_macro	BOP_REF_STR NOT_NULL	Spell_Macro	Specifies the Spell_Macro for validation.
required	INTEGER	Boolean_Table::enum	Identifies the Required flag, as follows:**0** -- Not required**1** -- Required
sample	nvarchar(240)		The sample value for this property.
sequence	INTEGER		Used to order the properties for an Issue.
value_description	STRING 240		Text description of the value.
validation_rule	BOP_REF_STR NOT_NULL	Property_Validation_Rule	Identifies the valid value rule.
validation_type	BOP_REF_STR NOT_NULL	Property_Validation_Type	Identifies the type of validation rule.
value	nvarchar(240)		Identifies the value of the property.

Issue_Status Table

Lists the states of the Issue, which you can also add. This table allows you to control whether the issue is active or inactive when it is changed to this status. Possible status include: open, approval in process, implementation in progress, verification in progress, cancelled, suspended, and closed.

- **SQL Name** -- issstat
- **Object** -- issstat

Field	Data Type	Reference	Remarks
active	INTEGER		Flag that indicates the following:**0** -- Inactive**1** -- Active
code	nvarchar (12)		Primary key of this table.
del	INTEGER		Delete flag that indicates the following:**0** -- Active**1** -- Inactive /marked as deleted
description	nvarchar (500)		Identifies the textual description of this status.
hold	INTEGER		Flag that specifies the following:**0** -- Start events**1** -- Stop events
id	INTEGER		Unique (to the table) numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
resolved	INTEGER		Flag that indicates the following:**0** -- Not yet resolved**1** -- Resolved
sym	nvarchar (30)		Identifies the symbolic name of the Issue status.

Key Control

Table of sequence numbers for requests, change orders, tickets, and foreign keys.

- **SQL Name** -- kc

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
key_name	STRING 20		
key_value	INTEGER		Indicates the next key available for handout.

Message Status

This article contains the following topics:

Mgs_Act_Log Table

History of activities associated with a managed survey. The types of activities are listed in the Act_Type table.

- **SQL Name** -- mgsalg

- **Object** -- mgsalg

Field	Data Type	Reference	Remarks
action_desc	nvarchar (700)		Specifies the text description of the activity log entry.
analyst	byte(16)	ca_contact::uuid	Foreign key to the contact_uuid field of the ca_contact table, this represents the Analyst who created this activity log.
description	nvarchar (1000)		Specifies the text description of the activity log.
id	INTEGER		Primary key of this table, this is a unique numeric ID.
internal	INTEGER		Designates the log as an Internal log.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
mgs_id	INTEGER	Managed_Survey::id	Specifies the unique (to the table) numeric ID.
persid	nvarchar (30)		Specifies the Persistent ID (SystemObjectName:id).
system_time	INTEGER		Represents the date and time of the record creation.
time_spent	INTEGER		Identifies the time spent on the activity by the user.
time_stamp	INTEGER		Specifies the date time spent on the activity by the user.
type	nvarchar (12)	Act_Type::code	Foreign key to the code field of the act_type table, this is the Type.

Mgs_Status Table

List of valid message status definitions.

- **SQL Name** -- mgsstat
- **Object** -- mgsstat

Field	Data Type	Reference	Remarks
active	INTEGER		Flag that indicates the following:**0** -- Inactive**1** -- Active
code	nvarchar (12)		Primary key of this table.
del	INTEGER	Active_Boolean_Table::enum	Delete flag that indicates the following:**0 --** Active**1 --** Inactive/marked as deleted
description	nvarchar (500)		Identifies the textual description of this status.

Field	Data Type	Reference	Remarks
hold	INTEGER		Flag that specifies the following:**0** -- Start events**1** -- Stop events
id	INTEGER		Unique (to the table) numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
sym	nvarchar (30)		Identifies the Managed Survey Status name.

Notification Table

This article contains the following topics:

Notification Table

Program control table used by Knowledge Management.

- **SQL Name** -- Notification
- **Object** -- Notification

Field	Data Type	Reference	Remarks
ALT_EMAIL	STRING 100		
ANALYST_ID	UUID	ca_contact::uuid	
DOC_ID	INTEGER		
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
NTF_LEVEL	INTEGER		**0** -- External and Internal **1** -- External only **2** -- Internal only

Notification_Urgency Table

Maps internal enums to strings for representing notification urgency for contacts.

- **SQL Name** -- noturg
- **Object** -- noturg

Field	Data Type	Index	Reference	Remarks
del	INTEGER NOT_NULL		Active_Boolean_Table::enum	**0** -- Present **1** -- Gone
desc	STRING 40			Specifies the description of notification urgency.
enum	INTEGER NOT_NULL			Indicates the enumeration value.
id	INTEGER UNIQUE NOT_NULL KEY	storage hash		Indicates the key ID.
sym	STRING 60 UNIQUE NOT_NULL S_KEY	sort dsc		Indicates the notify urgency symbol.

Notify_Log_Header Table

This table keeps track of each notify, and what happened to it.

- **SQL Name** -- not_log
- **Object** -- lr

Field	Data Type	Reference	Remarks
cmth_used	INTEGER	Contact_Method ::id	
cntxt_obj	STRING 30		Specifies the termination of sequence Context for notification.
context_instance	STRING 30		Contains the persistent ID of the associated Activity Log for the notifications.
del	INTEGER NOT_NULL	Active_Boolean_ Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID.
last_mod	LOCAL_TIME		Specifies the last modification time, for purging.
nlh_ack_by	LOCAL_TIME		Specifies the time deadline for ack.
	DURATION		Specifies how long for ack.

Field	Data Type	Reference	Remarks
nlh_ack_time			
nlh_c_addressee	UUID	ca_contact::uuid	Specifies the alias contact.
nlh_c_alias	UUID		
nlh_cm_method	INTEGER	Notification_Urgency::enum	
nlh_email	STRING 50		Specifies the resolved email address (the email notification sent was not associated with the proper contact).
nlh_end	LOCAL_TIME		Specifies the time of ACK or FYI final.
nlh_hdr	STRING 40		Specifies the msg header text.
nlh_msg	STRING 4000		Specifies the message text.
nlh_msg_html	STRING 32768		Specifies the html version of notification if sent through mail.
nlh_pri	INTEGER		Generating notification enum priority of transition event
nlh_start	LOCAL_TIME NOT_NULL		Specifies the notification start date.
nlh_status	INTEGER		Pending send, sent FYI.
nlh_transition	INTEGER		Specifies the notify method used - redefined in majic, points to 'noturg' object Transition point.
nlh_type	INTEGER		FYI or ack
nlh_user_ack	STRING 40		Sent ack, acked, nacked, cleared. Who acknowledged or cleared it.

Notify_Msg_Tpl Table

List of object attribute message template definitions for notification rules.

- **SQL Name** -- ntfm
- **Object** -- ntfm

Field	Data Type	Reference	Remarks
ID	INTEGER		Primary key
persid	nvarchar(30)		Object key
del	SREL integer -- > actbool		Delete indicator
sym	nvarchar(128)		Symbolic description; required field
notify_flag	INTEGER		Auto notification

Field	Data Type	Reference	Remarks
notify_level	SREL integer --> noturg		Notification level
notify_msg_title	nvarchar(255)		Notification message title (Required)
notify_msg_body	nvarchar(4000)		Notification message body
notify_msg_body_html	nvarchar(32768)		Notification HTML message
obj_type	SREL string --> ntfm_prod_list		Object type: cr, chg, iss; required field
last_mod_dt	DATE		Audit trail date
last_mod_by	SREL uuid --> cnt		Audit trail user

Notify_Object_Attr Table

List of object attribute contacts that may receive notifications.

- **SQL Name** -- ntfl
- **Object** -- ntfl

Field	Data Type	Reference	Remarks
description	STRING 240		Specifies the textual description.
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
object_attr	STRING 250		Specifies the attr name in object.
object_type	STRING 30		Specifies the object name.
persid	STRING 30		Persistent ID (SystemObjectName:id)
sym	STRING 30 NOT_NULL		

Notify_Rule Table

List of object attribute contacts and definitions for notification rules.

- **SQL Name** -- ntfr
- **Object** -- ntfr

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
persid	nvarchar (30)		Specifies the object key
del	INTEGER		Delete indicator
sym	nvarchar (128)		Symbolic description REQUIRED
description	nvarchar (500)		Long description
condition	nvarchar (30)	Spell_Macro	Specifies the foreign key to the condition macro.
obj_type	nvarchar (30)		Specifies the object type as cr, chg, or iss REQUIRED
last_mod_dt	LOCAL_TIME		Audit trail date
last_mod_by	UUID	ca_contact	Audit trail user
default_rule	INTEGER		**1** -- Default rule; do not allow condition
cr_notify_info	nvarchar (30)	ntfm	Specifies the foreign key for 'cr' obj_type to condition macro.
chg_notify_info	nvarchar (30)	ntfm	Specifies the foreign key for 'chg' obj_type to condition macro.
iss_notify_info	nvarchar (30)	ntfm	Specifies the foreign key for 'iss' obj_type to condition macro.
mgs_notify_info	nvarchar (30)	ntfm	Specifies the foreign key for 'mgs' obj_type to condition macro.
kd_notify_info	nvarchar (30)	ntfm	Specifies the foreign key for 'kd' obj_type to condition macro.
kd_comment_notify_info	nvarchar (30)	ntfm	Specifies the foreign key for 'kd_comment' obj_type to condition macro.
krc_notify_info	nvarchar (30)	ntfm	Specifies the foreign key for 'krc' obj_type to condition macro.
sa_notify_info	nvarchar (30)	ntfm	Specifies the foreigh key for 'sa' obj_type to condition macro.
cnt_notify_info	nvarchar (30)	ntfm	Specifies the foreigh key for 'cnt' obj_type to condition macro.
ci_notify_info	nvarchar (30)	ntfm	Specifies the foreigh key for 'ci' obj_type to condition macro.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.
ntfr_ntflist	LREL	ntfl	Associated Object Contacts
ntfr_ctplist	LREL	ctp	Associated Contact Types
ntfr_macrolist	LREL	macro	Macros (aty's) using this rule

Comments

This table contains the following topics:

O_COMMENTS Table

Program control table used by CA SDM Knowledge Management.

- **SQL Name** -- O_Comments
- **Object** -- O_Comments

Field	Data Type	Reference	Remarks
ASSIGNEE	UUID		SREL to the Contacts table.
CLOSE_DATE	DATE		Represents the timestamp of when this flag was closed.
CLOSE_DESC	nvarchar (50)		Displays the description when the flag is closed.
COMMENT_TEXT	nvarchar (255)		Displays comment text.
COMMENT_ TIMESTAMP	DATE		Indicates the timestamp of when this record was last created.
DEADLINE_DATE	DATE		Displays the date when the flag should be fixed by the user.
DOC_ID	INTEGER	SKELETONS :: id	Identifies the unique doc ID.
EMAIL_ADDRESS	nvarchar (75)		Identifies the email address.
FLG_CODE	nvarchar (50)		Prevents duplicate flags from being created for the same broken link.
FLG_STATUS	INTEGER	KT_FLG_ STATUS	Identifies the flag status as active or inactive.
FLG_TYPE	INTEGER		SREL to the KT_Flg_Type Table.
ID	INTEGER KEY		Unique (to the table) Numeric ID.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Indicates the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.
USER_ID	UUID	ca_contact: : uuid	Identifies the unique user ID
USER_NAME			Identifies the user name.

Field	Data Type	Reference	Remarks
	STRING 50		
VER_COUNT	INTEGER		Identifies the unique version ID and displays the number of versions created (1, 2, 3, 4...)

NR_Comment Table

Standard comments table.

- **SQL Name** -- nr_com
- **Object** -- nr_com

Field	Data Type	Reference	Remarks
attr_name	nvarchar (60)		For ITIL, this contains the Asset attribute that has changed.
com_comment	nvarchar (1000)		Identifies the comment text.
com_dt	INTEGER		Acts as the pointer to the parent row (nr_did), for the dt_comment written.
com_par_id	byte(16)	ca_owned_resource::uuid	Foreign key to the id field of the ca_owned_resource table, this is the Asset.
com_userid	nvarchar (40)		Identifies the userid of the commenting author.
id	INTEGER		Primary key of this table, this is a unique numeric ID.
new_value	nvarchar (1000)		For ITIL, this contains the new value of the Asset's attribute that has changed.
old_value	nvarchar (1000)		For ITIL, this contains the old value of the Asset's attribute that has changed.
writer_id	byte(16)		Primary key to the table, this is a unique identifier.

Promotion

This table contains the following topics:

- Object_Promotion Table (see page 3664)
- Promo_Hist Table (see page 3665)

Object_Promotion Table

Object Promotion definition for CA SDM application.

- SQL Name: object_promotion
- Object: object_promotion

Field	Data Type	Reference	Remarks
id	INTEGER		Unique numeric ID.
last_mod_dt	INTEGER		Indicates when the record was last modified.
last_mod_by	Byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified the record.
delete_flag	INTEGER		Specifies the default flag value for this access type.
object_name	nvarchar (60)		Provides the name of the promotable object.
description	nvarchar (512)		Provides the description of the promotable object.
start_date	INTEGER		Indicates the start date of promotable object.
end_date	INTEGER		Indicates the end date of promotable object.

Promo_Hist Table

Promotion History definition for CA SDM application.

- SQL Name: promo_hist
- Object: promo_hist

Field	Data Type	Reference	Remarks
id	INTEGER		Unique numeric ID.
last_mod_dt	INTEGER		Indicates when the record was last modified.
last_mod_by	Byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified the record.
created_user	nvarchar (255)		Name of the user who performed the operation.
description	nvarchar (512)		Provides the description of the executed operation.
start_date	INTEGER		Indicates the start date of the executed operation.
end_date	INTEGER		Indicates the end date of the executed operation.
package_name	nvarchar (255)		Package name of the executed operation.
promo_status	nvarchar (255)		Status of the executed operation.
promotion_cmd	nvarchar (255)		Promotion command of the executed operation.
report_file	nvarchar (255)		Report file name of the executed operation.
sdm_filter	nvarchar (512)		Filter of the executed operation.

status	INTEGER	Status code of the executed operation.
updated_user	nvarchar (255)	Name of the user who performed the operation.

Property

This table contains the following topics:

Property Table

Property value pairs for an object.

- **SQL Name** -- prp
- **Object** -- prp

Field	Data Type	Reference	Remarks
description	nvarchar(240)		Identifies the textual description of this property.
error_msg	STRING 240		Specifies the error message produced if validation fails.
id	INTEGER		Primary key of this table.
label	nvarchar(80)		Identifies the label value for this property.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
object_id	INTEGER	chg id	Identifies the unique (to the table) numeric ID.
object_type	nvarchar(30)		Specifies the short name of the object to which this property belongs.
owning_macro	BOP_REF_STR NOT_NULL	Spell_Macro	Specifies the Spell_Macro for validation.
persid	nvarchar(30)		Persistent ID (SystemObjectName:id).
property	INTEGER	Property_Template ::id	Foreign key to the id field of the prptpl table, this is the Template.
required	INTEGER	Boolean_Table:: enum	Specifies the Required field as follows:**0** -- Not required**1** -- Required
sample	nvarchar(240)		Indicates the sample value for this property.
sequence	INTEGER		Specifies the sequence value for this property.

Field	Data Type	Reference	Remarks
value_description	STRING 240		Text description of the value.
validation_rule	BOP_REF_STR NOT_NULL	Property_Validation_Rule	Identifies the valid value rule.
validation_type	BOP_REF_STR NOT_NULL	Property_Validation_Type	Identifies the type of validation rule.
value	nvarchar(240)		Specifies the value of the property.

Property_Template Table

Additional properties for objects.

- **SQL Name** -- prptpl
- **Object** -- prptpl

Field	Data Type	Reference	Remarks
code	nvarchar(12)		Specifies the non-editable handle for the query.
del	INTEGER	Active_Boolean_Table::enum	Deleted flag that indicates the following:**0** -- Active **1** -- Inactive/marked as deleted
description	nvarchar(240)		Specifies the textual description for the property template.
label	nvarchar(80)		Display the text for the property.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
object_attrname	nvarchar(30)		Specifies that this template belongs to the attribute name in the object.
object_attrval	INTEGER		Identifies the object attribute value, which drives the template attribute value.
object_type	nvarchar(30)		Specifies the short name of the object.
persid	nvarchar(30)		Persistent ID (SystemObjectName:id).
prptbl_id			Indicates the unique (to the table) numeric ID.
required	INTEGER NOT_NULL		Identifies the Required flag as follows:**0** -- Not Required**1** -- Required
sample	nvarchar(240)		Provides a sample, or Help text.
validation_rule	BOP_REF_STR NOT_NULL	Property_Validation_Rule	Identifies the valid value rule.
sequence	INTEGER		Specifies the display order.

Property_Validation_Rule Table

Property validation rule.

- **SQL Name** -- prpval_rule
- **Object** -- prpval_rule

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE NOT_NULL KEY		Specifies the primary key of this table.
persid	BOP_REF_STR		
del	INTEGER NOT_NULL		**0** -- Present **1** -- Not present
sym	STRING 30 UNIQUE NOT_NULL S_KEY		Specifies the name of the validation rule.
description	STRING 240		
validation_type	BOP_REF_STR	Property_Validation_ Type	Specifies the type of validation rule.
error_msg	STRING 240		Specifies the error message produced if validation fails.
owning_macro	BOP_REF_STR	Spell_Macro	Specifies the spell_Macro for validation.
label	LABEL_SYM NOT_NULL		Specifies the helper to pre-populate property template.
last_mod_dt	LOCAL_TIME		Indicates the timestamp indicating when this record was last modified.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.

Property_Validation_Type Table

Property validation type.

- **SQL Name** -- prpval_type
- **Object** -- prpval_type

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE NOT_NULL KEY		Specifies the primary key of this table.
persid	BOP_REF_STR		Persistent ID
del	INTEGER NOT_NULL		**0** -- Present **1** -- Not present

Field	Data Type	Reference	Remarks
sym	STRING 30 UNIQUE NOT_NULL S_KEY		Specifies the name of the validation rule.
description	STRING 240		
last_mod_dt	LOCAL_TIME		Indicates the timestamp indicating when this record was last modified.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.

Property_Value Table

Property values for an object.

- **SQL Name** -- prpval
- **Object** -- prpval

Field	Data Type	Reference	Remarks
id	INTEGER NOT_NULL		Specifies the primary key of this table.
persid	BOP_REF_STR		Specifies the persistent ID.
del	INTEGER NOT_NULL		**0** -- Present **1** -- Not present
sym	STRING 30 NOT_NULL S_KEY		Specifies the unique name of property value.
description	STRING 240		
owning rule	BOP_REF_STR NOT_NULL	Property_Validation_ Rule	Specifies the property validation rule this value applies to.
value	LONG_SYM NOT_NULL		Specifies the valid value.
is_default	INTEGER		**1** -- Default value for the rul/Pe
last_mod_dt	LOCAL_TIME		Specifies the last modified time.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified the record.

Query Policy

This article contains the following topics:

Query_Policy Table

Identifies the stored query event data for the Automated Policies feature in Knowledge Management.

- **SQL Name** -- query_policy
- **Object** -- query_policy

Field	Data Type	Reference	Remarks
ID	Long	Primary index.	Identifies the unique (to the table) numeric ID of the primary index.
persid	nvarchar (30)	Required field.	This is the Persistent ID.
Del	INTEGER (0/1)	Required field.	Deleted flag. **0** -- Active **1** -- Inactive/marked as deleted
last_mod_dt	Long (date)		Displays the last modified date.
last_mod_by	UUID	SREL to the ca_contacts table.	Displays the last date of when a user modified the record.
obj_type	nvarchar (30)	Required field. SREL to event_prod_list.	Kind of object for this event (knowledge document, and so forth).
query	nvarchar (30)	Required field. SREL to the cr_stored_queries.	Identifies the store query name.
sym	nvarchar (30)	Required field.	Identifies the policy name.
description	nvarchar (80)		Query policy description.

Query_Policy_Actions Table

Identifies the actions attached to the stored query event data for the Automated Policies feature in Knowledge Management. Each record represents a link between the macro and a query_policy record in the database.

- **SQL Name** -- query_policy_actions
- **Object** -- query_policy_actions

Field	Data Type	Reference	Remarks
ID	Long	Primary index.	Identifies the unique (to the table) numeric ID of the primary index.
policy	Long	Required field. SREL to query_policy.	Identifies the Policy ID.

Field	Data Type	Reference	Remarks
macro	STRING	Required field. SREL to splmac.	Identifies the action macro Persistent ID.
last_mod_dt	Long (date)		Displays the last modified date.
last_mod_by	UUID	SREL to the ca_contacts.	Displays the last date of when a user modified the record.

Request Property

This article contains the following topic:

Req_Property Table

Property value pairs for a Request.

- **SQL Name** -- cr_prp
- **Object** -- cr_prp

Field	Data Type	Reference	Remarks
description	nvarchar(240)		Specifies the textual description of this property.
error_msg	STRING 240		Specifies the error message produced if validation fails.
id	INTEGER		Primary key of this table, it is a unique, numeric ID.
label	nvarchar(80)		Specifies the label value for this Request property.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
owning_cr	nvarchar(30)	Call_Req::persid	Persistent ID (SystemObjectName:id)
owning_macro	BOP_REF_STR NOT_NULL	Spell_Macro	Specifies the Spell_Macro for validation.
required	INTEGER		Identifies the Required flag, as follows:**0** -- Not required**1** -- Required
sample	nvarchar(240)		The sample value for this Request_Property.
sequence	INTEGER		The sequence value for this Request property.
value_description	STRING 240		Text description of the value.
			Identifies the valid value rule.

Field	Data Type	Reference	Remarks
validation_rule	BOP_REF_STR NOT_NULL	Property_Validation_ Rule	
validation_type	BOP_REF_STR NOT_NULL	Property_Validation_ Type	Identifies the type of validation rule.
value	nvarchar(240)		Identifies the value of the property.

Req_Property_Template Table

Templates used to specify request properties.

- **SQL Name** -- cr_prptpl
- **Object** -- cr_prptpl

Field	Data Type	Reference	Remarks
description	STRING 240		Specifies the textual description of this template.
code	STRING 12 UNIQUE NOT_NULL S_KEY		Specifies the noneditable handle for query.
del	INTEGER NOT_NULL	Active_Boolean_ Table::enum	Deleted flag **0 --** Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
label	STRING 80 NOT_NULL		Specifies the display text for property.
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
owning_area	STRING 30 NOT_NULL	Prob_Category:: persid	Specifies the parent category.
persid	STRING 30		Persistent ID (SystemObjectName:id)
required	INTEGER NOT_NULL		**0** -- Not required
sample	STRING 240		Specifies the help text.
sequence	INTEGER NOT_NULL		Specifies the display order.
validation_rule	BOP_REF_STR NOT_NULL	Property_Validation_ Rule	Identifies the valid value rule.

Support Automation Table

This article contains the following topic:

sa_custom_category Table

Program control table used by Support Automation.

- **SQL Name** -- sa_custom_category
- **Object** -- sa_custom_category

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
categoryName	STRING 100		
isActive	INTEGER		NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_patch_history Table

Program control table used by Support Automation.

- **SQL Name** -- sa_patch_history
- **Object** -- sa_patch_history

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
patch_name	STRING 100		NOT_NULL
release_base	STRING 50		NOT_NULL
build_version	STRING 50		
epochq	LOCAL_TIME		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.

Field	Data Type	Reference	Remarks
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

SA_Policy Table

Policy information for dealing with automated creation and access of CA SDM components.

- **SQL Name** -- sapolicy
- **Object** -- sapolicy

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
persid	STRING 30		
del	INTEGER		NOT_NULL
sym	STRING 60		NOT_NULL
code	STRING 20		UNIQUE NOT_NULL S_KEY
description	STRING 300		
owning_policy	INTEGER	SA_Policy	
ticket_tmpl_fac	STRING 20		
ticket_tmpl_id	INTEGER		
ticket_tmpl_name	STRING 40		
is_default	INTEGER		
ret_usr_1	STRING 500		
ret_app_1	STRING 500		
dup_action	INTEGER		
dup_interval	DURATION		
is_internal	INTEGER		
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.

sa_portal_component Table

Program control table used by Support Automation.

- **SQL Name** -- sa_portal_component
- **Object** -- sa_portal_component

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
name	STRING 50		NOT_NULL
URL	STRING 255		NOT_NULL
beforeLogin	INTEGER		
afterLogin	INTEGER		
beforeProbDef	INTEGER		
afterProbDef	INTEGER		
displayColumn	INTEGER		
displayIndex	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

SA_Prob_Type Table

Problem type definitions used with automated creation policies within CA SDM applications.

- **SQL Name** -- saprobtyp
- **Object** -- saprobtyp

Field	Data Type	Reference	Remarks
description	STRING 300		Specifies the textual description.
code	STRING 20 UNIQUE NOT_NULL S_KEY		Specifies the unique code name.
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
dup_action	INTEGER		Specifies the enum for action to handle ticket duplication.
dup_interval	DURATION		Indicates the time range for searching duplicate tickets.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
is_default	INTEGER		

Field	Data Type	Reference	Remarks
			Specifies the one and only one for all policies.
is_internal	INTEGER	Active_Boolean_Table::enum	Specifies that the default problem types cannot be deleted.
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
owning_policy	INTEGER	SA_Policy::id	Specifies the owner of this problem type.
persid	STRING 30		Persistent ID (SystemObjectName:id)
ret_app_1	STRING 500		Specifies the text passed back to program for ticket creation.
ret_usr_1	STRING 500		Specifies the text passed back to human for ticket creation.
sym	STRING 40 NOT_NULL		Specifies the symobolic name of problem type.
ticket_tmpl_fac	STRING 20		Specifies the factory of the ticket template.
ticket_tmpl_id	INTEGER		Specifies the id of the ticket template.
ticket_tmpl_ name	STRING 40		Specifies the name of the ticket template

sa_property Table

Program control table used by Support Automation.

- **SQL Name** -- sa_property
- **Object** -- sa_property

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
propertyName	STRING 30		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_rejoin_code_mapping Table

Program control table used by Support Automation.

- **SQL Name** -- sa_rejoin_code_mapping
- **Object** -- sa_rejoin_code_mapping

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
rejoinCode	STRING 10		
rejoinString	STRING 100		
creationDate	LOCAL_TIME		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_rule_conduit_rule Table

Program control table used by Support Automation.

- **SQL Name** -- sa_rule_conduit_rule
- **Object** -- sa_rule_conduit_rule

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
functionName	STRING 100		NOT_NULL
className	STRING 100		
methodName	STRING 100		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_sound Table

Program control table used by Support Automation.

- **SQL Name** -- sa_sound
- **Object** -- sa_sound

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY

Field	Data Type	Reference	Remarks
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
soundName	STRING 255		
tenant	UUID	ca_tenant	

sa_sup_desk_hour_config Table

Program control table used by Support Automation.

- **SQL Name** -- sa_sup_desk_hour_config
- **Object** -- sa_sup_desk_hour_config

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
label	STRING 100		NOT_NULL
description	STRING 1024		
active	INTEGER		NOT_NULL
workshift	STRING 30	Bop_Workshift	
usehours	INTEGER	sa_hour_operation_mode	NOT_NULL
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_tenant_localization Table

Program control table used by Support Automation.

- **SQL Name** -- sa_tenant_localization
- **Object** -- sa_tenant_localization

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.

Field	Data Type	Reference	Remarks
toolInstanceID	INTEGER	sa_tool_instance_log	NOT_NULL
eventID	INTEGER	sa_event_history	NOT_NULL
tenant	UUID	ca_tenant	

sa_triage_script Table

Program control table used by Support Automation.

- **SQL Name** -- sa_triage_script
- **Object** -- sa_triage_script

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
queueID	INTEGER	sa_queue	NOT_NULL
scriptID	INTEGER	sa_script	NOT_NULL
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_data_routing_server Table

Program control table used by Support Automation.

- **SQL Name** -- sa_data_routing_server
- **Object** -- sa_data_routing_server

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
label	STRING 100		NOT_NULL
host	STRING 100		NOT_NULL
port	INTEGER		NOT_NULL
cssURL	STRING 150		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_datapool_channel Table

Program control table used by Support Automation.

- **SQL Name** -- sa_datapool_channel
- **Object** -- sa_datapool_channel

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
name	STRING 250		NOT_NULL
persistent	INTEGER		NOT_NULL
channelID	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_datapool_channel_user Table

Program control table used by Support Automation.

- **SQL Name** -- sa_datapool_channel_user
- **Object** -- sa_datapool_channel_user

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
channelID	INTEGER	sa_databpool_channel	NOT_NULL
sessionID	INTEGER	sa_login_session	NOT_NULL
snoop	INTEGER		NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_division_login_script Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_division_login_script

- **Object** -- sa_division_login_script

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
scriptText	INTEGER		
scriptName	STRING 128		
scriptDescription	STRING 32768		
scriptLanguage	STRING 24		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_division_role_join Table

Program control table used by Support Automation.

- **SQL Name** -- sa_division_role_join
- **Object** -- sa_division_role_join

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
roleID	INTEGER	sa_role	NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_division_tool_join Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_division_tool_join
- **Object** -- sa_division_tool_join

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
toolID	INTEGER	sa_tool	NOT_NULL
enabled	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.

Field	Data Type	Reference	Remarks
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_field Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_notif
- **Object** -- sa_notif

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
fieldType	INTEGER	sa_field_type	NOT_NULL
fieldName	STRING 50		NOT_NULL
fieldOrder	INTEGER		NOT_NULL
mandatory	INTEGER		NOT_NULL
active	INTEGER		NOT_NULL
displayName	STRING 150		
guestMandatory	INTEGER		NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_field_type Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_field_type
- **Object** -- sa_field_type

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
fieldType	INTEGER		NOT_NULL
fieldTypeDescription	STRING 255		NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt			

Field	Data Type	Reference	Remarks
	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_function_arg Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_function_arg
- **Object** -- sa_function_arg

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
functionID	INTEGER	sa_lib_function	NOT_NULL
arg_name	STRING 75		NOT_NULL
description	STRING 255		
index_value	INTEGER		NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_default_credential Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_default_credential
- **Object** -- sa_default_credential

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
Domain	STRING 255		
Login	STRING 255		NOT_NULL
Pwd	STRING 255		NOT_NULL
label	STRING 100		
active	INTEGER		

Field	Data Type	Reference	Remarks
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_display_template_loc Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_display_template_loc
- **Object** -- sa_display_template_loc

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
localizationID	INTEGER	sa_localizatio n	NOT_NULL
eventType	INTEGER	sa_event_typ e	NOT_NULL
displayTemplat e	STRING 510		NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_flow_control_rule Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_flow_control_rule
- **Object** -- sa_flow_control_rule

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
pageName	STRING 100		NOT_NULL
state	STRING 100		NOT_NULL
directedURL	STRING 500		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_alert_config_param Table

Program control table used by Support Automation.

- **SQL Name** -- sa_alert_config_param
- **Object** -- sa_alert_config_param

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
paramName	STRING 255		NOT_NULL
paramValue	INTEGER		NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_hour_operation_mode Table

Program control table used by Support Automation.

- **SQL Name** -- sa_hour_operation_mode
- **Object** -- sa_hour_operation_mode

Field	Data Type	Reference	Remarks
id	INTEGER		NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
sym	STRING 20		NOT_NULL
enum	INTEGER		NOT_NULL

sa_iss_template Table

Program control table used by Support Automation.

- **SQL Name** -- sa_iss_template
- **Object** -- sa_iss_template

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt			

Field	Data Type	Reference	Remarks
	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tpl	STRING 30	Iss_Template	NOT_NULL
is_default	STRING 50		NOT_NULL
isActive	INTEGER		NOT_NULL
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_large_data_record Table

Program control table used by Support Automation.

- **SQL Name** -- sa_large_data_record
- **Object** -- sa_large_data_record

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
recordID	INTEGER		NOT_NULL
recordOrder	INTEGER		NOT_NULL
originalTableName	STRING 100		
data	STRING 32768		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_lib_function Table

Program control table used by Support Automation.

- **SQL Name** -- sa_lib_function
- **Object** -- sa_lib_function

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
functionName	INTEGER		NOT_NULL
libFunction	INTEGER		NOT_NULL
funcDesc			

Field	Data Type	Reference	Remarks
	STRING 1024		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_group_event_join Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_group_event_join
- **Object** -- sa_group_event_join

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
groupID	INTEGER	sa_group	NOT_NULL
eventID	INTEGER	sa_event_history	NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_group_history Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_group_history
- **Object** -- sa_group_history

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
groupID	INTEGER	sa_group	NOT_NULL
startEpoch	LOCAL_TIME		NOT_NULL
endEpoch	LOCAL_TIME		NOT_NULL
sessionID	INTEGER	sa_login_session	NOT_NULL

Field	Data Type	Reference	Remarks
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_group_tool_invocation Table

Program control table used by Support Automation.

- **SQL Name** -- sa_group_tool_invocation
- **Object** -- sa_group_tool_invocation

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
groupID	INTEGER	sa_group	NOT_NULL
toolID	INTEGER	sa_tool	NOT_NULL
toolInstanceID	INTEGER	sa_tool_instance	NOT_NULL
toolStartEpoch	LOCAL_TIME		NOT_NULL
toolStartTime	STRING 50		
toolInstanceLogID	INTEGER	sa_tool_instance_log	
extraData	STRING 100		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_keyword Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_keyword
- **Object** -- sa_keyword

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
keyname	STRING 100		

Field	Data Type	Reference	Remarks
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_keyword_queue_join Table

Program control table used by Support Automation.

- **SQL Name** -- sa_keyword_queue_join
- **Object** -- sa_keyword_queue_join

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
keywordID	INTEGER	sa_keyword	NOT_NULL
queueID	INTEGER	sa_queue	NOT_NULL
weight	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_milepost Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_milepost
- **Object** -- sa_milepost

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
sessionID	INTEGER	sa_login_session	NOT_NULL
milepost	INTEGER		
epoch	LOCAL_TIME		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_milepost_history Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_milepost_history
- **Object** -- sa_milepost_history

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
sessionID	INTEGER	sa_login_session	NOT_NULL
milepost	INTEGER		NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_art_tool_avail Table

Program control table used by Support Automation.

- **SQL Name** -- sa_art_tool_avail
- **Object** -- sa_art_tool_avail

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
roleID	INTEGER	sa_role	
availBits	STRING 30		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_bin_temp Table

Program control table used by Support Automation.

- **SQL Name** -- sa_bin_temp
- **Object** -- sa_bin_temp

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
data	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_branding Table

Program control table used by Support Automation.

- **SQL Name** -- sa_branding
- **Object** -- sa_branding

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
localization	INTEGER	sa_localization	NOT_NULL
stylesheetURL	STRING 512		
header	STRING 32768		
footer	STRING 32768		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_comm_temp Table

Program control table used by Support Automation.

- **SQL Name** -- sa_comm_temp
- **Object** -- sa_comm_temp

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
data	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.

last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_cr_template Table

Program control table used by Support Automation.

- **SQL Name** -- sa_cr_template
- **Object** -- sa_cr_template

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tpl	STRING 30	Cr_Template	NOT_NULL
is_deafult	INTEGER		NOT_NULL
isactive	INTEGER		NOT_NULL
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_localization Table

Program control table used by Support Automation.

- **SQL Name** -- sa_localization
- **Object** -- sa_localization

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
localizationID	INTEGER		UNIQUE NOT_NULL
enabled	INTEGER		
name	STRING 100		
is_default	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_login_session Table

Program control table used by Support Automation.

- **SQL Name** -- sa_login_session
- **Object** -- sa_login_session

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca-contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
userID	UUID	ca_contact	
startEpoch	LOCAL_TIME		
endEpoch	LOCAL_TIME		
waitTime	INTEGER		
supportLength	INTEGER		
CanDownloadScriptApplets	INTEGER		
CanDownloadDlls	INTEGER		
CanRunAppletComms	INTEGER		
CanDownloadExes	INTEGER		
jvm	STRING 150		
NoPrompt	INTEGER		
ClientIsEXE	INTEGER		
Timezone	INTEGER		
availableTime	LOCAL_TIME		
unavailableTime	LOCAL_TIME		
browser	STRING 150		
DirectSessionCode	STRING 100		
Question	STRING 1024		
initialQueueID	INTEGER	sa_queue	
QueuedEpoch			

Field	Data Type	Reference	Remarks
	LOCAL_TIME		
QueuedTime	STRING 50		
OnHoldEpoch	LOCAL_TIME		
OnHoldTime	STRING 50		
HandledEpoch	LOCAL_TIME		
HandledTime	STRING 50		
GroupID	INTEGER	sa_group	
AbandonFlag	INTEGER		
IsCurrent	INTEGER		
SelfServe	INTEGER		
localizationID	INTEGER	sa_localization	
profileOverride	INTEGER		
AccessibilityExtEnabled	INTEGER		
IsWebClient	INTEGER		
CategoryID	INTEGER	sa_custom_category	
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_named_user_license Table

Program control table used by Support Automation.

- **SQL Name** -- sa_named_user_license
- **Object** -- sa_named_user_license

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
userID	UUID	ca_contact	NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_notif Table

Program control table used by Support Automation.

- **SQL Name** -- sa_notif
- **Object** -- sa_notif

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
notif_type	INTEGER		Specifies one of the following notification types: **1** -- Queue Entry Notification - end user joins Assistance Session Queue **2** -- Queue Entry Notification - Assistance Session is transferred to an Assistance Session Queue **3** -- reserved **4** -- Invite End User to Assistance Session - Incident **5** -- Invite End User to Assistance Session - Issue **6** -- Session Ended Notification
queue_id	INTEGER	sa_queue	REQUIRED
queued_user_id	INTEGER	sa_queued_user	
queued_group_id	INTEGER	sa_queued_group	
end_user_uuid	UUID	cnt	Specifies the UUID of the end user.
analyst_uuid	UUID	cnt	Specifies the UUID of the analyst.
sd_obj_type	STRING 5		Defines if the assistance session is integrated with iss, cr, or in.
sd_obj_id	INTEGER		Defines the cr/iss related record.
cr_persid_rel	STRING 30	Call_Req	Specifies the persid of the cr.
iss_persid_rel	STRING 30	Issue	Specifies the persid of the iss.
analyst_message	nvarchar (1024)		Specifies the text of the message sent by the analyst.
session_url	Long nvarchar		Specifies the URL of the assistance session.
msg_title	nvarchar (255)		Specifies the title of the nofitication.
msg_body	Long nvarchar		Specifies the description of the notification.
survey_id	INTEGER		Specifies the ID of the survey.

Field	Data Type	Reference	Remarks
survey_persid_rel	STRING 30		
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_sdconfig Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_sdconfig
- **Object** -- sa_sdconfig

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
propertyKey	STRING 50		NOT_NULL
propertyValue	STRING 512		

sa_sdgroup_map Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_sdgroup_map
- **Object** -- sa_sdgroup_map

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
groupID	INTEGER	sa_group	NOT_NULL
SDTicketID	STRING 50		NOT_NULL
SDRefNum	STRING 50		NOT_NULL
tenant	UUID	ca_tenant	

sa_sdsession_ticket_map Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_sdsession_ticket_map
- **Object** -- sa_sdsession_ticket_map

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
sessionID	INTEGER	sa_login_session	NOT_NUL
SDTicketID	STRING 50		NOT_NUL
SDRefNum	STRING 50		NOT_NUL
tenant	UUID	ca_tenant	

sa_system_message Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_system_message
- **Object** -- sa_system_message

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
messageTag	STRING 100		NOT_NULL
tenant	UUID	ca_tenant	
localizationID	INTEGER	sa_localization	NOT_NULL
messageText	STRING 1024		

sa_system_property Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_system_property

- **Object** -- sa_system_property

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	
propertyKey	STRING 300		NOT_NULL
propertyValue	STRING 32768		
propertyDescription	STRING 32768		
isGlobal	INTEGER		
obsolete	INTEGER		

sa_version Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_version
- **Object** -- sa_version

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
DBVersion	STRING 100		

sa_virtual_session Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_virtual_session
- **Object** -- sa_virtual_session

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt			

Field	Data Type	Reference	Remarks
	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
queueID	INTEGER	sa_queue	
userID	UUID	ca_contact	
sessionID	INTEGER	sa_login_session	
queuedEpoch	LOCAL_TIME		
handledEpoch	LOCAL_TIME		
endEpoch	LOCAL_TIME		
waitTime	INTEGER		
handledTime	INTEGER		
abandonFlag	INTEGER		
firstFlag	INTEGER		
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_wait_component Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_wait_component
- **Object** -- sa_wait_component

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.
queueID	INTEGER	sa_queue	
waitURL	STRING 300		
isExternal	INTEGER		
pagetype	INTEGER	sa_wait_component_type	

sa_wait_component_type Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_wait_component_type
- **Object** -- sa_wait_component_type

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
enum	INTEGER		
sym	STRING 50		
is_optional	INTEGER		

Support Automation - Security

This article contains the following topics:

sa_security_group Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_security_group
- **Object** -- sa_security_group

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	
groupName	STRING 50		NOT_NULL

Field	Data Type	Reference	Remarks
description	STRING 512		
rank	INTEGER		
localizationID	INTEGER		

sa_security_group_dir Table

Program control table that is used by Support Automation policies.

- **SQL Name** -- sa_security_group_dir
- **Object** -- sa_security_group_dir

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
groupID	INTEGER	sa_security_group	NOT_NULL
directory	STRING 150		
tenant	UUID	ca_tenant	

sa_security_group_function Table

Program control table that is used by Support Automation policies.

- **SQL Name** -- sa_security_group_function
- **Object** -- sa_security_group_function

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
groupID	INTEGER	sa_security_group	NOT_NULL
functionID	INTEGER	sa_security_tool_function	NOT_NULL
value	INTEGER		NOT_NULL
tenant	UUID	ca_tenant	

sa_security_group_loc Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_security_group_loc
- **Object** -- sa_security_group_loc

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
groupID	INTEGER	sa_security_group	NOT_NULL
localizationID	INTEGER	sa_localization	NOT_NULL
groupName	STRING 50		
description	STRING 512		
tenant	UUID	ca_tenant	

sa_security_grp_role_join Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_security_grp_role_join
- **Object** -- sa_security_grp_role_join

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
roleID	INTEGER	sa_role	NOT_NULL
groupID	INTEGER	sa_security_group	NOT_NULL
isDefault	INTEGER		NOT_NULL
tenant	UUID	ca_tenant	

sa_security_login_function Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_security_login_function
- **Object** -- sa_security_login_function

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
sessionID	INTEGER	sa_login_session	NOT_NULL
functionID	INTEGER	a_security_tool_function	NOT_NULL
value	INTEGER		NOT_NULL
localizationID	INTEGER		
tenant	UUID	ca_tenant	

sa_security_request_order Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_security_request_order
- **Object** -- sa_security_request_order

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
toolID	INTEGER	sa_tool	NOT_NULL
functionID	INTEGER	sa_security_tool_function	NOT_NULL
orderbit	INTEGER		NOT_NULL
tenant	UUID	ca_tenant	

sa_security_text_localized Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_security_text_localized
- **Object** -- sa_security_text_localized

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
TextID	INTEGER		NOT_NULL
localizationID	INTEGER	sa_localization	NOT_NULL
TextValue	STRING 100		NOT_NULL

sa_security_tool_function Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_security_tool_function
- **Object** -- sa_security_tool_function

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
toolID	INTEGER	sa_tool	NOT_NULL
functionName	STRING 50		
canPrompt	INTEGER		
localizationID	INTEGER	sa_localization	

sa_security_tool_localized Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_security_tool_localized
- **Object** -- sa_security_tool_localized

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
functionID	INTEGER	sa_security_tool_function	NOT_NULL
localizationID	INTEGER	sa_localization	NOT_NULL
functionName	STRING 100		
tenant	UUID	ca_tenant	

sa_security_user_directory Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_security_user_directory
- **Object** -- sa_security_user_directory

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
sessionID	INTEGER	sa_login_session	NOT_NULL
directory	STRING 150		NOT_NULL
tenant	UUID	ca_tenant	

Support Automation - Script

This topic contains the following information:

sa_script Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_script
- **Object** -- sa_script

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
scriptText	INTEGER		
scriptName	STRING 128		
scriptDescription	STRING 2000		
isLocked	INTEGER		
version	INTEGER		
GUID	STRING 255		
credLogin	STRING 50		
credPswd	STRING 255		
credDomain	STRING 50		
impersonate	INTEGER		
credentialsType	INTEGER		
disclaimer	INTEGER	sa_disclaimer	
surveyID	INTEGER	sa_survey	
percentShown	INTEGER		
loginRequired	INTEGER		
restrictFunctions	INTEGER		
scriptTimeout	INTEGER		
wsEnabled	INTEGER		
groupID	INTEGER	sa_script_group	NOT_NULL
last_mod_by	UUID	cnt	

Field	Data Type	Reference	Remarks
			Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_script_acquired_data Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_script_acquired_data
- **Object** -- sa_script_acquired_data

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
sessionID	INTEGER	sa_login_session	NOT_NULL
scriptID	INTEGER	sa_script	NOT_NULL
scriptInstanceID	INTEGER	sa_script_execution_log	NOT_NULL
epoch	LOCAL_TIME		NOT_NULL
acquiredData	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_script_exec_log_join Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_script_exec_log_join
- **Object** -- sa_script_exec_log_join

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
scriptInstanceID	INTEGER	sa_script_execution_log	NOT_NULL
eventID	INTEGER	sa_event_history	NOT_NULL
last_mod_by	UUID	cnt	

Field	Data Type	Reference	Remarks
			Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_script_exec_status Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_script_exec_status
- **Object** -- sa_script_exec_status

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
eventID	INTEGER	sa_event_history	NOT_NULL
scriptID	INTEGER	sa_script	NOT_NULL
executedStatus	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_script_execution_log Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_script_execution_log
- **Object** -- sa_script_execution_log

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
scriptID	INTEGER	sa_script	NOT_NULL
selfServeSessionID	INTEGER	sa_self_serve_session	NOT_NULL
sessionID	INTEGER	sa_login_session	NOT_NULL
executedEpoch	LOCAL_TIME		NOT_NULL

surveyShown	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_script_function_lib Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_script_function_lib
- **Object** -- sa_script_function_lib

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
scriptID	INTEGER	sa_script	NOT_NULL
libID	INTEGER	sa_scriptlib	NOT_NULL
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_script_group Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_script_group
- **Object** -- sa_script_group

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
groupName	STRING 128		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_script_role_join Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_script_role_join
- **Object** -- sa_script_role_join

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
scriptID	INTEGER	sa_script	NOT_NULL
roleID	INTEGER	sa_role	NOT_NULL
autorun	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_script_security_join Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_script_security_join
- **Object** -- sa_script_security_join

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
scriptID	INTEGER	sa_script	NOT_NULL
functionID	INTEGER	sa_security_tool_function	NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_script_user_field Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_script_user_field
- **Object** -- sa_script_user_field

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
fieldID	INTEGER	sa_field	NOT_NULL
scriptID	INTEGER	sa_script	NOT_NULL
isProfileField	INTEGER		NOT_NULL
tenant	UUID	ca_tenant	

sa_scriptlib Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_scriptlib
- **Object** -- sa_scriptlib

Field	Data Type	Reference	Remarks
id	INTEGER		NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
libName	STRING 128		NOT_NULL
libLang	INTEGER	sa_scriptlib_language	NOT_NULL
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.
active	INTEGER		NOT_NULL
version	INTEGER		NOT_NULL
islocked	INTEGER		
description	STRING 1024		

sa_scriptlib_language Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_scriptlib_language
- **Object** -- sa_scriptlib_language

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
sym	STRING 30		NOT_NULL
enum	INTEGER		NOT_NULL

Support Automation - Direct Session

This topic contains the following information:

sa_direct_session Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_direct_session
- **Object** -- sa_direct_session

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
code	STRING 100		NOT_NULL
groupID	INTEGER	sa_group	
expired	LOCAL_TIME		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_direct_session_page Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_direct_session_page
- **Object** -- sa_direct_session_page

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
stage	INTEGER		NOT_NULL

Field	Data Type	Reference	Remarks
epoch	LOCAL_TIME		NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_direct_session_preset Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_direct_session_preset
- **Object** -- sa_direct_session_preset

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
responseID	INTEGER	sa_chat_preset	NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

Support Automation - Event

This topic contains the following information:

sa_event_history Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_event_history
- **Object** -- sa_event_history

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
eventEpoch	LOCAL_TIME		NOT_NULL

Field	Data Type	Reference	Remarks
eventType	ITNEGER	sa_event_type	NOT_NULL
sd_obj_type	STRING 10		
sd_obj_id	INTEGER		
cr_rel	STRING 30	Call_Req	
iss_rel	STRING 30	Issue	
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_event_history_param Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_event_history_param
- **Object** -- sa_event_history_param

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
eventID	INTEGER	sa_event_history	NOT_NULL
paramID	INTEGER	sa_event_type_param	NOT_NULL
paramValue	STRING 4000		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_event_type Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_event_type
- **Object** -- sa_event_type

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
displayTemplate	STRING 255		

Field	Data Type	Reference	Remarks
eventDescription	STRING 50		
localizationID	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_event_type_param Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_event_type_param
- **Object** -- sa_event_type_param

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
paramName	STRING 255		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

Support Automation - Queue

This topic contains the following information:

sa_queue Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_queue
- **Object** -- sa_queue

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
queueName	STRING 100		NOT_NULL
isDefault	INTEGER		NOT_NULL
isActive	INTEGER		NOT_NULL
enableAutoMatching	INTEGER		NOT_NULL
enableAutoEscalation	INTEGER		NOT_NULL
escalationTimeout	INTEGER		
escalationTargetQueue	INTEGER	sa_queue	
customerDisplayName	STRING 100		NOT_NULL
onDeckPriority	INTEGER		
categoryID	INTEGER	sa_custom_category	
responseID	INTEGER	sa_chat_preset	
isscat_rel	STRING 30	Issue_Category	
pcat_rel	STRING 30	Prob_Category	
cr_template	STRING 30	Call_Req	
iss_template	STRING 30	Issue	
workshift	STRING 30	Bop_Workshift	
is_special	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_queue_hour_setting Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_queue_hour_setting

- **Object** -- sa_queue_hour_setting

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
queueID	INTEGER	sa_queue	NOT_NULL
url	STRING 2048		
isExternal	INTEGER		
useHours	INTEGER	sa_hour_operation_mode	
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_queue_localized Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_queue_localized
- **Object** -- sa_queue_localized

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
queueID	INTEGER	sa_queue	NOT_NULL
localizationID	INTEGER	sa_localization	NOT_NULL
customerDisplayName	STRING 100		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_queue_summary_field Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_queue_summary_field
- **Object** -- sa_queue_summary_field

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
fieldID	INTEGER	sa_field	NOT_NULL
fieldOrder	INTEGER		NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_queue_tool_join Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_queue_tool_join
- **Object** -- sa_queue_tool_join

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
queueID	INTEGER	sa_queue	NOT_NULL
toolID	INTEGER	sa_tool	NOT_NULL
displayOrder	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_queue_transfer_target Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_queue_transfer_target
- **Object** -- sa_queue_transfer_target

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
roleID	INTEGER	sa_role	NOT_NULL
queueID	INTEGER	sa_queue	NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_queued_group Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_queued_group
- **Object** -- sa_queued_group

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
queueID	INTEGER	sa_queue	NOT_NULL
groupID	INTEGER	sa_group	NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_queued_user Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_queued_user
- **Object** -- sa_queued_user

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
queueID	INTEGER	sa_queue	NOT_NULL
sessionID	INTEGER	sa_login_session	NOT_NULL
entryEpoch	LOCAL_TIME		
status	INTEGER		
user_route_rel	INTEGER	sa_user_route	
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

Support Automation - User and Role

This topic contains the following information:

sa_role Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_role
- **Object** -- sa_role

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
roleName	STRING 100		
isAgent	INTEGER		
defaultSecurityGroup	INTEGER		
joinSession	INTEGER		
allowSecLevelChange	INTEGER		
isActive	INTEGER		NOT_NULL
onDeck	INTEGER		NOT_NULL
allow_script_ide	INTEGER		
sa_client_launch_mode	INTEGER		
description	STRING 1024		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_role_queue_join Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_role_queue_join
- **Object** -- sa_role_queue_join

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
roleID	INTEGER	sa_role	NOT_NULL
queueID	INTEGER	sa_queue	NOT_NULL
isDefault	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_role_tool_join Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_role_tool_join
- **Object** -- sa_role_tool_join

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
roleID	INTEGER	sa_role	NOT_NULL
toolID	INTEGER	sa_tool	NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_role_tool_non_art_join Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_role_tool_non_art_join
- **Object** -- sa_role_tool_non_art_join

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
roleID	INTEGER	sa_role	NOT_NULL REF

Field	Data Type	Reference	Remarks
toolID	INTEGER	sa_tool_non_art	NOT_NULL REF
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.

sa_sd_user_map Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_sd_user_map
- **Object** -- sa_sd_user_map

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
SDUUID	UUID		NOT_NULL
tenant	UUID	ca_tenant	

sa_group Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_group
- **Object** -- sa_group

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
groupName	STRING100		
startEpoch	LOCAL_TIME		
endEpoch	LOCAL_TIME		
isCurrent	INTEGER		
ownerSessionID	INTEGER	sa_login_session	
status	INTEGER		
escalationDate	LOCAL_TIME		

Field	Data Type	Reference	Remarks
creatorUserID	UUID	ca_contact	
originalGroupID	INTEGER	sa_group	
categoryID	INTEGER	sa_custom_category	
groupType	INTEGER		
sd_obj_type	STRING 10		
sd_obj_id	INTEGER		
cr_rel	STRING 30	Call_Req	
iss_rel	STRING 30	Issue_Category	
user_route_rel	INTEGER	sa_user_route	
isscat_rel	STRING 30	Issue_Category	
pcat_rel	STRING 30	Prob_Category	
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_group_current_user Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_group_current_user
- **Object** -- sa_group_current_user

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
groupID	INTEGER	sa_group	NOT_NULL
sessionID	INTEGER	sa_login_session	NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_guest_agent_code Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_guest_agent_code
- **Object** -- sa_guest_agent_code

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
agentCode	STRING 5		NOT_NULL
groupID	INTEGER	sa_group	
createdEpoch	LOCAL_TIME		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_guest_profile Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_guest_profile
- **Object** -- sa_guest_profile

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
sessionID	INTEGER	sa_login_session	NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_guest_user_field Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_guest_user_field
- **Object** -- sa_guest_user_field

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
fieldID	INTEGER	sa_field	NOT_NULL

Field	Data Type	Reference	Remarks
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_agent_consult_history Table

Program control table used by Support Automation.

- **SQL Name** -- sa_agent_consult_history
- **Object** -- sa_agent_consult_history

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
userID	UUID	ca_contact	NOT_NULL
epoch	LOCAL_TIME		NOT_NULL
groupID	INTEGER	sa_group	
type	INTEGER		
targetID	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_user_alert_config Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_sa_user_alert_config
- **Object** -- sa_sa_user_alert_config

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
userID	UUID	ca_contact	NOT_NULL
AlertType	INTEGER		NOT_NULL
AlertTrigger	INTEGER		NOT_NULL
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_user_route Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_user_route
- **Object** -- sa_user_route

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
userID	UUID	ca_contact	
queue_id	INTEGER	sa_queue	
login_session_id	INTEGER	sa_login_session	
launch_type	INTEGER		
sd_obj_type	INTEGER		
sd_obj_id	STRING 10		
cr	STRING 30	Call_Req	
iss	STRING 30	Issue	
user_description	STRING 4000		
sdm_web_addrs	STRING 255		
isscat_rel	STRING 30	Issue_Category	
pcat_rel	STRING 30	Prob_Category	
priority	INTEGER	Priority	NOT_NUL
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_user_route_prop Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_user_route_prop
- **Object** -- sa_user_route_prop

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	

Field	Data Type	Reference	Remarks
			Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
login_session_id	INTEGER	sa_login_session	NOT_NULL
self_serve_session_id	INTEGER	sa_self_serve_session	
user_route	INTEGER	sa_user_route	
sequence	INTEGER		NOT_NULL
description	STRING 1024		
label	STRING 256		NOT_NULL
value	STRING 128		
required	INTEGER		
sample	STRING 128		
validation_rule	INTEGER	Property_Validation_Rule	
validation_type	INTEGER	Property_Validation_Type	
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.
persid	STRING 30		

sa_userdrserver_join Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_userdrserver_join
- **Object** -- sa_userdrserver_join

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
userID	UUID	ca_contact	NOT_NULL
drServerID	INTEGER	sa_data_routing_server	NOT_NULL

Field	Data Type	Reference	Remarks
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

Support Automation - Disclaimer

This topic contains the following information:

sa_disclaimer Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_disclaimer
- **Object** -- sa_disclaimer

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
disclaimerName	STRING 30		NOT_NULL
disclaimerText	INTEGER		NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_disclaimer_accept_log Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_disclaimer_accept_log
- **Object** -- sa_disclaimer_accept_log

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
selfServeSessionID	INTEGER	sa_self_serve_session	NOT_NULL
scriptID	INTEGER	sa_script	NOT_NULL
disclaimerID	INTEGER	sa_disclaimer	NOT_NULL
accepted	INTEGER		NOT_NULL
epoch			NOT_NULL

Field	Data Type	Reference	Remarks
	LOCAL_TIME		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_disclaimer_history Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_disclaimer_history
- **Object** -- sa_disclaimer_history

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
sessionID	INTEGER	sa_login_session	NOT_NULL
disclaimerID	INTEGER	sa_disclaimer	NOT_NULL
response	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_disclaimer_localized Table

Program control table used bySupport Automation.

- **SQL Name** -- sa_disclaimer_localized
- **Object** -- sa_disclaimer_localized

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
disclaimerID	INTEGER	sa_disclaimer	NOT_NULL
localizationID	INTEGER	sa_localization	NOT_NULL
disclaimerText	INTEGER		NOT_NULL

last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

Support Automation - Chat

This topic contains the following information:

sa_chat_preset Table

Program control table used by Support Automation.

- **SQL Name** -- sa_chat_preset
- **Object** -- sa_chat_preset

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
responseName	STRING 128		NOT_NULL
responseText	INTEGER		
responseTitle	STRING 128		
responseType	INTEGER	sa_chat_preset_type	NOT_NULL
categoryID	INTEGER	sa_chat_preset_category	NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_chat_preset_agent_cat Table

Program control table used by Support Automation.

- **SQL Name** -- sa_chat_preset_agent_cat
- **Object** -- sa_chat_preset_agent_cat

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
userID	UUID	ca_contact	NOT_NULL
groupID	INTEGER	sa_chat_preset_category	NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_chat_preset_cat_loc Table

Program control table used by Support Automation.

- **SQL Name** -- sa_chat_preset_cat_loc
- **Object** -- sa_chat_preset_cat_loc

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
groupID	INTEGER	sa_chat_preset_category	NOT_NULL
localizationID	INTEGER	sa_localization	NOT_NULL
name	STRING 256		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_chat_preset_category Table

Program control table used by Support Automation.

- **SQL Name** -- sa_chat_preset_category
- **Object** -- sa_chat_preset_category

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
groupName	STRING 128		
lastUpdateDate	LOCAL_TIME		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_chat_preset_localized Table

Program control table used by Support Automation.

- **SQL Name** -- sa_chat_preset_localized
- **Object** -- sa_chat_preset_localized

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
responseID	INTEGER	sa_chat_preset	NOT_NULL
localizationID	INTEGER	sa_localization	NOT_NULL
responseName	STRING 128		NOT_NULL
responseText	INTEGER		
responseTitle	STRING 128		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_chat_preset_type Table

Program control table used by Support Automation.

- **SQL Name** -- sa_chat_preset_type

- **Object** -- sa_chat_preset_type

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
enum	INTEGER		NOT_NULL
sym	STRING 20		NOT_NULL
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.

Support Automation - Static Content

This topic contains the following information:

sa_static_cont_script_join Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_static_cont_script_join
- **Object** -- sa_static_cont_script_join

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
scriptID	INTEGER	sa_script	NOT_NULL
itemID	INTEGER	sa_static_content	NOT_NULL
tenant	UUID	ca_tenant	

sa_static_content Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_static_content
- **Object** -- sa_static_content

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID		

Field	Data Type	Reference	Remarks
		ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	
GUID	STRING 255		
itemName	STRING 255		
itemDesc	STRING 255		
itemMimeType	STRING 50		
version	INTEGER		
isLocked	INTEGER		
itemContents	INTEGER		

Survey

This article contains the following topics:

sa_survey Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_survey
- **Object** -- sa_survey

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt			

Field	Data Type	Reference	Remarks
	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	
surveyName	STRING 32		NOT_NULL
question	STRING 512		NOT_NULL
responseType	INTEGER		NOT_NULL
isDeleted	INTEGER		

sa_survey_localized Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_survey_localizedg
- **Object** -- sa_survey_localizedg

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
surveyID	INTEGER	sa_survey	NOT_NULL
localizationID	INTEGER	sa_localization	NOT_NULL
question	STRING 512		NOT_NULL
tenant	UUID	ca_tenant	

sa_survey_result Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_sa_survey_result
- **Object** -- sa_sa_survey_result

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
surveyID	INTEGER	sa_survey	NOT_NULL

Field	Data Type	Reference	Remarks
selfServeSessionID	INTEGER	sa_self_serve_session	NOT_NULL
scriptID	INTEGER	a_script	NOT_NULL
response	INTEGER		
completion	INTEGER		NOT_NULL
SurveyComment	STRING 512		
surveyEpoch	LOCAL_TIME		
tenant	UUID	ca_tenant	

Survey Table

Customer Survey.

- **SQL Name** -- survey
- **Object** -- survey

Field	Data Type	Reference	Remarks
comment_label	nvarchar (80)		Specifies the comment label value for this Survey.
conclude_text	nvarchar (400)		Indicates the text to display after the survey is completed.
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive/marked as deleted
description	nvarchar (400)		Specifies the textual description for this survey.
id	INTEGER		Specifies the primary key of this table.
include_comment	INTEGER		Specifies the Include Comment flag, as follows: **0** -- No comment allowed
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
nx_comment	nvarchar (200)		Identifies the comment value for this Survey.
object_id	INTEGER		Identifies the ID of the object for this survey.
object_type	nvarchar (10)		Identifies the object type for this survey, for eample, CR, CHG, and so on.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).

Field	Data Type	Reference	Remarks
sym	nvarchar (12)		Identifies the symbolic name of this survey.

Survey_Answer Table

Customer Survey Answer.

- **SQL Name** -- survey_answer
- **Object** -- svy_ans

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_ Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive/marked as deleted
id	INTEGER		Primary key of this table.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
own_srvy_ question	INTEGER	Survey_Question :: id	Unique (to the table) numeric ID.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
selected	INTEGER		Identifies the selected value for this Survey_Answer.
sequence	INTEGER		Specifies the display order of the survey answers.
txt	nvarchar (400)		Specifies the question text.

Survey_Answer_Template Table

Customer Survey Answer Template.

- **SQL Name** -- survey_atpl
- **Object** -- svy_atpl

Field	Data Type	Reference	Remarks
atbl_id	INTEGER		Identifies the unique (to the table) numeric ID.
del	INTEGER	Active_Boolean_Tabl e::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive/marked as deleted
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.

Field	Data Type	Reference	Remarks
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
own_srvy_question	INTEGER	Survey_Question_Template::id	Unique (to the table) numeric ID.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
sequence	INTEGER		Specifies the display order of the survey answers.
txt	nvarchar (400)		Identifies the answer text.

Survey_Question Table

Customer Survey Question.

- **SQL Name** -- survey_question
- **Object** -- svy_ques

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive /marked as deleted
id	INTEGER		Primary key of this table.
include_qcomment	INTEGER		Specifies the Include Question Comment flag, as follows:**1** -- Include comment box for this question
last_mod_by	byte (16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
mult_resp_flag	INTEGER		Specifies the Multiple Response flag, as follows:**0** -- Choose 1 response (radio)**1** -- Choose "N" (check boxes)
owning_survey	INTEGER	Survey_id	Specifies the unique (to the table) numeric ID.
persid	nvarchar(30)		Persistent ID (SystemObjectName:id).
qcomment_ label	nvarchar(80)		Specifies the label for the comment.
resp_required	INTEGER		Specifies the Required Response flag, as follows:**1** -- Respondents must answer the question
response	INTEGER		Specifies the sequence number of the response.
sequence			Specifies the display order.

Field	Data Type	Reference	Remarks
	INTEGER		
txt	nvarchar (400)		Identifies the question text.

Survey_Question_Template Table

Customer Survey Question Template.

- **SQL Name** -- survey_qtpl
- **Object** -- svy_qtpl

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive /marked as deleted
id	INTEGER		Primary key of this table.
include_qcomment	INTEGER		Specifies the Include Question Comment flag, as follows:**1** -- Include comment box for this question
last_mod_by	byte (16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
mult_resp_flag	INTEGER		Specifies the Multiple Response flag, as follows:**0** -- Choose 1 response (radio)**1** -- Choose "N" (check boxes)
owning_survey	INTEGER	Survey_Template::id	Specifies the unique (to the table) numeric ID.
persid	nvarchar(30)		Persistent ID (SystemObjectName:id).
qcomment_label	nvarchar(80)		Specifies the label for the comment.
resp_required	INTEGER		Specifies the Required Response flag, as follows:**1 --** Respondents must answer the question
sequence	INTEGER		Specifies the display order of the survey questions.
txt	nvarchar(400)		Identifies the question text.

Survey_Stats Table

This table contains customer survey statistics.

- **SQL Name** -- survey_statistics
- **Object** -- svystat

Field	Data Type	Reference	Remarks
cyc_counter	INTEGER		Identifies the cycle counter to be compared against the cycle (described in the next field).
cycle	INTEGER		Identifies the submission cycle.
del	INTEGER	Active_Boolean_Table::enum	Specifies the status of the Deleted flag, as follows:**0** -- Active**1** -- Inactive/marked deleted)
eval_counter	INTEGER		Identifies the number of times called to evaluate for notification submission.
id	INTEGER		Primary key of this table.
persid	nvarchar (30)		Specifies the Persistent ID: (SystemObjectName:id).
sub_counter	INTEGER		Identifies the number of times notification submission was approved.
tplid	INTEGER	Survey_Template::id	Identifies the unique (to the table) numeric ID.

Survey_Template Table

Customer Survey Template.

- **SQL Name** -- survey_tpl
- **Object** -- svy_tpl

Field	Data Type	Reference	Remarks
comment_label	nvarchar (80)		Identifies the comment label value for this Survey_Template.
conclude_text	nvarchar (400)		Specifies the text to display after the survey has been completed.
cycle_counter	INTEGER		Indicates to keep a running count for Submit Cycle.
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive/marked as deleted
description	nvarchar (400)		Indicates the textual description for this template.
id	INTEGER		Primary key of this table.
include_comment	INTEGER		Specifies the Include Question Comment flag, as follows: **0** -- No comment allowed
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.

Field	Data Type	Reference	Remarks
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
submit_cycle	INTEGER		Indicates to send the survey every 'nth' time.
sym	nvarchar (12)		Identifies the symbolic name of the survey template.
tracking_flag	INTEGER		Specifies the flag to track responses.

Survey_Tracking Table

Table used to tack status of managed surveys.

- **SQL Name** -- survey_tracking
- **Object** -- svytrk

Field	Data Type	Reference	Remarks
cntid	byte(16)	ca_contact::uuid	Primary key of this table.
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive /marked as deleted
id	INTEGER		Primary key of this table, this is a unique numeric ID.
notif_dt	INTEGER		Specifies the time of the last notification.
object_id	INTEGER		Identifies the ID of the object for this survey.
object_type	nvarchar (10)		Indicates the object type for this survey, such as, CR, CHG, and so on.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
recv_dt	INTEGER		Identifies the time the completed survey was received.
status	INTEGER		Identifies the Status flag, as follows:**1** -- Survey submitted
tplid	INTEGER	Survey_Template ::id	Unique (to the table) numeric ID.

Managed_Survey Table

Stores the definition of the managed surveys.

- **SQL Name** -- managed_survey
- **Object** -- mgs

Field	Data Type	Reference	Remarks
create_date	INTEGER		Identifies when the managed survey was created.
del	INTEGER	Boolean_Table ::enum	Specifies the Deleted flag, as follows:**0** -- Active **1** -- Inactive/marked as deleted
description	nvarchar (400)		Identifies the textual description of this managed survey.
end_date	INTEGER		Specifies the end of survey period.
group_id	byte(16)		Foreign key to the contact_uuid field of the ca_contact table, this is the Group.
id	INTEGER		Primary key of this table.
initial_method	INTEGER	Contact_Method::id	Foreign key to the id field of the ct_mth table, this specifies the Contact Method.
initial_msgbody	nvarchar (1000)		Identifies the message body of the initial notification message.
initial_msgtitle	nvarchar (80)		Identifies the message title of the initial notification message.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
owner	byte(16)	ca_contact::uuid	Foreign key to the contact_uuid field of the ca_contact table, this specifies the Owner.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id)
reminder_method	INTEGER	Contact_Method::id	Foreign key to the id field of the ct_mth table, this is the Reminder Contact Method.
reminder_msgbody	nvarchar (1000)		Identifies the reminder message body of the initial notification message.
reminder_msgtitle	nvarchar (80)		Identifies the message title of the initial notification message.
start_date	INTEGER		Specifies the start of the survey period.
status	nvarchar (12)	Mgs_Status::code	Foreign key to the code field of the mgsstat table, this is the Status.
sym	nvarchar (12)		Identifies the symbolic name for this Managed Survey.
tplid	INTEGER	Survey_Template::id	Foreign key to the id field of the survey_tpl table, this is the Survey Template.

Support Automation - Agent

This topic contains the following information:

sa_agent_present_history Table

Program control table used by Support Automation.

- **SQL Name** -- sa_agent_present_history
- **Object** -- sa_agent_present_history

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
agentSessionID	INTEGER	sa_login_session	NOT_NULL
eventType	INTEGER		NOT_NULL
eventEpoch	LOCAL_TIME		NOT_NULL
agentUserID	UUID	ca_contact	
eventTime	STRING 50		
presentedItemType	INTEGER		
presentedItemID	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_agent_status_history Table

Program control table used by Support Automation.

- **SQL Name** -- sa_agent_status_history
- **Object** -- sa_agent_status_history

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
agentSessionID	INTEGER	sa_login_session	NOT_NULL
newStatus	INTEGER		NOT_NULL
statusChangeEpoch	LOCAL_TIME		NOT_NULL
agentUserID	UUID	ca_contact	

Field	Data Type	Reference	Remarks
statusChangeTime	STRING 50		
nextStatusChange Epoch	LOCAL_TIME		
nextStatusChange Time	STRING 50		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_agent_availability Table

Program control table used by Support Automation.

- **SQL Name**—sa_agent_availability
- **Object**—sa_agent_availability

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
agentID	UUID	ca_contact	NOT_NULL
queueID	INTEGER	sa_queue	NOT_NULL
status	INTEGER		
availEpoch	LOCAL_TIME		
clientSessionID	INTEGER	sa_login_session	
matchEpoch	LOCAL_TIME		
groupID	INTEGER	sa_group	
incidentCount	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

Sequence Control

Sequence_Control Table

Used to determine what to use for a prefix and suffix when generating call request numbers. Users may not create new records or delete records in this table.

- **SQL Name** -- seqctl
- **Object** -- seq

Field	Data Type	Reference	Remarks
description	STRING 240		Textual description
code	STRING 12 UNIQUE NOT_NULL S_KEY		noneditable key for record
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
prefix	STRING 5		Indicates the prefix to sequence number.
suffix	STRING 5		Indicates the suffix to sequence number.
sym	STRING 30 NOT_NULL		

Server

This topic contains the following information:

Server_Aliases Table

Contain server alias names that are valid for various server-client zones.

- **SQL Name** -- srvr_aliases
- **Object** -- srvr_aliases

Field	Data Type	Reference	Remarks
alias_name	STRING 30 NOT_NULL		Alias name

del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
host_addr	STRING 30		Translated Host Address
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
zone_id	INTEGER NOT_NULL	Server_Zones::id	Zone name

Server_Zones Table

Contain regional server zone names.

- **SQL Name** -- srvr_zones
- **Object** -- srvr_zones

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
is_default	INTEGER	Boolean_Table::enum	1 default zone
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
zone_name	STRING 30 NOT_NULL		Zone name

Service

This topic contains the following information:

Service_Contract Table

Used to track relationships between orgs, ticket attr's and svc types. Used for SLA management.

- **SQL Name** -- svc_contract
- **Object** -- svc_contract

Field	Data Type	Reference	Remarks
active	INTEGER	Active_Boolean_Table::enum	Specifies the status of the contract, as follows:**0** -- Inactive**1** -- Active
contract_num	nvarchar(50)		Identifies the Contract ID.
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive /marked as deleted
dflt_chgcat_st	nvarchar(30)	Service_Desc::code	Defines the default service type for the change category.
dflt_cnt_st	nvarchar(30)	Service_Desc::code	Defines the default service type for the end user.
dflt_isscat_st	nvarchar(30)	Service_Desc::code	Defines the default service type for the issue category.
dflt_nr_st	nvarchar(30)	Service_Desc::code	Defines the default service type for the asset.
dflt_pcat_st	nvarchar(30)	Service_Desc::code	Defines the default service type for the request area.
dflt_pri_st	nvarchar(30)	Service_Desc::code	Defines the default service type for the priority.
expiration	INTEGER		Specifies the Contract expiration date.
id	INTEGER		Primary key of this table.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
nx_desc	nvarchar(240)		Specifies descriptive information.
org_svc_type	nvarchar(30)	Service_Desc::code	Defines the service type for the organization.
persid	nvarchar(30)		Persistent ID (SystemObjectName:id).
svc_advocate	byte(16)	ca_contact::uuid	Identifies the customer advocate for the organizations assigned to the contract.
svc_owner	byte(16)	ca_contact::uuid	Foreign key to the contact_uuid field of the ca_contact table, this is the service desk person responsible for contract.
sym	nvarchar(80)		Specifies the symbolic name of the contract level.

Service_Desc Table

This table contains the Call Request Service Types that are not related to service level agreements in Problem Manager. These may be used to associate the types of service call requests to receive, and are can be defined by the user. Examples include: Platinum, Gold, Silver, or Bronze.

- **SQL Name** -- srv_desc
- **Object** -- sdsc

Field	Data Type	Reference	Remarks
code	nvarchar (30)		Specifies the primary key of this table.
del	INTEGER	Active_Boolean_ Table::enum	Specifies the status of the Deleted flag as follows:**0** -- Active **1** -- Inactive/marked as deleted
description	nvarchar (500)		Provides the text description of service.
id	INTEGER		Specifies the primary key of this table.
last_mod_ by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_ dt	INTEGER		Identifies the timestamp for when this record was last modified.
owning_co ntract	INTEGER	Service_Contract :: id	Specifies the unique (to the table) numeric ID.
persid	nvarchar (30)		Identifies the Persistent ID: (SystemObjectName:id)
rank	INTEGER		Identifies the ranking status of the service type to determine level of priority.
schedule	nvarchar (30)	Bop_Workshift:: persid	Foreign key to the peristent_id field of the bpwshft table, this is the Schedule.
sym	nvarchar (30)		Identifies the name of the service type.
violation_c ost	INTEGER		Specifies the monetary cost for violation.

Session

This topic contains the following information:

session_log Table

Session log.

- **SQL Name** -- session_log

- **Object** -- session_log

Field	Data Type	Reference	Remarks
contact	byte (16)	ca_contact::uuid	Foreign key to the contact_uuid field of the ca_contact table, this is the User.
id	INTEGER		Primary key of this table
login_time	INTEGER		Indicates the time of when the session began.
logout_time	INTEGER		Indicates the time of when the session ended.
policy	INTEGER	SA_Policy::id	Specifies the session policy.
session_id	INTEGER		Displays the ID if the status is okay.
session_type	INTEGER	session_type::id	Specifies the unique (to the table) numeric ID.
status	INTEGER		Identifies the Login status: **0** -- Okay

session_type Table

Session type (Web client, Java client, and so on).

- **SQL Name** -- session_type
- **Object** -- session_type

Field	Data Type	Reference	Remarks
description	nvarchar (500)		Identifies the description of the session type.
id	INTEGER		Primary key of this table.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id)
sym	nvarchar (30)		Identifies the name of the Session type.

Severity

List of severity definitions used by CA SDM applications.

- **SQL Name** -- sevrty
- **Object** -- sev

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_ Table:: enum	Identifies the Deleted flag as follows:**0** -- Active **1** -- Inactive/marked as deleted
enum	INTEGER		Primary key of this table.
id	INTEGER		Unique (to the table) numeric ID.
last_mod_ by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_ dt	INTEGER		Indicates the timestamp of when this record was last modified.
nx_desc	nvarchar (40)		Describes the severity.
sym	nvarchar (12)		Identifies the symbolic name for this severity.

Service Level Agreement

This topic contains the following information:

SLA_Contract_Map Table

Maps a service type to a reference object; used by Service_Contract objects.

- **SQL Name** -- sdsc_map
- **Object** -- sdsc_map

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_ by	UUID	ca_contact:: uuid	Specifies the UUID of the contact who last modified this record
last_mod_ dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
map_cont ract	INTEGER NOT_NULL	Service_Contra ct::id	
map_persi d	STRING 60		
map_sdsc	STRING 30	Service_Desc:: code	
persid	STRING 30		Persistent ID (SystemObjectName:id)

SLA_Template Table

Service Level Agreement Templates for Call and Change. Not related to service level agreements in problem manager. Links Service Descriptions with Events.

- **SQL Name** -- slatpl
- **Object** -- slatpl

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
elapsed	DURATION NOT_NULL		Specifies the elapsed time to delay event.
event	STRING 30	Events::persid	Specifies the event.
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified
object_type	STRING 30		Specifies the object type for this SLA (cr, chg).
persid	STRING 30		Persistent ID (SystemObjectName:id)
service_type	STRING 30 NOT_NULL	Service_Desc::code	
sym	STRING 30 NOT_NULL S_KEY		Specifies the name of the SLA.

Spell Macro

This topic contains the following information:

Spell_Macro Table

This table stores proprietary Spell macros and macro fragments.

- **SQL Name** -- splmac
- **Object** -- macro

Field	Data Type	Reference	Remarks
description	STRING 80		Identifies the text description.
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Specifies the Deleted flag status, such as: **0** -- Active **1** -- Inactive/marked as deleted
fragment	STRING 4000		
id	INTEGER UNIQUE NOT_NULL KEY		Identifies the Numeric ID that is unique to the table.
last_mod_dt	LOCAL_TIME		Indicates the timestamp for when this record was last modified.
lock_object	INTEGER NOT_NULL		Specifies the boolean of the object.
msg_html	STRING 32768		Identifies the message used to keep the html template.
ob_type	STRING 30 NOT_NULL		
persid	STRING 30		Identifies the Persistent ID: (SystemObjectName:id)
sym	STRING 30 NOT_NULL UNIQUE NOT_NULL		
type	STRING 30 NOT_NULL	Spell_Macro_Type::persid	
usr_integer1	INTEGER		
usr_integer2	INTEGER		
usr_integer3	INTEGER		
usr_string2	STRING 250		
usr_string3	STRING 125		
usr_string4	STRING 25		

Spell_Macro_Type Table

Stores type information for proprietary Spell macros and macro fragments .

- **SQL Name** -- splmactp
- **Object** -- macro_type

Field	Data Type	Reference	Remarks
description	STRING 200		Textual description
arg_list	STRING 80		
code	STRING 30 UNIQUE NOT_NULL NOT_NULL		
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
display_name	STRING 30		form name to display
execute_script	STRING 800		
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
lock_object_ flag	INTEGER		
persid	STRING 30		Persistent ID (SystemObjectName:id)
sym	STRING 30 NOT_NULL		
tech_desc	STRING 300		
validate_script	STRING 400		

Show Object

Show_Obj Table

Program control table used by Knowledge Management.

- **SQL Name** -- SHOW_OBJ
- **Object** -- SHOW_OBJ

Field	Data Type	Reference	Remarks
EXPIRE_DATE	LOCAL_TIME		
ID	INTEGER KEY		Unique (to the table) Numeric ID
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
OBJ_PERSID	STRING 255		Persistent ID (SystemObjectName:id)
PWD	STRING 255		

SQL Script

This article contains the following topics:

SQL_Script Table

Stores SQL scripts used by the CA SDM applications.

- **SQL Name** -- sql_tab

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL		Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
sql_desc	STRING 240		user title for script
sql_name	STRING 30 S_KEY		user name for script
sql_script	STRING 500		actual script

Pcat_Loc Table

The following tables are added to support many-to-many relationships between Categories, Groups that can service the Categories, and Locations that groups are able to service. This is all used for the Auto-Assignment functionality. Used to build a list of Service Locations valid for the Category.

- **SQL Name** -- pcat_loc
- **Object** -- pcat_loc

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
l_attr	STRING 30		left hand attribute name
l_persid	STRING 60		left hand key
l_sql	INTEGER		left hand sort order
r_attr	STRING 30		right hand attribute name
r_persid	STRING 60		right hand key
r_sql	INTEGER		right hand sort order

Person_Contacting Table

Reference table to denote the type of customer that made the contact. For example, the consumer, lawyer, media, and so on.

- **SQL Name** -- perscon
- **Object** -- perscnt

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL	Active_Boolean_Table::enum	Deleted flag that indicates the following:**0** -- Active **1** -- Inactive/marked as deleted
id	INTEGER		Primary key of this table.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
persid	nvarchar(30)		Persistent ID (SystemObjectName:id)
sym	nvarchar(60)		The symbolic value for this Person_Contacting.

pr_trans Table

A transition object controls the current and next ticket status. The pr_trans table lists the status, new status, and actions that need to occur for a default transition.

- **SQL Name** -- pr_trans
- **Object** -- pr_trans

Label	Field	Description
id	INTEGER	Unique key.
status	SYMBOL	Specifies the current ticket status.
new_status	SYMBOL	Specifies the new ticket status
must_comment	INTEGER	Comment required when using a transition. On new default: 0
is_default	INTEGER	Default transition that appears when the Status field is empty. On new default: 0
condition	BOP_REF_STR_REF Macro	Site condition macro to approve transition.
condition error	STRING 255	Error message for site condition.
description	STRING 255	Description of this transition.
last_mod_dt	LOCAL_TIME	Timestamp of last update to this record.

Label	Field	Description
last_mod_by	UUID REF ca_contact	User who last updated this.
del	INTEGER nn	Logical database delete status.
tenant	UUID REF ca_tenant	Reference to Tenant information.

Impact

Impact is a measure of the significance of an event by the user. It is used on Incident Reports.

- **SQL Name** -- impact
- **Object** -- imp

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive /marked as deleted
enum	INTEGER		Primary key for this table.
id	INTEGER		Specifies the unique (to the table) numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
nx_desc	nvarchar (40)		Specifies the textual description of this impact.
sym	nvarchar (12)		Identifies the symbolic value for this impact.
value	INTEGER		Shows the numeric representation of this impact.

Web Screen Painter

This article contains the following topics:

wspcol Table

There are one to three rows in this table for every column created or updated by WSP. The columns table_name+column_name+status form a unique key. See also comments in wsp.maj.

- **SQL Name** -- wspcol
- **Object** -- wspcol

Field	Data Type	Reference	Remarks
description	STRING 300		Description

Field	Data Type	Reference	Remarks
addl_info	STRING 500		Triggers, QREL stuff, and so on.
column_name	STRING 40 NOT_NULL		Column Majic name
dbms_name	STRING 40		DBMS schema name
display_name	STRING 80		Human-readable name
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
is_cluster	INTEGER		1 = DBMS cluster index
is_descending	INTEGER		1 = DBMS descending index
is_indexed	INTEGER		1 = DBMS-indexed column
is_local	INTEGER		1 = local column
is_not_null	INTEGER		1 = column cannot be null
is_order_by	INTEGER		1 = DBMS order by index
is_required	INTEGER		1 = column required
is_skey	INTEGER		1 = column is secondary key
is_unique	INTEGER		1 = DBMS unique index
is_write_new	INTEGER		1 = read-only after creation
is_wsp	INTEGER		1 = table created by WSP
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
on_ci_set	STRING 80		Value to set on update
on_new_default	STRING 80		Default value of attribute
persid	STRING 30		Persistent ID (SystemObjectName:id)
schema_name	STRING 40		CA SDM schema name
status	INTEGER NOT_NULL		Modification status
string_len	INTEGER		String len
table_name	STRING 40 NOT_NULL		Table Majic name
type	INTEGER		Column type
xrel_table	STRING 80		Operand of SRELBRELQREL

wsptbl Table

There are one to three rows in this table for every table created or updated by WSP. The columns table+name+status form a unique key. See also comments in wsp.maj for interpretation of integer codes.

- **SQL Name** -- wsptbl
- **Object** -- wsptbl

Field	Data Type	Reference	Remarks
description	STRING 300		Identifies the description of the table.
common_name	STRING 40		Specifies the name for the identification column.
dbms_name	STRING 40		Specifies the DBMS schema name.
display_group	STRING 40		Identifies the Grouping to display.
display_name	STRING 80		Specifies the user-readable name.
function_group	STRING 40		Identifies the Security function group.
id	INTEGER UNIQUE NOT_NULL KEY		Specifies the numeric ID, which is also unique to the table.
is_local	INTEGER		Identifies whether the table is local (1 = local table).
is_wsp	INTEGER		Identifies whether the table is created by WSP (1 = table created by WSP).
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Identifies the timestamp for when this record was last modified.
methods	STRING 500		Identifies Spell methods.
persid	STRING 30		Identifies the Persistent ID: (SystemObjectName:id)
rel_attr	STRING 40		Specifies the Foreign key column.
schema_name	STRING 40		Specifies the CA SDM schema name.
sort_by	STRING 150		Specifies the Default sort sequence.
status	INTEGER NOT_NULL		Identifies the Modification status.
table_name	STRING 40 NOT_NULL		Specifies the Table Majic name.
triggers	STRING 500		Identifies any Triggers for the table.

USP Window

This article contains the following topics:

usp_window Table

Contains information on the blackout and maintenance window.

- **SQL Name** -- usp_window
- **Object** -- window

Column	Type	Remarks
id	INTEGER	UNIQUE NOT_NULL KEY
sym	INTEGER	UNIQUE Name of window
window_type	INTEGER	REQUIRED References usp_window_type and specifies blackout or maintenance.
start_date	LOCAL_TIME	REQUIRED Start date of first recurrence
end_date	LOCAL_TIME	REQUIRED End date of first recurrence
final_end_date	LOCAL_TIME	REQUIRED End date of last recurrence
timezone	STRING 30	Timezone
icon	STRING 100	URL to icon
recurs	INTEGER	Specifies the following: **0** -- None **1** -- Daily **2** -- Weekly **3** -- Monthly **4** -- Annually
recurrence_interval	INTEGER	Days, weeks, months, or years
sunday	INTEGER	Restricts daily or weekly recurrence
monday	INTEGER	Restricts daily or weekly recurrence
tuesday	INTEGER	Restricts daily or weekly recurrence
wednesday	INTEGER	Restricts daily or weekly recurrence
thursday	INTEGER	Restricts daily or weekly recurrence
friday	INTEGER	Restricts daily or weekly recurrence

Column	Type	Remarks
saturday	INTEGER	Restricts daily or weekly recurrence
occurrence	INTEGER	Restricts monthly or yearly recurrence **1** -- First **2** -- Second **3** -- Third **4** -- Fourth **5** -- Last
description	STRING 400	Text of window
legend	STRING 100	Legend on the Change Calendar
color	STRING 100	Web color of text
bgcolor	STRING 100	Web background color
style	STRING 100	Text style (italic, bold or normal)
last_mod_dt	LOCAL_TIME	Indicates the timestamp of when this record was last modified.
last_mod_by	UUID	Specifies the UUID of the contact who last modified this record.
del	INTEGER	
tenant	UUID	References the ca_tenant table.

The significance of recurrence_interval, occurrence, and the weekday attributes (sunday, monday, and so on) depend on the value of recurs:

- **1 (daily)**
  Specifies the days on which the event recurs.
  If the recurrence_interval is greater than one, the weekday attributes are ignored, and the event recurs at the interval you specified. Occurrence is ignored.

- **2 (weekly)**
  Specifies the number of weeks between recurrences, and the weekday attributes specify the days within the week the window recurs. Occurrence is ignored.

- **3 (monthly)**
  Specifies the number of months between occurrences.
  If the occurrence is zero, the recurrence is always on the day of the month of the start_date. If the occurrence is non-zero, it specifies that recurrence occurs in the first, second, third, fourth, or last week of the month on the weekday of the start_date (which will be the only non-zero weekday attribute).

- **4 (yearly)**
  Specifies the number of years between occurrences.
  If the occurrence is zero, the recurrence is always on the date of the start_date. If the occurrence is non-zero, it specifies that recurrence occurs in the first, second, third, fourth, or last week of the month on the weekday of the start_date (which will be the only non-zero weekday attribute).

usp_window_type Table

Contains information on blackout and maintenance windows.

- **SQL Name** -- usp_window_type
- **Object** -- window_type

Column	Type	Remarks
id	INTEGER	UNIQUE NOT_NULL KEY
del	INTEGER	NOT_NULL
sym	STRING 60	NOT_NULL S_KEY
description	STRING 100	
last_mod_by	UUID	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME	Indicates the timestamp of when this record was last modified.

Role Table

This article contains the following topics:

usp_role Table

Contains the information on the Roles.

- **SQL Name** -- usp_role
- **Object** -- role

Column	Type	Remarks
id	INTEGER	
admin	INTEGER	Admin Function Access
call_mgr	INTEGER	Requests Function Access
change_mgr	INTEGER	Change Orders Function Access
code	STRING 30	Code
data_partition	SREL dmn	
default_flag	INTEGER	Default
description	STRING (1024)	Description
form_group	SREL fmgrp	
grant_level	SREL acc_lvls	
help_view	SREL help_set	
initial_form	STRING (256)	Initial Form

Column	Type	Remarks
interface_type	INTEGER	Interface Type
inventory	INTEGER	Inventory Function Access
issue_mgr	INTEGER	Issues Function Access
kcat	INTEGER	
kd	INTEGER	
kd_query_description	STRING (255)	
kd_query_id	SREL crsq	
kt_admin	INTEGER	Knowledge System Administrator
kt_analyst	INTEGER	Knowledge Analyst
kt_customer	INTEGER	Knowledge Customer
kt_engineer	INTEGER	Knowledge Engineer
kt_manager	INTEGER	Knowledge Manager
kt_type	INTEGER	kt type
name	STRING (80)	Role Name
notify	INTEGER	Notify Function Access
override_cnt_datapart	INTEGER	Override Contact Data Partition
pref_doc	INTEGER	Preferred Document
reference	INTEGER	Reference Function Access
sd_admin	INTEGER	CA SDM System Administrator
sd_analyst	INTEGER	CA SDM Analyst
sd_customer	INTEGER	CA SDM Customer
sd_employee	INTEGER	CA SDM Employee
security	INTEGER	Security Function Access
single_tenant	SREL tenant	
tenant	SREL tenant	
tenant_access	INTEGER	Tenant Access
tenant_group	SREL tenant_group	
tn_admin	INTEGER	
update_global	INTEGER	Update Global
view_internal	INTEGER	View Internal

usp_role_go_form Table

Links between Roles and Go Form type Web Forms.

- **SQL Name** -- usp_role_go_form
- **Object** -- role_go_form

Field	Data Type	Reference	Remarks
id	INTEGER		Specifies the unique (to the table) numeric ID.
is_default	INTEGER		Indicates if this is the default Go Form for the role.
role_obj	INTEGER	usp_role::id	Foreign key to the role_id field of the usp_role table.
web_form_obj	INTEGER	usp_web_form::id	Foreign key to the web form id field of the usp_web_form table.
menu_bar_obj	INTEGER	usp_menu_bar::id	Foreign key to the menu bar id field of the usp_menu_bar table.

usp_role_tab Table

Links between Roles and their Tabs.

- **SQL Name** -- usp_role_tab
- **Object** -- role_tab

Field	Data Type	Reference	Remarks
id	INTEGER		Specifies the unique (to the table) numeric ID.
sequence	INTEGER		Used to order the role's tabs in the web interface.
role_obj	INTEGER	usp_role::id	Foreign key to the role_id field of the usp_role table.
tab_obj	INTEGER	usp_tab::id	Foreign key to the tab id field of the usp_tab table.

usp_role_web_form Table

Links between Roles and Report type Web Forms.

- **SQL Name** -- usp_role_web_form
- **Object** -- role_web_form

Field	Data Type	Reference	Remarks
id	INTEGER		Specifies the unique (to the table) numeric ID.
role_obj	INTEGER	usp_role::id	Foreign key to the role_id field of the usp_role table.
web_form_obj	INTEGER	usp_web_form::id	Foreign key to the web form id field of the usp_web_form table.

usp_acctyp_role Table

Links between Activity Types and Roles.

- **SQL Name** -- usp_acctyp_role

- **Object** -- acctyp_role

Field	Data Type	Reference	Remarks
access_type	INTEGER	Access_Type_v2::id	Foreign key to access type id in Access_Type_v2.
id	INTEGER		Specifies the unique (to the table) numeric ID.
is_default	INTEGER		Specifies if this is the default role for this access type. 1 = default
role_obj	INTEGER	usp_role::id	Foreign key to the role_id field of the usp_role table.

Contact

This article contains the following topics:

usp_contact Table

This table provides extensions to the ca_contact table that are used only by CA SDM products.

- **SQL Name** -- usp_contact
- **Object** -- cnt

Field	Data Type	Reference	Remarks
c_acctyp_id	INTEGER	Access_Type::id	Identifies the unique (to the table) numeric ID.
c_available	INTEGER		Displays as a check box to indicate that the analyst is available.
c_cm_id1	INTEGER	Contact_Method::id	Foreign key to the id field of the ct_mth table, this identifies the low priority of the contact method.
c_cm_id2	INTEGER	Contact_Method::id	Foreign key to the id field of the ct_mth table, this identifies the next level of low priority for the contact method.
c_cm_id3	INTEGER	Contact_Method::id	Foreign key to the id field of the ct_mth table, this identifies the standard level of priority for the contact method.
c_cm_id4	INTEGER	Contact_Method::id	Foreign key to the id field of the ct_mth table, this identifies the high level of priority for the contact method.
c_domain	INTEGER	Domain:id	Foreign key to the id field of the dmn table, this is the Data Partition.
c_email_service	nvarchar 30		(Not used by CA SDM) Identifies the pointer to the access type email service (such as, PROFS, and so on).
c_nx_ref_1	byte (16)		Foreign key to the contact_uuid field of the ca_contact table, this is a user-defined field.

Field	Data Type	Reference	Remarks
c_nx_ref_2	byte (16)		Foreign key to the contact_uuid field of the ca_contact table, this is a user-defined field.
c_nx_ref_3	byte (16)		Foreign key to the contact_uuid field of the ca_contact table, this is a user-defined field.
c_nx_string1	nvarchar(40)		Identifies the emergency Workshift 4 Smag fields.
c_nx_string2	nvarchar(40)		Allows for a user-defined string field.
c_nx_string3	nvarchar(40)		Allows for a user-defined string field.
c_nx_string4	nvarchar(40)		Allows for a user-defined string field.
c_nx_string5	nvarchar(40)		Allows for a user-defined string field.
c_nx_string6	nvarchar(40)		Allows for a user-defined string field.
c_parent	byte (16)		(Not used in CA SDM) Foreign key to the contact_uuid field of the ca_contact table.
c_schedule	nvarchar 30	Bop_Workshift::persid	Foreign key to the persistent_id field of the bpwshft table, this is the Analyst's workshift for Auto Assignment.
c_service_type	nvarchar 30	Service_Desc::code	Foreign key to the code field of the srv_desc table, this identifies the Classic Service Type.
c_timezone	nvarchar(12)	Timezone::code	Foreign key to the code field of the tz table, this defines the Timezone.
c_val_req	INTEGER		Specifies a Force validation of the userid.
c_vendor	byte (16)	ca_company::company_uuid	Foreign key to the id filed of the ca_company table, this represents the Vendor.
c_ws_id1	nvarchar 30	Bop_Workshift::persid	Foreign key to the persistent_id field of the bpwshft table, this represents a workshift ID.
c_ws_id2	nvarchar 30	Bop_Workshift::persid	Foreign key to the persistent_id field of the bpwshft table, this represents a workshift ID.
c_ws_id3	nvarchar 30	Bop_Workshift::persid	Foreign key to the persistent_id field of the bpwshft table, this represents a workshift ID.
c_ws_id4	nvarchar 30	Bop_Workshift::persid	Foreign key to the persistent_id field of the bpwshft table, this represents a workshift ID.
contact_uuid	byte (16)		Primary key of this table.
global_queue_id	INTEGER	Global_Queue_Names::id	Specifies the pointer to the global queue.
ldap_dn	nvarchar(512)		Identifies the ldap dn value for this usp_contact.

usp_contact_handling Table

The usp_contact_handling table associates contacts with a special handling classification.

Attribute	Data Type	SREL References	Flags
contact	UUID	ca_contact	NOT_NULL
id	INTEGER		UNIQUE NOT_NULL KEY
special_handling	INTEGER	usp_special_handling	NOT NULL
tenant	UUID	ca_tenant	

usp_credentials_Table

The usp_credentials table contains all the UNC credential details to access UNC shared drive in the Advance availability configuration.

Attribute	Data Type	Reference	Description
id	INTEGER		Specifies the primary key of this table.
persid	STRING		Persistent ID.
del	INTEGER		Deleted flag 0 = Active 1 = Inactive or marked as deleted.
sym	INTEGER		60 NOT_NULL UNIQUE NOT_NULL S_KEY
description	STRING 500		Textual description of the UNC Credentials details.
unc userid	STRING		User name used for authentication to access the UNC shared drive.
unc password	STRING		Password in encrypted format to access UNC shared drive.
last_mod_dt	LOCAL_TIME		Timestamp of when the record was last modified.
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
tenant	UUID	ca_tenant	

usp_rest_access Table

The following table lists the usp_rest_access attributes:

- **SQL Name** -- usp_rest_access
- **Object** -- rest_access

Field	Data Type	Reference	Remarks
id	INTEGER		Primary key to this table, it is a unique numeric ID.
access_key	INTEGER		UNIQUE

contact	UUID	ca_contact	Specifies the UUID of the contact.
secret_key	STRING 64		Encrypted shared secret key value.
expiration_date	LOCAL_TIME		Specifies the expiration date of the REST Access Key.

Resolution

This article contains the following topics:

usp_resolution_code Table

The usp_resolution_code table details the categorization of the incident/request resolution.

- **SQL Name** -- usp_resolution_code
- **Object** -- resocode

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
persid	STRING 30		Persistent ID
del	INTEGER NOT NULL	Active_Boolean_ Table::enum	Deleted flag **0** -- active **1** -- inactive/marked as deleted
sym	STRING 128 UNIQUE NOT_NULL S_KEY		
last_mod_dt	LOCAL_TIME		Timestamp of when this record was last modified.
last_mod_by	UUID REF	ca_contact	Specifies the UUID of the contact who last modified this record.
description	STRING 240		Textual description of the root cause.
tenant	UUID REF	ca_tenant	

usp_resolution_method Table

The usp_resolution_method table details how the incident was resolved or how the service was restored.

- **SQL Name** -- usp_resolution_method
- **Object** -- resomethod

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
persid	STRING 30		Persistent ID
del	INTEGER NOT NULL	Active_Boolean_ Table::enum	Deleted flag **0** -- active **1** -- inactive/marked as deleted
sym	STRING 128 UNIQUE NOT_NULL S_KEY		
last_mod_dt	LOCAL_TIME		Timestamp of when this record was last modified.
last_mod_by	UUID REF	ca_contact	Specifies the UUID of the contact who last modified this record.
description	STRING 240		Textual description of the root cause.
tenant	UUID REF	ca_tenant	

USP Menu

This article contains the following topics:

usp_menu_bar Table

Contains the information on the menu bars used in the Role Based UI.

- **SQL Name** -- usp_menu_bar
- **Object** -- menu_bar

Column	Type	Remarks
id	INTEGER	
name	STRING (80)	Name of the role.
code	STRING 30	Code
del	INTEGER	Active_Boolean_Table::enum
description	STRING (255)	Description
htmpl_name	STRING (40)	Name of the HTMPL file containing the menu bar

usp_menu_tree Table

Each record is a node in a menu tree used in the Role Based UI.

- **SQL Name** -- usp_menu_tree
- **Object** -- menu_tree

Field	Data Type	Reference	Remarks
id	INTEGER		
caption	STRING (50)		Caption displayed for the menu tree node
description	STRING (255)		Description
has_childrenn	INTEGER		0 indicates that this is a leaf node on the menu tree. 1 indicates that this node has child nodes.
parent_id	INTEGER		The id of the parent menu_tree node if this is a child node.
mt_resource	INTEGER	usp_menu_tree_res::id	The id of the usp_menu_tree_res that contains the resource for this node. Empty if this node is a label node only.
tree_name	INTEGER	usp_menu_tree_name::id	The id of the usp_menu_tree_name record for this menu_tree.
internal	INTEGER	Boolean_Table::enum	Indicates if this menu tree is delivered out-of-box. If so, the menu tree is not customizable. User created menu trees are customizable.

usp_menu_tree_name Table

Contains the information on the named menu trees used in the Role Based UI.

- **SQL Name** -- usp_menu_tree_name
- **Object** -- menu_tree_name

Field	Data Type	Reference	Remarks
id	INTEGER		
name	STRING (80)		Name of the menu tree
code	STRING 30		Code

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	
description	STRING (255)		Description
internal	INTEGER	Boolean_Table::enum	Indicates if this menu tree is delivered out-of-box. If so, the menu tree is not customizable. User created menu trees are customizable.

usp_menu_tree_res Table

Contains the information on the menu tree resources used by menu trees in the Role Based UI.

- **SQL Name** -- usp_menu_tree_res
- **Object** -- menu_tree_res

Field	Data Type	Reference	Remarks
id	INTEGER		
name	STRING (50)		Name of the menu tree resource
del	INTEGER	Active_Boolean_Table::enum	
description	STRING (255)		Description
mtr_resource	STRING (255)		The URL that displayed the web page
mtr_type	INTEGER		Internal flag used by CA Service Desk development. User created usp_menu_tree_res records will have mtr_type = 0.

USP Mailbox

This article contains the following topics:

- usp_mailbox_violation_log_type Table (see page 3777)

usp_mb_rule_action_type Table

The usp_mb_rule_action_type table lists the types of filters in the usp_mailbox_rule table.

Field	Data Type	Description
del	INTEGER	
id	INTEGER	Specifies the REL_ATTR value of the table.
sym	STRING 60	Specifies the symbolic value for the action type.

The following values are the defaults for the usp_mb_rule_action_type table:

id	sym
1	Ignore Email
2	Ignore Email and Reply
3	Update Object
4	Create/Update Object

usp_mb_rule_filter_type Table

The usp_mb_rule_filter_type table lists the types of filters in the usp_mailbox_rule table.

Field	Data Type	Description
del	INTEGER	
id	INTEGER UNIQUE KEY	Specifies the REL_ATTR value of the table.
sym	STRING 60	Specifies the symbolic value for the filter type.

The following values are the defaults for the usp_mb_rule_filter_type table:

id	sym
1	Subject contains
2	Body contains
3	(Reserved for future use)
4	From Address contains

usp_mb_rule_subject_handling Table

The usp_mb_rule_subject_handling table lists how subjects are handled (prepend or append subjects) in the usp_mailbox_rule table.

Field	Data Type	Description
del	INTEGER	
id	INTEGER UNIQUE KEY	Specifies the REL_ATTR value of the table.
sym	STRING 60	Specifies the symbolic value for the subject handling type.

The following values are the defaults for the usp_mb_rule_subject_handling table:

id	sym
1	Prepend
2	Append

usp_mailbox Table

A mailbox object represents a connection to a mail server for a single inbox. The usp_mailbox table lists the filter, policy, and actions that must occur for an inbox.

Label	Field	Data Type	Reference	Description
id		INTEGER UNIQUE KEY		Specifies the primary key of this table.
	last_mod_dt	LOCAL_TIME		Specifies the time stamp of when this record was last modified.
	last_mod_by	UUID REF	ca_contact	Specifies the UUID of the contact who last modified this record.
Active	del	INTEGER NOT_NULL		Specifies if the mailbox is active. Inactive mailboxes are not polled.
Check Interval	check_interval	INTEGER		Specifies the number of seconds to wait between checks of the mailbox. 30 seconds is the default.
Name	name	STRING 60 UNIQUES_KEY		Names the mailbox connection
Allow Anonymous	allow_anonymous	INTEGER		Allows messages to create or update tickets with sender addresses not attached to a known Contact.

Label	Field	Data Type	Reference	Description
Email Type	email_type	STRING 10		Specifies the email type: NONE, IMAP, or POP3. If NONE is selected, the mailbox is not polled.
Hostname	host_name	STRING 128		Specifies the host name or IP address of the mail server.
Port Override	host_port	INTEGER		Specifies a port number to override the default for Email Type. The default is 110 for POP3 and 143 for IMAP.
Userid	userid	STRING 64		Specifies the userid to log in to the mail server.
Password	password	STRING 64		Specifies the password for userid.
Security Level	security_lvl	INTEGER		Specifies a security level for encoding of login information: **0** -- Clear Text **1** -- APOP (POP3 only) **2** -- NTLM **3** -- MD5
Attachment Repository	attmnt_repository	STRING 60	Document_Repository	Specifies the repository for attachments. The repository must be local to pdm_maileater_nxd. If not specified, the mailbox is not polled.
Attach Entire Email	attach_email	INTEGER		Attaches the entire email to a ticket. This option overrides the default value of splitting out attachments.
Force Attachment Splitout	split_out_attachment	INTEGER		Forces attachment split out if attach Entire Email is set. The entire message and individual attachments are all attached to the ticket.
Save Unknown Emails	save_unknown_emails	INTEGER		Saves emails that are not able to be processed in NX_ROOT/site/unknown_mails.
Description	description	STRING 1000		Describes the mailbox.
Email Address/Hour	email_address_per_hour	INTEGER		Specifies the maximum number of emails per email address per hour. You can specify the following values: **-1** -- No limit (default) **0** -- No emails allowed. **1** or more -- Maximum number of emails allowed.
Log Violation	log_policy_violation	INTEGER		

Label	Field	Data Type	Reference	Description
			usp_mailbox_violation_log_type	Controls logging of policy violations to the standard log.You can specify the following values: Do not log First violation only (default) All violations
Inclusion List	inclusion_list	STRING 32768		Specifies email addresses or domains that are allowed to process emails -- only emails matching the list are allowed. You can specify multiple addresses or domains by delimiting them with a space character or new line.
Exclusion Lists	exclusion_list	STRING 32768		Specifies email addresses or domains that are not allowed to process emails. You can specify multiple addresses or domains by delimiting them with a space character or new line.
	tenant	UUID	ca_tenant	Specifies the tenant.

usp_mailbox_artifact_type Table

The usp_mailbox_artifact_type table lists the artifacts types referenced by the filter_min_artifact_type field in the usp_mailbox_rule table.

Field	Data Type	Description
id	INTEGER UNIQUE KEY	Specifies the REL_ATTR value of the table.
sym	STRING 60	Specifies the symbolic value for the artifact type.

The following values are the defaults for the usp_mailbox_artifact_type table:

id	sym	prefix
1	Protected	A
2	Secure	B

usp_mailbox_rule Table

The usp_mailbox_rule table lists the filter, the rule, and any action, any replies, or both that must occur when the filter matches.

Label	Field	Data Type	Reference	Description
id		INTEGER UNIQUE KEY		Specifies the primary key of this table.
last_mod_by		UUIDREF	ca_contact	Specifies the UUID of the contact who last modified this record.

Label	Field	Data Type	Reference	Description
last_mod_dt		LOCAL_TIME		Specifies the time stamp of when this record was last modified.
Sequence	sequence	INTEGER		Specifies the sequence number of the rule. Rules are processed in sequence number order.
Mailbox	mailbox	INTEGER	usp_mailbox	Specifies the mailbox that this rule belongs to.
Active	del	INTEGER NOT_NULL		Specifies that the rule is active. A rules is not processed if it is inactive. Rules can be deleted, the active flags let you disable rules temporarily.
Description	description	STRING 1000		Describes the rule.
Filter	filter_type	INTEGER	usp_mb_rule_filter_type	Specifies the field to check against the Filter String.
Filter String	filter_string	STRING 255		Specifies a regular expression string to match. You can use the placeholder “{{object_id}}” to identify the object ID that the Text API can use with the Action Object field to identify the ticket.
Ignore Case	filter_ignore_case	INTEGER		Specifies case-insensitive pattern matching for Filter String.
Action	action_operation	INTEGER	usp_mb_rule_action_type	Specifies the action to perform if the filter matches.
Action Object	action_object	STRING 30	usp_ticket_type	Specifies the type of ticket object to use for the action.
Write to Stdlog	action_write_to_log	INTEGER		Writes the entire email text to the standard log (STDLOG) if the filter matches.
Log Entry Prefix	action_log_prefix	STRING 30		Specifies a prefix for log entries. Lets you match rules to logs.
Add Subject Line	action_subject_handling	INTEGER	usp_mb_rule_subject_handling	Adds a subject line to the message body before processing as follows: append, prepend, or null (do not add subject).
TextAPI Defaults	text_api_defaults	STRING 1000		Specifies additional default commands for the Text API when the filter matches. Combines with the contents of the [EMAIL_DEFAULTS] section of the text_api.cfg file.
TextAPI Ignore Incoming	text_api_ignore_incoming	STRING 1000		Specifies additional Ignore Details for the Text API when the filter matches. Combines with the contents of the [EMAIL_IGNORE_INCOMING] section of the text_api.cfg file.

Label	Field	Data Type	Reference	Description
Reply	reply_method	INTEGER	Contact_Method	Specifies the notification method to use for automatic replies. If not set, no reply is created.
Reply Subject	reply_subject	STRING 200		Specifies a subject line to use for automatic replies.
Reply Success Text	reply_success_text	STRING 10000		Specifies the message body in plain text for the automatic response that is sent when the message is processed successfully.
Reply Success HTML	reply_success_html	STRING 10000		Specifies the message body in HTML for the automatic response that is sent when the message is processed successfully.
Reply Failure Text	reply_failure_text	STRING 10000		Specifies the message body in plain text for the automatic response that is sent when a failure occurs processing the message.
Reply Failure HTML	reply_failure_html	STRING 10000		Specifies the message body in HTML for the automatic response that is sent when a failure occurs processing the message.

usp_mailbox_violation_log_type Table

The usp_mailbox_violation_log_type table lists the violation log types referenced by the Log Violation drop-down list (log_policy_violation) in the usp_mailbox table.

Field	Description
id	Specifies the REL_ATTR value of the table.
sym	Specifies the symbolic value for the violation log type.

The following values are the defaults for the usp_mailbox_violation_log_type table:

id	sym
1	First violation only
2	All violations
3	Do not log

USP Relational Table - Macros

This article contains the following topics:

usp_lrel_false_action_act_f Table

Relates macros to events. Identifies the macros to execute upon a false evaluation of the event condition.

- **SQL Name** -- usp_lrel_false_action_act_f
- **Object** -- lrel_false_action_act_f

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
evt	STRING 30	Events	
macro	STRING 30	Spell_Macro	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	

usp_lrel_false_bhv_false Table

Relates macros to workflow task behaviors. Identifies the macros to execute upon a false evaluation of a behavior condition.

- **SQL Name** -- usp_lrel_false_bhv_false
- **Object** -- lrel_false_bhv_false

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
bhvtpl	INTEGER	Behavior_Template	
macro	STRING 30	Spell_Macro	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_true_action_act_t Table

Relates macros to events. Identifies the macros to execute upon a true evaluation of the event condition.

- **SQL Name** -- usp_lrel_true_action_act_t
- **Object** -- lrel_true_action_act_t

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY

Field	Data Type	Reference	Remarks
evt	STRING 30	Events	
macro	STRING 30	Spell_Macro	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_true_bhv_true Table

Relates macros to workflow task behaviors. Identifies the macros to execute upon a true evaluation of a behavior condition.

- **SQL Name** -- usp_lrel_true_bhv_true
- **Object** -- lrel_true_bhv_true

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
bhvtpl	INTEGER	Behavior_Template	
macro	STRING 30	Spell_Macro	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

USP Relational Table - Stakeholders Notify List

This article contains the following topics:

usp_lrel_notify_list_cntchgntf Table

Relates contacts to change orders and supports the Stakeholders Notify List.

- **SQL Name** -- usp_lrel_notify_list_cntchgntf
- **Object** -- lrel_notify_list_cntchgntf

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
chg	INTEGER	Change_Request	
cnt	UUID	ca_contact	
last_mod_dt	LOCAL_TIME		

Field	Data Type	Reference	Remarks
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_notify_list_cntissntf Table

Relates contacts to issues and supports the Stakeholders Notify List.

- **SQL Name** -- usp_lrel_notify_list_cntissntf
- **Object** -- lrel_notify_list_cntissntf

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
iss	STRING 30	Issue	
cnt	UUID	ca_contact	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_notify_list_cntntf Table

Relates contacts to requests and supports the Stakeholders Notify List.

- **SQL Name** -- usp_lrel_notify_list_cntntf
- **Object** -- lrel_notify_list_cntntf

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
cr	STRING 30	Call_Req	
cnt	UUID	ca_contact	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

USP Relational Table - Notification Rule

This article contains the following topics:

usp_lrel_ntfr_cntlist_att_ntfrlist Table

Relates contacts to a Notification Rule. For example, the Contacts tab on the Notification Rule Detail page uses this relational data.

- **SQL Name** -- usp_lrel_ntfr_cntl_att_ntfrl
- **Object** -- lrel_ntfr_cntlist_att_ntfrlist

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
ntfr	INTEGER	Notify_Rule	
cnt	UUID	ca_contact	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_ntfr_ctplist_att_ntfrlist Table

Relates contact types to a notification rule. For example, the Contact Types tab on the Notification Rule Detail page uses this relational data.

- **SQL Name** -- lrel_ntfr_ctplist_att_ntfrl
- **Object** -- lrel_ntfr_ctplist_att_ntfrlist

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
ntfr	INTEGER	Notify_Rule	
ctp	INTEGER	ca_contact_type	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_ntfr_macrolist_att_ntfrlist Table

Relates a macro to a notification rule. Because this table contains internal data, do not change this data.

- **SQL Name** -- usp_lrel_ntfr_macrolist_att_ntfrllist
- **Object** -- lrel_ntfr_macrolist_att_ntfrllist

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
ntfr	INTEGER	Notify_Rule	
macro	STRING 30	Spell_Macro	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_ntfr_ntflist_att_ntfrlist Table

Relates object contacts to notification rules. For example, the Object Contacts tab of a Notification Rule Detail page uses this relational data.

- **SQL Name** -- usp_lrel_ntfr_ntflist_att_ntfrl
- **Object** -- lrel_ntfr_ntflist_att_ntfrlist

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
ntfr	INTEGER	Notify_Rule	
ntfl	INTEGER	Object_Attr	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

USP Relational Table - Service Groups

This article contains the following topics:

usp_lrel_svc_grps_svc_chgcat Table

Relates service groups to a change category for auto-assignment.

- **SQL Name** -- usp_lrel_svc_grps_svc_chgcat
- **Object** -- lrel_svc_grps_svc_chgcat

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
chgcat	STRING 12	Change_Category	
cnt	UUID	ca_contact	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_svc_grps_svc_isscat Table

Relates service groups to an issue category for auto-assignment.

- **SQL Name** -- usp_lrel_svc_grps_svc_isscat
- **Object** -- lrel_svc_grps_svc_isscat

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
isscat	STRING 12	Issue_Category	
cnt	UUID	ca_contact	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_svc_grps_svc_pcat Table

Relates service groups to a request, problem, or incident area for auto-assignment.

- **SQL Name** -- usp_lrel_svc_grps_svc_pcat
- **Object** -- lrel_svc_grps_svc_pcat

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
pcat	STRING 30	Prob_Category	
cnt	UUID	ca_contact	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	

Field	Data Type	Reference	Remarks
tenant	UUID	ca_ tenant	

usp_lrel_svc_grps_svc_wftpl Table

Relates service groups to a classic workflow task template for auto-assignment.

- **SQL Name** -- usp_lrel_svc_grps_svc_wftpl
- **Object** -- lrel_svc_grps_svc_wftpl

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
wftpl	INTEGER	Workflow_Task_ Template	
cnt	UUID	ca_contact	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_svc_locs_svc_chgcat Table

Relates service locations to a change category for auto-assignment.

- **SQL Name** -- usp_lrel_svc_locs_svc_chgcat
- **Object** -- lrel_svc_locs_svc_chgcat

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
chgcat	STRING 12	Change_Category	
loc	UUID	ca_location	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_svc_locs_svc_groups Table

Relates service groups and locations for auto-assignment.

- **SQL Name** -- usp_lrel_svc_locs_svc_groups
- **Object** -- lrel_svc_locs_svc_groups

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
cnt	UUID	ca_contact	
loc	UUID	ca_location	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_svc_locs_svc_isscat Table

Relates service locations to an issue category for auto-assignment.

- **SQL Name** -- usp_lrel_svc_locs_svc_isscat
- **Object** -- lrel_svc_locs_svc_isscat

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
isscat	STRING 12	Issue_Category	
loc	UUID	ca_location	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_svc_locs_svc_pcat Table

Relates service locations to a request, problem, or incident area for auto-assignment.

- **SQL Name** -- usp_lrel_svc_locs_svc_pcat
- **Object** -- lrel_svc_locs_svc_pcat

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
pcat	STRING 30	Prob_Category	
loc	UUID	ca_location	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_tenant	

usp_lrel_svc_schedules_chgcat_svc Table

Relates workshifts to change categories and supports service schedules for auto-assignment.

- **SQL Name** -- usp_lrel_svc_sch_chgcat_svc
- **Object** -- lrel_svc_schedules_chgcat_svc

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
chgcat	STRING 12	Change_Category	
wrkshft	STRING 30	Bop_Workshift	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_svc_schedules_isscat_svc Table

Relates workshifts to issue categories and supports service schedules for auto-assignment.

- **SQL Name** -- usp_lrel_svc_sch_isscat_svc
- **Object** -- lrel_svc_schedules_isscat_svc

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
isscat	STRING 12	Issue_Category	
wrkshft	STRING 30	Bop_Workshift	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_svc_schedules_pcat_svc Table

Relates workshifts to request, problem, or incident areas and supports service schedules for auto-assignment.

- **SQL Name** -- usp_lrel_svc_sch_pcat_svc
- **Object** -- lrel_svc_schedules_pcat_svc

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
pcat	STRING 30	Prob_Category	

Field	Data Type	Reference	Remarks
wrkshft	STRING 30	Bop_Workshift	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

USP Relational Table

This article contains the following topics:

usp_lrel_asset_chgnr Table

Relates CIs to Change Orders. For example, the Configuration Items tab on a Change Order Detail page uses this relational data.

- **SQL Name** -- usp_lrel_asset_chgnr
- **Object** -- lrel_asset_chgnr

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
chg	INTEGER	Change_Request	
nr	UUID		ca_owned_resource
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_asset_issnr Table

Relates CIs to Issues. For example, the Configuration Items tab on an Issue Detail page uses this relational data.

- **SQL Name --** usp_lrel_asset_issnr

- **Object** -- lrel_asset_issnr

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
iss	STRING 30	issue	
nr	UUID	ca_owned_ resource	
last_mod_ dt	LOCAL_TIME		
last_mod_ by	UUID	ca_contact contact_uuid	
tenant	UUID		

usp_lrel_att_cntlist_macro_ntf Table

Relates contacts to notification-type macros.

- **SQL Name** -- usp_lrel_att_cntlist_macro_ntf
- **Object** -- usp_lrel_att_cntlist_macro_ntf

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
macro	STRING 30	Spell_Macro	
cnt	UUID	ca_contact	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_att_ctplist_macro_ntf Table

Relates contact types to notification-type macros.

- **SQL Name** -- usp_lrel_att_ctplist_macro_ntf
- **Object** -- lrel_att_ctplist_macro_ntf

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
macro	STRING 30	Spell_Macro	
ctp	INTEGER	ca_contact_type	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_att_ntflist_macro_ntf Table

Relates object contacts to notification-type macros.

- **SQL Name** -- usp_lrel_att_ntflist_macro_ntf
- **Object** -- usp_lrel_att_ntflist_macro_ntf

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
macro	STRING 30	Spell_Macro	
ntfl	INTEGER	Notify_Object_Attr	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_aty_events Table

Relates events to activity notifications. For example, the Events tab of the Activity Notification Detail page uses this relational data.

- **SQL Name** -- usp_lrel_aty_events
- **Object** -- lrel_aty_events

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
aty	STRING 12	Act_Type	
evt	STRING 30	Events	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_cenv_cntref Table

Relates CIs to contacts. For example, the Environment tab on a Contact page uses this relational data.

- **SQL Name** -- usp_lrel_cenv_cntref
- **Object** -- lrel_cenv_cntref

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
cnt	UUID	ca_contact	
nr	UUID	ca_owned_resource	

last_mod_dt	LOCAL_TIME	
last_mod_by	UUID	ca_contact
tenant	UUID	ca_ tenant

usp_lrel_kwrds_crsolref Table

Relates key words to request solutions.

- **SQL Name** -- usp_lrel_kwrds_crsolref
- **Object** -- lrel_kwrds_crsolref

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
crsol	STRING 30	Call_Solution	
kwrd	INTEGER	Knowledge_Keywords	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_oenv_orgref Table

Relates CIs to an organization. For example, the Environment tab of the Organization Detail page uses this relational data.

SQL Name -- usp_lrel_oenv_orgref

Object -- lrel_oenv_orgref

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
org	UUID	ca_organization	
nr	UUID	ca_owned_resource	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_status_codes_tsktypes Table

Relates change order status to workflow task types. For example, the Status Codes tab on a Workflow Task Type Detail page uses this relational data.

- **SQL Name** -- usp_lrel_status_codes_tsktypes

- **Object** -- lrel_status_codes_tsktypes

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
tskty	STRING 12	Task_Type	
tskstat	STRING 12	Task_Status	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_bm_reps_assets Table

Relates CIs to a NSM repository.

- **SQL Name** -- usp_lrel_bm_reps_assets
- **Object** -- lrel_bm_reps_assets

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
nr	UUID	ca_owned_resource	
bmrep	INTEGER	Business_Management_ Repository	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

usp_lrel_bm_reps_bmhiers Table

Relates CI relationships to a NSM repository.

- **SQL Name** -- usp_lrel_bm_reps_bmhiers
- **Object** -- lrel_bm_reps_bmhiers

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
bmhier	INTEGER	Business_Management	
bmrep	INTEGER	Business_Management_Repository	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_ tenant	

USP Relational Table - Managed Surveys

This article contains the following topics:

usp_lrel_dist_cntlist_mgs_ntf Table

Relates contact lists to managed surveys.

- **SQL Name** -- usp_lrel_dist_cntlist_mgs_ntf
- **Object** -- lrel_dist_cntlist_mgs_ntf

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
cnt	UUID	ca_contact	
mgs	INTEGER	Managed_Survey	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_tenant	

usp_lrel_dist_ctplist_mgs_ntf Table

Relates contact types to managed surveys.

- **SQL Name** -- usp_lrel_dist_ctplist_mgs_ntf
- **Object** -- lrel_dist_ctplist_mgs_ntf

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
ctp	INTEGER	ca_contact_type	
mgs	INTEGER	Managed_Survey	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_tenant	

usp_lrel_dist_ntflist_mgs_ntf Table

Relates notifications to managed surveys.

- **SQL Name** -- usp_lrel_dist_ntflist_mgs_ntf
- **Object** -- lrel_dist_ntflist_mgs_ntfTable

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
ntfl	INTEGER	Notify_Object_Attr	
mgs	INTEGER	Managed_Survey	
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_tenant	

USP Functional Access

This article contains the following topics:

usp_functional_access Table

Defines allowable functional access areas.

- **SQL Name** -- usp_functional_access
- **Object** -- func_access

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
code	STRING 30	UNIQUES_KEY	A string value that represents the functional access area. This value matches what is currently in the FUNCTION_GROUP field in object definition in Majic.
type	INTEGER	usp_functional_access_type	
sym	STRING 60	S_KEY	A synonym or localized friendly name

Field	Data Type	Reference	Remarks
description	STRING 1000		A reference (SREL) to the usp_functional_access_type table that allows for categorization of the functional access.

usp_functional_access_level Table

Defines the access permissions for a functional access area. This table is a static table and cannot be updated by the user.

- **SQL Name** -- usp_functional_access_level
- **Object** -- func_access_level

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
access_level	INTEGER		Integer value that represents the level of the access.
type	INTEGER	usp_functional_access_type	Reference to a usp_functional_access_type record. This value signifies the type this level belongs to.
sym	STRING 60		A localized friendly name for the access type.
description	STRING 1000		

usp_functional_access_role Table

Maps the many-to-many relationship between the usp_functional_access table and the usp_role table. This table also defines the access level such as None, View, and Modify.

- **SQL Name** -- usp_functional_access_role
- **Object** -- func_access_role

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY

Field	Data Type	Reference	Remarks
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
access_level	INTEGER	usp_functional_access_level	Reference to a usp_functional_access_level record that describes the access level for the relationship
func_access	STRING 30	usp_functional_access	Reference to a usp_functional_access record.
role	INTEGER	usp_role	Reference to a usp_role record
description	STRING 1000		

usp_functional_access_type Table

Categorizes the functional areas into types such as Object and Process. This table is a static table that the user cannot update.

- **SQL Name** -- usp_functional_access_type
- **Object** -- func_access_type

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE KEY
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
sym	STRING 60		A localized friendly name for the access type.
default_access	INTEGER	usp_functional_access_level	Reference to a usp_functional_access record. This is the default access for new or missing usp_functional_access_role records.
description	STRING 1000		

USP Tables - KPI

This article contains the following topics:

- Kpi_Ticket_Data Table (see page 3797)

Kpi Table

Contains KPIs of Stored Query type, SQL type, and System type.

- **SQL Name** -- usp_kpi
- **Object** -- kc

Field	Data Type	Reference	Remarks
name	string		Defines the name of the KPI.
type	integer		Indicates where the KPI data is retrieved from, such as the crsq database table, BPVirtdb, or daemons in the BOP system.
status	integer		Indicates the on/off state of the KPI.
process_type	integer		Indicates the daemon process where the KPI data resides.
metric_type	integer		Indicates the type of metric the KPI produces (for example, count or sum).
stored_query_id	string		Provides a REF to the id attribute in the Crsq table. It is a SREL to REL_ATTR of object crsq, and contains the value of the code of a row in the crsq object.
user_context	string		Provides a UUID REF to the ca_contact table.
sql_query	string		Defines a SQL query.
description	string		Describes the measurement goal for the KPI.
refresh_time	integer		The time interval at which the KPI data is updated.
sys_name	string		The internal KPI name for sys type KPIs.
curr_kpi_time_stamp	integer		The last collection time of this KPI.
version_number	integer		Indicate the version of this KPI.
tenant	string		Provides a UUID REF to the ca_tenant table.
last_mod_by	string		Specifies the foreign key of the ca_contact table (UUID).
last_mod_dt	integer		Specifies the date and time of last update (integer value in UNIX ticks).

Kpi_Data Table

Contains the KPI data periodically retrieved from system daemons by the kpi_daemon. Provides raw data for web reporting.

- **SQL Name** -- usp_kpi_data
- **Object** -- kcd

Field	Data Type	Reference	Remarks
id	integer		Specifies the id of the record.
kpi_id	integer		Provides a REF to the id in the KPI.
kpi_time_stamp	integer		Indicates the time when a new KPI record is inserted into this table.
metric_type	integer		Indicates the type of metric the KPI produces (count, sum, max, or duration).
kpi_value	integer		Indicates the value of the metric produced by the KPI. The value matches the metric_type (count, sum, max, or duration).
duration_max	integer		Specifies the maximum value of duration for KPIs of duration metric_type. The time unit is millisecond.
duration_sum	integer		Specifies the total duration for KPIs of duration metric_type. The time unit is seconds.
duration_count	integer		Indicates the amount of duration data that has been collected in a period of time.
duration_average	integer		Indicates the average duration in a period of time for KPIs with duration metric_type. The time unit is milliseconds.
execute_time	integer		Indicates the total time for retrieving the KPI data, from the time the request is sent to time the result is received. The time unit is milliseconds.
version_number	integer		Indicate the version of this KPI.

Kpi_Ticket_Data Table

This table contains data retrieved from CA SDM tickets. The data can be used for reporting on ticket performance, such as how long a ticket was in each state.

- **SQL Name** -- usp_kpi_ticket_data
- **Object** -- ktd

Note: This table can collect data for custom fields when you manually add the UI_INFO flag to the custom fields in a majic file. For example, you can use the following attributes:

```
priority SREL pri REQUIRED { ON_NEW SET 0 ;
UI_INFO "KPI" ;} ;
urgency SREL urg { UI_INFO "KPI" ; };
```

Field	Data Type	Reference Remarks
id	integer	Specifies the id of the record.
end_time	integer	Indicates the time when a ticket attribute is changed. It can also be used as a unique id for identifying a ticket object in which one or more attributes are changed.
prev_time	integer	Indicates the time stamp of the last change to this ticket object.
obj_name	string	Indicates ticket objects in majic files (cr, chg, iss,in and pr). Identifies a ticket in which an attribute is changed.
obj_id	integer	Indicates the id of a ticket object in which an attribute is changed.
obj_type	string	Contains type names for call request, such as Problem, Incident, or Request.
field_name	string	Indicates an attribute name in the ticket object in majic files of which the value is changed. They are assignee, priority, customer, etc.
field_value	string	Indicates the attribute value before current value. If it is a SREL, use a common name.
next_value	string	Indicates the attribute value after current value. If it is a SREL, use a common name.
operation	string	There are three kinds of operations: insert, delete and update. Insert or delete creates a usp_kpi_ticket_data record without setting the attribute fields.
attr_obj	string	The name of the object table the SREL links to.
attr_from_id	integer	The previous attr_obj id.
attr_from_uuid	uuid	The previous attr_obj uuid.
attr_to_id	integer	The next attr_obj id.
attr_to_uuid	uuid	The next attr_obj uuid.
user_context	uuid	Whenever the attribute of a ticket object has been changed, the user_context field needs to be filled. It is an SREL to cnt.
ktd_duration	integer	Indicates the calculated time duration between two changes.

Field	Data Type	Reference	Remarks
			Note: The calculated duration is based on a change to values in a ticket in real time, not in business hours.

Transition

This topic contains the following information:

Transition_Points Table

Lists the transitions of interest to the Notification System. E.g. Incident_report creation, or reassignment, TT creation TT closure and so on.

- **SQL Name** -- nottrn

Field	Data Type	Reference	Remarks
del	INTEGER NOT_NULL		Deleted flag **0** -- Active **1** -- Inactive/marked as deleted
enum	INTEGER NOT_NULL		Enumerated value for this entry - specifies ordering in lists and relative values
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
nx_desc	STRING 40		longer description of event
sym	STRING 30 UNIQUE NOT_NULL S_KEY		transition event symbol
tp_use_pri	INTEGER		flag indicating whether priority is meaningfull

Transition_Types Table

Transition types and their corresponding status transitions control when employees using self-service can close or reopen incidents or requests.

- **SQL Name** -- transition_type
- **Object** -- transition_type

Label	Field	Description
id	INTEGER	Unique key
sym		

Label	Field	Description
	STRING 80 nn	
ss_flag	INTEGER nn	Specifies whether the status transition appears in the Employee Self-Service interface.
ss_button_text	STRING 80	Displays text on the button that performs the status transition.
ss_header_text	STRING 128	Used as the form header when the employee is prompted for comments after selecting a status transition button.
description	STRING 1000	Provides a description of the record.
del	INTEGER nn	Deleted flag: **0** -- Active **1** -- Inactive/marked as deleted
last_mod_dt	LOCAL_TIME	Indicates the timestamp of when this record was last modified.
last_mod_by	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.

Timespan

List of defined time-span elements used by applications to calculate hours-of-operation time calculations.

- **SQL Name** -- tspan
- **Object** -- tspan

Field	Data Type	Reference	Remarks
code	STRING 10 UNIQUE NOT_NULL		
end_day	STRING 5		
end_hour	STRING 5		
end_minute	STRING 5		
end_month	STRING 5		
end_year	STRING 5		
id	INTEGER UNIQUE KEY		Unique (to the table) Numeric ID
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
nx_desc	STRING 240		
start_day	STRING 5		

Field	Data Type	Reference	Remarks
start_hour	STRING 5		
start_minute	STRING 5		
start_month	STRING 5		
start_year	STRING 5		
sym	STRING 30 UNIQUE NOT_NULL		
trigger_day	STRING 5		
trigger_hour	STRING 5		
trigger_minute	STRING 5		
trigger_month	STRING 5		
trigger_year	STRING 5		

Tasks

This topic contains the following information:

Task_Status Table

Workflow task states. Possible states include: Wait, pending, approve, reject, and so on.

- **SQL Name** -- tskstat
- **Object** -- tskstat

Field	Data Type	Reference	Remarks
allow_accumulate	INTEGER		Identifies the Allow Accumulate flag, as follows:**0 --** Do not accumulate**1 --** Accumulate
allow_task_update	INTEGER		Specifies the Allow Task Update flag, as follows:**0 --** Cannot update**1** -- Can update
code	nvarchar (12)		Primary key of this table.
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive /marked as deleted
description	nvarchar (500)		Provides a text description of the status.

Field	Data Type	Reference	Remarks
do_next_task	INTEGER		Sets the Do Next Task flag, as follows:**0** -- No**1** -- Yes
hold	INTEGER		Sets the Hold flag, as follows:**0** -- Start events**1** -- Stop events
id	INTEGER		Specifies the unique (to the table) numeric ID.
is_internal	INTEGER		Specifies the Internal flag, as follows:**0** -- No**1** -- Yes (do not display in most status selections).
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp of when this record was last modified.
no_update_msg	nvarchar (500)		Sets the No Update Message flag to No.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
sym	nvarchar (30)		Identifies the Task Status name.
task_complete	INTEGER		Sets the Task Complete, as follows:**0** -- No**1** -- Yes

Task_Type Table

This table contains the list of task types used in the workflow used by CA SDM.

- **SQL Name** -- tskty
- **Object** -- tskty

Field	Data Type	Reference	Remarks
code	nvarchar (12)		Primary key of this table.
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive/marked as deleted
description	nvarchar (500)		Identifies the text description of the task.
id	INTEGER		Identifies the numeric ID, which is unique to the table.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp for when this record was last modified.
persid	nvarchar (30)		Identifies the Persistent ID: (SystemObjectName:id).
sym			Identifies the name of task.

Field	Data Type Reference	Remarks
	nvarchar (30)	

Service Type

This article contains the following topics:

target_tgttpls_srvtypes Table

Links the Target Template to Service Types.

- **SQL Name** -- target_tgttpls_srvtypes
- **Object** -- tgt_tgttpls_srvtypes

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY Unique (to the table) Numeric ID.
del	INTEGER		NOT_NULL Deleted flag: **0** -- Active **1** -- Inactive/marked as deleted
last_mod_dt	LOCAL_TIME		Indicates the timestamp when this record was last modified.
last_mod_by	UUID	ca_contact	UUID of the contact who last modified this record.
tenant	UUID	ca_tenant	UUID REF to the ca_tenant table.
tgt_time_tpl	INTEGER	target_time_tpl	NOT_NULL. The Service Target Template that is linked to a Service Type.
sdsc	STRING 30	Service_Desc	NOT_NULL.The Service Type to which the template is linked.
target_duration	DURATION		NOT_NULL. The amount of time in which this target is reached.
set_actual	INTEGER	Boolean_Table	A flag that determines whether the Set Actual Service Target Action is available on the ticket.
reset_actual	INTEGER	Boolean_Table	A flag that determines whether the Reset Actual Service Target Action is available on the ticket.
cost	STRING 255		Text information to appear on the ticket.
work_shift	STRING 30	Bop_Workshift	The workshift used in time calculations.

target_time Table

Represents a Service Target that is attached to a ticket.

- **SQL Name** -- target_time
- **Object** -- tgt_time

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY Unique (to the table) Numeric ID.
del	INTEGER		NOT_NULL Deleted flag: **0** -- Active **1** -- Inactive/marked as deleted
sym	STRING 60		NOT_NULL Identifies the symbolic value for this target.
last_mod_dt	LOCAL_ TIME		Indicates the timestamp when this record was last modified.
last_mod_by	UUID	ca_contact	UUID of the contact who last modified this record.
tenant	UUID	ca_tenant	UUID REF to the ca_tenant table.
target_durati on	DURATI ON		NOT_NULL. The amount of time in which this target is reached.
condition	STRING 30	Macro	Identifies the condition to be detected in determining that this target has been reached.
condition_ou tcome	INTEGER	Boolean_Ta ble	Specifies the required outcome of the evaluation of the condition.
service_type	STRING 30	Service_De sc	NOT_NULL. The Service Type to which this target belongs.
object_type	STRING 30		NOT_NULL Ticket type that this target is attached.
object_id	INTEGER	S_KEY	NOT_NULL id of the ticket that this target is attached.
set_actual	INTEGER	Boolean_Ta ble	A flag that determines whether the Set Actual Service Target Action is available on the ticket.
reset_actual	INTEGER	Boolean_Ta ble	A flag that determines whether the Reset Actual Service Target Action is available on the ticket.
lock_target	INTEGER	Boolean_Ta ble	Prevents Service Target recalculations for tickets that transition to and from the Hold status.
cost	STRING 255		Text information to appear on the ticket.
target_time	LOCAL_ TIME		Deadline for the Service Target.
actual_time	LOCAL_ TIME		The time that the target completed.
time_left			Number of remaining minutes.

	DURATION		
_mapped_cr	STRING 30	Call_Req	Pointer to the Request, Incident, or Problem that uses this Service Target.
_mapped_chg	INTEGER	Change_Request	Pointer to the Change Order that uses this Service Target.
_mapped_iss	STRING 30	Issue	Pointer to the Incident that uses this Service Target.
target_tpl	INTEGER	target_tpl	Identifies the target template for this target.
work_shift	STRING 30	Bop_Workshift	Identifies the workshift to use for calculating the target.

target_time_tpl Table

Contains the Service Target template defaults to link to a Service Type.

- **SQL Name** -- target_time_tpl
- **Object** -- tgt_time_tpl

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY Unique to the table Numeric ID.
del	INTEGER		NOT_NULL Deleted flag: **0** -- Active **1** -- Inactive/marked as deleted
sym	STRING 60		NOT_NULL Identifies the symbolic value for this target.
last_mod_dt	LOCAL_TIME		Indicates the timestamp when this record was last modified.
last_mod_by	UUID	ca_contact	UUID of the contact who last modified this record.
tenant	UUID	ca_tenant	UUID REF to the ca_tenant table.
target_duration	DURATION		NOT_NULL. The amount of time in which this target is reached.
condition	STRING 30	Macro	Identifies the condition to use to determine whether the target was met.
condition_outcome	INTEGER	Boolean_Table	Specifies the required outcome of the evaluation of the condition.
object_type	STRING 30		NOT_NULL. Identifies the valid ticket type for this template.
set_actual	INTEGER	Boolean_Table	A flag that determines whether the Set Actual Service Target Action is available on the ticket.
reset_actual	INTEGER	Boolean_Table	A flag that determines whether the Reset Actual Service Target Action is available on the ticket.

cost	STRING 255		Indicates the text information to appear on the ticket.
work_shift	STRING 30	Bop_Workshift	Indicates the workshift used for time calculations.

True and False Strings

True_False_Table Table

Contains localized True or False strings that display on the UI.

- **SQL Name** -- True_False_Table
- **Object** -- true_false

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY Unique to the table Numeric ID.
del	INTEGER		NOT_NULL Deleted flag: **0** -- Active **1** -- Inactive/marked as deleted
enum	INTEGER		NOT_NULL Enumerated value for this entry **0** -- False **1** -- True
sym	STRING 60		UNIQUE NOT_NULL S_KEY Identifies the symbolic value for this target
desc	STRING 40		Describes the enum

Type of Contact

Type_Of_Contact Table

Reference table to denote the type of issue. examples: complaint, complement and so on.

- **SQL Name** -- toc
- **Object** -- typecnt

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive /marked as deleted
id	INTEGER		Primary key of this table, this is the unique numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
	INTEGER		

Field	Data Type	Reference	Remarks
last_mod_dt			Species the timestamp of when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
sym	nvarchar (60)		The symbolic value for this Type_Of_Contact.

User Query

User_Query Table

User scoreboard queries.

- **SQL Name** -- usq
- **Object** -- usq

Field	Data Type	Reference	Remarks
expanded	INTEGER		
factory	STRING 30		
id	INTEGER UNIQUE NOT_NULL KEY		Unique (to the table) Numeric ID
label	STRING 80 NOT_NULL		
last_mod_by	UUID	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
obj_persid	STRING 60		Persistent ID (SystemObjectName:id)
parent	INTEGER	usq::id	
persid	STRING 30		Persistent ID (SystemObjectName:id)
query	STRING 30	Cr_Stored_Queries::code	
query_set	INTEGER		
query_type	INTEGER		
sequence	INTEGER NOT_NULL		

Urgency

List of urgency codes/descriptions used in CA SDM applications.

- **SQL Name** -- urgncy
- **Object** -- urg

Field	Data Type	Reference	Remarks
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive /marked as deleted
enum	INTEGER		Primary key of this table.
id	INTEGER		Identifies the unique (to the table) numeric ID.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Indicates the timestamp of when this record was last modified.
nx_desc	nvarchar (40)		Provides the description of the urgency level.
sym	nvarchar (12)		Identifies the symbolic name of this urgency.
value	INTEGER		Indicates the numeric representation of this urgency.

Timezone

This table contains the Timezones used in CA SDM applications.

- **SQL Name** -- tz
- **Object** -- tz

Field	Data Type	Reference	Remarks
code	nvarchar (12)		Primary key of this table.
del	INTEGER	Active_Boolean_Table::enum	Specifies the Deleted flag, as follows:**0** -- Active**1** -- Inactive /marked as deleted
description	nvarchar (500)		Identifies the text description of the timezone.
dst_delta	INTEGER		Specifies the delta seconds for daylight saving time.
end_abs_date	LOCAL_TIME		Identifies the *absolute* start date.
end_day	INTEGER		Represents the end day of the week, such as 0-6.
end_mon	INTEGER		Represents the ending month, such as 0-11 for the month of the year.
end_pos	INTEGER		Represents the ending position, such as 0 for "First" or 1 for "Last".
	INTEGER		Represents the delta seconds from GMT.

Field	Data Type	Reference	Remarks
gmt_delta			
id	INTEGER		Identifies the numeric ID, which is unique to the table.
last_mod_by	byte(16)	ca_contact::uuid	Specifies the UUID of the contact who last modified this record.
last_mod_dt	INTEGER		Identifies the timestamp for when this record was last modified.
persid	nvarchar (30)		Persistent ID (SystemObjectName:id).
start_abs_date	INTEGER		Identifies the *absolute* start date.
start_day	INTEGER		Represents the Start day used to calculate DST, for example, 0-6 day of the week.
start_mon	INTEGER		Represents the starting month for the timezone, such as 0-11 for the month of the year.
start_pos	INTEGER		Represents the starting position, such as 0 for "First" or 1 for "Last".
sym	nvarchar (30)		Specifies the name of the service type.

Support Automation - Self Service

This article contains the following topics:

sa_self_serve_event_join Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_self_serve_event_join
- **Object** -- sa_self_serve_event_join

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
selfServeSessionID	INTEGER	sa_self_serve_session	NOT_NULL

Field	Data Type	Reference	Remarks
eventID	INTEGER	sa_event_history	NOT_NULL
tenant	UUID	ca_tenant	

sa_self_serve_keyword Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_self_serve_keyword
- **Object** -- sa_self_serve_keyword

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
selfServeSessionID	INTEGER	sa_self_serve_session	NOT_NULL
keyword	STRING 255		NOT_NULL
tenant	UUID	ca_tenant	

sa_self_serve_login_field Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_self_serve_login_field
- **Object** -- sa_self_serve_login_field

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
selfServeSessionID	INTEGER	sa_self_serve_session	NOT_NULL
fieldID	INTEGER	sa_field	NOT_NULL
value	STRING 500		
tenant	UUID	ca_tenant	

Support Automation - Tool

This article contains the following topics:

sa_tool Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_tool
- **Object** -- sa_tool

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
toolName	STRING 100		
URL	STRING 255		
suggestion	INTEGER		
imageName	STRING 255		
displayURL	STRING 255		
width	INTEGER		
height	INTEGER		
toolType	INTEGER		
useViewport	INTEGER		
agentDefault	INTEGER		
isAdmin	INTEGER		
isSpecial	INTEGER		
	INTEGER		

Field	Data Type	Reference	Remarks
localizationID			

sa_tool_inst_log_evt_join Table

Program control table used by Support Automation.

- **SQL Name** -- sa_tool_inst_log_evt_join
- **Object** -- sa_tool_inst_log_evt_join

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
toolInstanceID	INTEGER	sa_tool_instance_log	NOT_NULL
eventID	INTEGER	sa_event_history	NOT_NULL
tenant	UUID	ca_tenant	

sa_tool_instance Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_tool_instance
- **Object** -- sa_tool_instance

Field	Data Type	Reference	Remarks
groupID	INTEGER	sa_group	NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
toolInstanceID	INTEGER		NOT_NULL
id	INTEGER	sa_group	UNIQUE NOT_NULL KEY
toolID	INTEGER	sa_tool	
toolInstanceLogID	INTEGER	sa_tool_instance_log	
lastUpdated	LOCAL_TIME		

Field	Data Type	Reference	Remarks
writeLockID	INTEGER		
tenant	UUID	ca_tenant	

sa_tool_instance_log Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_tool_instance_log
- **Object** -- sa_tool_instance_log

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
groupID	INTEGER	sa_group	
toolID	INTEGER	sa_tool	
startEpoch	LOCAL_TIME		
endEpoch	LOCAL_TIME		
tenant	UUID	ca_tenant	

sa_tool_log Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_tool_log
- **Object** -- sa_tool_log

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
toolID	INTEGER	sa_tool	NOT_NULL
logStart	LOCAL_TIME		
logEnd	LOCAL_TIME		
toolData	INTEGER		

sa_tool_log_message Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_tool_log_message
- **Object** -- sa_tool_log_message

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
toolID	INTEGER	sa_tool	NOT_NULL
logStart	STRING 300		NOT_NULL

sa_tool_module Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_sa_tool_module
- **Object** -- sa_sa_tool_module

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
toolID	INTEGER	sa_tool	NOT_NULL
seqID	INTEGER		NOT_NULL
moduleLocation	STRING 512		
agentModuleName	STRING 255		NOT_NULL
customerModuleName	STRING 255		NOT_NULL
delayLoading	INTEGER		

sa_tool_name_localized Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_tool_name_localized
- **Object** -- sa_tool_name_localized

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY

last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	
toolID	INTEGER	sa_tool	NOT_NULL
localizationID	INTEGER	sa_localization	NOT_NULL
name	STRING 200		

sa_tool_non_art Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_tool_non_art
- **Object** -- sa_tool_non_art

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
sym	STRING 100		
art_pos	INTEGER		
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.

sa_tool_property Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_sa_tool_property
- **Object** -- sa_sa_tool_property

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	
toolID	INTEGER	sa_tool	NOT_NULL
propertyID	INTEGER	sa_property	NOT_NULL

Field	Data Type	Reference	Remarks
valuee	STRING 100		

sa_tool_start_message Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_tool_start_message
- **Object** -- sa_tool_start_message

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	
toolID	INTEGER	sa_tool	NOT_NULL
showMessage	INTEGER		NOT_NULL
toolStartMessage	STRING 200		

sa_tool_version Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_tool_version
- **Object** -- sa_tool_version

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
localizationID	INTEGER	sa_localization	NOT_NULL
moduleName	STRING 100		NOT_NULL
moduleVersion	STRING 30		

CA Process Automation

This article contains the following topics:

usp_caextwf_instances Table

Associates CA Process Automation process instances that launched from the CA SDM interface. Includes the CA SDM entity to which the instance belongs.

- **SQL Name** -- usp_caextwf_instances
- **Object** -- caextwf_inst

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
inactive	INTEGER		NOT_NULL
instance_id	STRING 255		CA Process Automation instance ID
object_persid	STRING 60		The persistent id of the CA SDM entity from which a CA Process Automation process instance was launched.
procname	STRING 32768		The CA Process Automation process definition name and reference path.
starttime	LOCAL_TIME		Indicates CA Process Automation workflow start time.
endtime	LOCAL_TIME		Indicates CA Process Automation workflow end time.

usp_caextwf_start_forms Table

Stores CA SDM objects with the launchable CA Process Automation process definitions. The Start Request Form indicates the process that runs on the CA Process Automation server, but CA SDM stores the process information.

- **SQL Name** -- usp_caextwf_start_forms
- **Object** -- caextwf_sfrm

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
object_persid	STRING	60	

			UNIQUE NOT_NULL KEY The CA SDM object that provides the CA Process Automation process definition information for launching a new process instance.
caextwf_form	STRING	255	CA Process Automation Process Definition name.
caextwf_path	STRING	32768	The CA Process Automation reference path where this Process Definition is stored in the CA Process Automation library.

Support Automation - Session

This topic contains the following information:

sa_session_event_join Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_session_event_join
- **Object** -- sa_session_event_join

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
sessionID	INTEGER	sa_login_session	NOT_NULL
eventID	INTEGER	sa_event_history	NOT_NULL
tenant	UUID	ca_tenant	

sa_session_login_field Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_self_serve_login_field
- **Object** -- sa_self_serve_login_field

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
	UUID	ca_contact	

Field	Data Type	Reference	Remarks
last_mod_by			Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
sessionID	INTEGER	sa_login_session	NOT_NULL
fieldID	INTEGER	sa_field	NOT_NULL
value	STRING 500		
tenant	UUID	ca_tenant	

sa_session_security_info Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_session_security_info
- **Object** -- sa_session_security_info

Field	Data Type	Reference	Remarks
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
sessionID	INTEGER	sa_login_session	NOT_NULL
folderAccessBit	INTEGER		
securityLevelID	INTEGER	sa_security_group	
hasCustom	INTEGER		
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

Support Automation - Keyword

This topic contains the following information:

sa_keyword Table

Program control table that is used by Support Automation.

- **SQL Name** -- sa_keyword

- **Object** -- sa_keyword

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
keyname	STRING 100		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	DATE		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

sa_keyword_queue_join Table

Program control table used by Support Automation.

- **SQL Name** -- sa_keyword_queue_join
- **Object** -- sa_keyword_queue_join

Field	Data Type	Reference	Remarks
id	INTEGER		KEY
keywordID	INTEGER	sa_keyword	NOT_NULL
queueID	INTEGER	sa_queue	NOT_NULL
weight	INTEGER		
last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record.
last_mod_dt	LOCAL_TIME		Specifies the timestamp of when this record was last modified.
tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

Outage Table

This article contains the following topics:

usp_outage_reason Table

The usp_outage_reason table associates an outage reason with a special handling classification.

- **SQL Name** -- usp_outage_reason
- **Object** -- None

Attribute	Data Type	SREL References	Flags
del	INTEGER		NOT_NULL

Attribute	Data Type	SREL References	Flags
description	STRING 4000		
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	
last_mod_dt	LOCAL_TIME		
sym	STRING 60		NOT NULL
tenant	UUID	ca_tenant	

usp_outage_type Table

The usp_outage_type table associates outage types with a special handling classification.

- **SQL Name** -- usp_outage_type
- **Object** -- outage_type

Attribute	Data Type	SREL References	Flags
del	INTEGER		NOT_NULL
description	STRING 4000		
id	INTEGER		UNIQUE NOT_NULL KEY
last_mod_by	UUID	ca_contact	
last_mod_dt	LOCAL_TIME		
sym	STRING 60		NOT NULL
tenant	UUID	ca_tenant	

Technical Reference

This section lists all the CA Service Desk Manager commands:

CA SDM Text API Interface

This article contains the following topics:

Overview of Text API

The *Text API* is an interface that lets you use text-based input to create and update objects in the CA SDM database, such as issues, requests, contacts, and assets. Using the Text API, you can assign values to most fields that are accessible to users.

Important! CA SDM requires that all input be in UTF-8 format, or data can be corrupted. The pdm_unconv utility (see page 3882) lets you convert data from a local charset to UTF-8 and from UTF-8 to a local charset.

You can access the Text API by using the following interfaces:

- Command line
- Email
- CA NSM

Note: You can use web services as the alternative to the Text API for cross-application integration.

Command Line Interface

Use the *pdm_text_cmd* command to activate the Text API command line interface. You can then specify information such as the table to process and the operation to perform by using parameters to the pdm_text_cmd command.

The input to the Text API is passed to the pdm_text_cmd command in the form of an input file, or directly from STDIN.

Note: When passing the parameters from command prompt, use Ctrl+Z in Windows and Ctrl+D in POSIX.

Important! You cannot use single or double quotation marks as parameters for the bop_cmd and pdm_text_nxd commands.

CA Network and Systems Management Interface

When CA NSM and CA SDM are integrated and you are creating requests from CA NSM events, the user_parms parameter in writer rule definitions is passed to the Text API. The CA SDM writer process (tngwriter) defines its own replacement parameters for changing the text before sending it to the Text API. The keyword LOG_AGENT is added to the end of the input to set the log_agent for the request.

Note: You need to update the Text_API.cfg file for all additional fields that are passed from CA NSM Alert Management Systems to CA SDM. This file is used for integrations with web services, email and AHD.DLL.

Input Format

Input to the Text API is specified in the following ways:

- In the command-line interface, input is typically specified in a text file passed to the pdm_text_cmd command.
- In the email interface, input is specified in the text of the email. You specify a regular expression to find the target object identifiers.

You format the Text API input in the same way no matter which interface you use.

The basic format for input is as follows:

```
%keyword=value
```

or

```
%PROPERTY={{property_label}}value
```

The normal behavior of Text API commands has the following exceptions, where the last-appearing of two or more conflicting commands takes precedence:

- When a message contains multiple valid ticket ID artifacts matching the mailbox rule filter string, or multiple Text API ticket ID commands, the first one encountered is used. Also, a ticket ID artifact, which is identified using the mailbox rule filter string, overrides any Text API ticket ID command, regardless of which appears first.
- When a message contains multiple log comment Text API commands, all comments are posted, although the order in which they appear in the ticket activity log can vary.

All ticket ID artifacts that match the filter, valid or otherwise, and Text API ticket ID commands within the message, applicable or otherwise, applied or otherwise, are commented out before the message is posted. The ticket ID artifacts identified through the mailbox rule filters appear as -((...))-. Leading percentage signs (%) in Text API ticket ID commands are converted to two opening parentheses ((, and two closing parentheses)) follow the command. If a Text API ticket ID command appears after another Text API command with a log comment (%LOG=…), then the commented-out Text API ticket ID command is made into a separate log comment.

Note: The log comment is the only Text API command that can appear multiple times in one message and still have each occurrence applied. For any other commands, the Text API uses the last occurrence only, because multiple occurrences of other commands conflict with each other. Multiple log comment commands post separate log comment messages to the ticket, and not necessarily in any particular order.

In addition, if a Text API ticket ID command appears in the message either at the beginning of the message or in between two other Text API commands, it is converted into a log comment. If the previous command is a log comment (%LOG=…) or update description (%DESCRIPTION=…), it is appended to that command, rather than becoming a separate log comment.

Incoming messages that are sent HTML-only, without a plain-text version included, lose their message body. If the message matches any mailbox rule filters with an empty message body, a ticket can be created with an empty Description, or with the quoted message subject as the entirety of the ticket description.

How the Text API Uses Keywords

You can use two types of keywords as input to the Text API.

- Definitions in the [KEYWORDS] section of the text_api.cfg file -- This type is a group of keywords that are related directly to the fields for the various tables that you can update. For example, most of the fields on the Issue Detail form are defined the [KEYWORDS] section. Using these keywords, you can set values for fields in the record that you are updating or creating. For example, the following line sets the priority of the issue to 5:

```
%PRIORITY=5
```

The [KEYWORDS] section of the text_api.cfg file lists all keywords. You can define additional keywords (for example, to allow Text API access to fields that you have added when customizing your database schema).

- The following special keywords are always defined as follows, regardless of the contents of the text_api.cfg file:

Keyword	Description
ASSET	Used to attaches an item to a ticket (valid for requests, issues, and change orders). The value specified is the item name, which must already exist. You can specify this keyword multiple times, because a ticket can have multiple items attached to it.
ATTACHMENT	Used internally by the email interface to add email attachments to a ticket.
DESCRIPTION	Specifies the value to use for the ticket's description field. This keyword is assumed if input is sent to the Text API without an explicit keyword. This keyword is applied automatically by the Mail Eater when the message does not begin with a keyword but does contain a ticket ID artifact or keyword. You can change how the DESCRIPTION keyword is handled for updates using the following entry in the [OPTIONS] section of text_api.cfg: UPDATE_DESC_IS_LOG If this option is set to YES, the value is used to create a log comment. If the value is set to NO, the value overwrites the existing description field.
FROM_EMAILFROM_EMAIL_OVERRIDE	Used by the email interface to match against the Email Address field in the ca_contact record. It is also used as the log_agent for the ticket. If both are supplied, FROM_EMAIL is ignored. **Note:** FROM_EMAIL is set automatically by the Mail Eater with the sender address of the message.
FROM_PERSID	Used by the command line interface to define the log_agent for an operation (for example, when a ca_contact record does not have a User ID). This keyword is passed automatically by pdm_text_cmd if the -p parameter is specified. The value is matched to a ca_contact record persistent_id.
FROM_USERID	Used only in the command line interface to define the log_agent for an operation. This keyword is passed automatically by pdm_text_cmd if the -u parameter is specified. The value is matched to a contact's User ID.
LOG	Used to create a log entry (valid for requests, change orders, issues, and contacts). This keyword is applied automatically by the Mail Eater when the message does not begin with a keyword but does contain either a ticket ID artifact or keyword, or a DESCRIPTION keyword.
LOG_AGENT	Used by the CA NSM interface to define the log_agent for an operation. The value is matched to a contact record's ID field.
PROPERTY	

Keyword	Description
	Used to set the value of a property (valid only for requests, change orders, and issues). Unlike other keywords, which are followed by an equal sign and a value, the PROPERTY keyword syntax must include the property label, as follows: PROPERTY={{property_label}}value You must specify the *property_label* exactly as it appears in the database.
SEARCH	Used only in the command-line interface and the CA NSM interface to supply a list of keywords for use in a query to update multiple tickets for an asset. The value is a list of keywords used in the search. The SEARCH keyword is automatically set by the CA NSM interface.
SEARCH_EXPLICIT	Used only in the CA NSM interface to override the SEARCH keyword supplied by the CA NSM interface. The values supplied are the same as the SEARCH keyword.

Keyword Input Conventions

The following conventions apply to keyword input formatting:

- Prefix every keyword (including PROPERTY) with a percent (%) sign. The percent sign must be in column position one. If the first nonempty line of the input does not have a percent sign at the start of the line, either %DESCRIPTION= or %LOG= is used as the prefix for the incoming data, depending on whether a ticket ID artifact or keyword was found. If %DESCRIPTION is set, the contents of the message up to the first Keyword is posted as a ticket description. If %LOG= is set, the contents of the message up to the first Keyword is posted as a log comment.
- Do not use any intervening spaces within the keyword between the percent sign and the keyword, or between the keyword and the equal (=) sign.
- Do not quote values; all data after the equal sign is assumed to be the value.
- Keywords are not case sensitive.
- If the input includes duplicate keywords, the last keyword is used; otherwise, the order in which you specify the keyword/value pairs is unimportant.
- Specify keyword values as you would for the corresponding field in the web interface. For example, to specify an Analyst contact type, you use %CONTACT_TYPE=Analyst, even though in the database this value is stored as an integer. The CONTACT_TYPE keyword is defined in text_api.cfg so that it converts the specified value (see page 3832) to match the stored value.

  Note: Whether the value is case sensitive depends on your underlying DBMS.

- You can extend string data across multiple lines.

Format an Email Message To Update a Ticket

A user can format an email message to create or update a ticket.

To format an email message to create or update a ticket, use the following fields:

- **To**
  Specifies the mailbox name assigned to the CA SDM contact set up for the privileged user.

- **From**
  Specifies the person sending the email. The person must be defined in the ca_contact table unless the Allow Anonymous option is specified in the applicable mailbox rule.

  Note: The From address is typically part of your email program configuration, and it is not typically set on a per-message basis.

- **Attachments**
  Attaches documents and other files to the email to send attachments to the Text API.

- **Subject**
  Matches keywords in a mailbox rule filter string, particularly when creating a ticket.

- **Body**
  Specifies the message body of the email using the Text API. You can specify the keyword ISSUE_ID, REQUEST_ID, or CHANGE_ID, depending on the type of ticket to create or update a ticket.

Start and End Email Message Delimiters

Some email interfaces add information to the beginning or end of mail messages (for example, MIME encoding) that can cause the email interface to malfunction. If your email interface adds information, you can use the following delimiters: start-request and end-request. The email interface ignores information that is specified prior to start-request and subsequent to end-request.

Note: The Mail Eater does not support emails in the RTF or HTML-only formats.

Example: Use start-request and end-request Delimiters

```
"start-request"
message_body
"end-request"
```

How the Text API Uses Artifacts

The Text API processes the subject or body of email notifications. Mailbox rules let you identify artifacts and values that the Text API uses. For example, you can define the rule for incidents as Incident:{{object_id}}, so finding Incident:1234 translates to %INCIDENT_ID=1234 for the Text API. 1234 is the ref_num for the Incident. Because the artifact must be unique in the email and easy to find, you can make the artifact more distinctive such as %Incident:{{object_id}}%.

Follow the {{object_id}} keyword with a character which is not a letter, number, comma, forward-slash (/), plus sign (+), or equals (=) sign, because these characters can appear within an artifact. Otherwise, it is possible that characters which follow the artifact can be misinterpreted as part of the value of the artifact, or that a character within the value of the artifact can be misinterpreted as the character which follows the value.

Mail Eater does the following:

1. Finds the artifact within an email (such as Incident:1234) that maps to the appropriate ticket or other object supported by the Text API.

2. Translates the artifact to a Text API token (such as %INCIDENT_ID=1234).

3. Mail Eater submits the tagged message to the Text API. The Text API processes the email, applies the text, commands, or both which it contains to the appropriate ticket, and generates an automatic response email indicating whether the email message it received was successfully applied. Depending on the actions performed, a notification email message is also sent separately to indicate certain specific events, such as the creation of a ticket.

How to Set Up Notification Replies to Update Tickets

The Text API daemon (pdm_text_nxd) creates and updates tickets with information from external interfaces, such as the command line and email. You can set up mail to use the Text API so that users (contacts) can update tickets by replying to email notifications. The text of the reply is added as a log comment activity to the ticket.

To set up notification replies to update tickets, do the following:

1. Set the notification method that the contact uses to pdm_mail - T *reply_email_address* or pdm_mail - F *reply_email_address.* The *reply_email_address* specifies the incoming address for the mailbox. When the contact clicks reply on an email that address is filled in from the From or Reply-To address of the message to which they are replying.
   -T sets the Reply-To address. -F sets the From address, which is used as the reply address if a separate one is not specified.

   Note: Some mail programs do not or cannot honor a Reply-To address.

2. Create or update a mailbox rule using a Text API keyword.
   The user-defined artifacts in the mailbox rule filters replace the following Text API keywords:

Object	Text API Keyword	Identifier
Incident	%INCIDENT_ID	Ref_num
Problem	%PROBLEM_ID	Ref_num
Request	%REQUEST_ID	Ref_num
Chg_ref_num	%CHANGE_ID	Chg_ref_num
Issue	%ISSUE_ID	Ref_num

1. Create or update a notification phrase that matches the rule.
2. Create or update a message template that uses the notification phrase.
3. Update the mailbox rule that you created in Step 2 to specify the message template that you created or updated in Step 4.

After the user receives the notification and replies to it, the following actions occur:

1. When the filter string is found, the relevant ticket ID keyword and value denoted by the placeholder, if any, are appended to the message.
2. If a matching ticket ID artifact is found, the corresponding ticket is updated, with either a log comment, a new description, or other values in accordance with the text, keywords, and commands in the message.
3. If a matching ticket ID artifact is not found, a ticket is created with a description and other parameters in accordance with the text, keywords, and commands in the message.

How to Set Up a Reply to an Incident Notification Example

This example shows how to set up a reply to an incident notification.

To set up a reply to an incident notification, do the following:

1. Create a mailbox rule using the following fields and values:
   - Filter -- Body contains
   - Filter String -- %Incident:{{object_id}}%
   - Ignore Case -- YES
   - Action -- Update Object
   - Action Object -- Incident
2. Create a notification phrase that includes the rule as follows:
   - Symbol -- Incident Reply
   - Code -- IncidentReply
   - Active -- Active
   - Description -- Comment that embeds the reply for an Incident/Problem/Request.
   - Phrase -- In order to add a comment to your @{call_req_id.type.sym}, just reply to this email or include the line below (on a line by itself):

```
%Incident:{call_req_id.ref_num}%
```

Note: In auto-reply text of the mailbox rule, omit the call_req_id. prefix. This prefix applies a context which the mailbox rule text is already in, and such a context change is not valid when already acting within that context.

3. Create or update a message template that uses the notification phrase as follows:

   - Notification Message Body

```
This is a simple notification.

@{notification_phrase[IncidentURL1].phrase}
```

4. Update the mailbox rule that you created in Step 1 to specify the message template that you created in Step 3, as follows:
   Message Template -- *mailbox rule name*

How an End User Updates a Ticket Example

The following example demonstrates how an end user (John Smith) replies to an email notification to update an incident ticket.

The Body or Subject of the email includes the object identifier. The {{object_id}} placeholder within the filter string denotes the object identifier.

1. A notification is sent to John Smith and includes the following instructions:

```
In order to add a comment to your incident, just reply to this email or include
the line below (on a line by itself).
%Incident:1234%
```

2. John Smith replies to the notification as follows:

```
This is my response...
```

3. The Mail Eater receives the following text version of the John Smith's email:

```
This is my response...
From: Service Desk
Sent: Wednesday, September 18, 2009 10:22 AM
To: Smith, John
Subject: Simple Notification
This is a simple notification.
In order to add a comment to your incident, just reply to this email or include
the line below (on a line by itself).
%Incident:1234%
```

4. The Mail Eater processes rules in order and finds the %Incident:1234% artifact:

```
This is my response...
From: Service Desk
Sent: Wednesday, September 18, 2009 10:22 AM
To: Smith, John
```

```
Subject: Simple Notification
This is a simple notification.
In order to add a comment to your incident, just reply to this email or include
the line below (on a line by itself).
%INCIDENT_ID=1234
```

5. The Mail Eater adds the Text API keywords and the {{object_id}} value to an %INCIDENT_ID= statement and leaves a marker where the {{object_id}} value was found. The following text shows the data that is sent to the Text API. The bold text shows values added by the Mail Eater.

```
%LOG=This is my response...
From: Service Desk
Sent: Wednesday, September 18, 2009 10:22 AM
To: Smith, John
Subject: Simple Notification
This is a simple notification.
In order to add a comment to your incident, just reply to this email or include
the line below (on a line by itself).
%Incident:-((...))-%
%FROM_EMAIL=john.smith@company.com
%INCIDENT_ID=1234
```

6. The Text API add a log comment for Incident 1234.

Keyword Conversion Methods

Many of the keywords defined in text_api.cfg have an associated method to convert the value specified to a value that is appropriate for storage in the database. This feature lets users specify values just as they would in the web interface without having any knowledge of the underlying implementation.

The configuration file has several examples of this type of keyword definition, including ISSUE. PRIORITY and CONTACT.CONTACT_TYPE. If you need to define additional keywords (for example, to allow Text API access to fields that you have added when customizing your database schema), you can use one of the following predefined methods:

Method	Output Type
lookup_actbool	INTEGER
lookup_asset_by_name	UUID
lookup_asset_by_persid	UUID
lookup_chg_category	STRING
lookup_chg_status	STRING
lookup_cnt_by_email	UUID
lookup_cnt_by_last_first_middle	UUID
lookup_cnt_by_logonid	UUID
lookup_cnt_by_persid	UUID
lookup_cnt_meth	INTEGER

Method	Output Type
lookup_cnt_type	INTEGER
lookup_company	UUID
lookup_cr_status	STRING
lookup_cr_template	STRING
lookup_domain	INTEGER
lookup_grc	INTEGER
lookup_group	UUID
lookup_impact	INTEGER
lookup_iss_category	STRING
lookup_iss_status	STRING
lookup_loc	UUID
lookup_mfr_model	UUID
lookup_nr_family	INTEGER
lookup_org	UUID
lookup_person_contacting	INTEGER
lookup_position	INTEGER
lookup_priority	INTEGER
lookup_prob_category	STRING
lookup_product	INTEGER
lookup_resource_status	INTEGER
lookup_service_lvl	STRING
lookup_severity	INTEGER
lookup_state	INTEGER
lookup_timezone	STRING
lookup_type_of_contact	INTEGER
lookup_urgency	INTEGER
lookup_workshift	STRING

If the value you need to convert is not addressed by any of these predefined methods, you need to write a customized method. The method should take a STRING value as its input and return a value (either INTEGER, STRING or UUID) as its output. Return a value of -1 (or “-1”) to denote that the value cannot be determined and is therefore, not set. For UUID, return a “(uuid) NULL”.

For example, you might develop a method to convert a user ID to a ca_contact table reference. The incoming value, such as Administrator, would be passed to the method, and the method would return the ca_contact table id for the user ID of Administrator.

The manner in which you define keywords in the configuration file offers you the advantage of defining multiple keyword mappings to the same field, including different conversion methods, depending on the value being specified. For example, assignee can have several different keyword

mappings to define how to set its value based on different input values. One input might be user ID, another might be last name, first name, middle name, and still another might be the actual ca_contact id (for example, 793ED69B4E87A545BD8E911834D829FC). Each keyword maps to a different conversion method, except the last one, which does not need to be converted.

The Configuration File

This article contains the following topics:

The text_api.cfg file defines the keywords that are related directly to the fields of the various tables that you can update. You use this file both as a reference to find certain predefined values, such as keywords, and as a mechanism for configuring the Text API, although the default configuration file works for most installations without modification.

The text_api.cfg file is located in the following directory:

- UNIX -- $NX_ROOT/site
- Windows -- *installation-directory*\site. For example: C:\Program Files\CA\Service Desk\site

The configuration file is divided into sections, with particular attributes defined within each section. Attribute definitions are of the following form:

```
keyword=value
```

None of the keywords are case-sensitive, whereas all values (except in the [OPTIONS] section) are case-sensitive.

Note: You can view and modify the text_api.cfg file using any text editor.

Important! If you are integrating with the CA NSM Alert Management Systems component, you must update text_api.cfg for any additional fields that are passed to CA SDM.

Options

The [OPTIONS] section of the text_api.cfg file defines processing options that may differ from one site to another. For example, there are options to determine the incoming date format, which fields allow linefeeds to be retained, and whether to allow issues, requests, or change orders to be updated using the email interface. All options in this section are configurable. Be aware that although you can remove table names from the VALID_TABLE_LIST, if you do not want to support Text API access to those tables, you cannot add table names to this list.

Defaults

Use the [XX_DEFAULTS] section provided in the text_api.cfg file for each interface using the Text API (for example, [EMAIL_DEFAULTS] for the email interface and [CMD_DEFAULTS] for the command line interface). The [XX_DEFAULTS] section defines the default values for fields and properties that are required in case the user does not supply them directly. XX refers to the interface type, such as CMD or EMAIL.

To set default values, use one of the following formats:

- table_name**.**keyword**=**value
  The *keyword* must be defined either in the [KEYWORDS] section or as properties in your database. Any method associated with the keyword is automatically applied to the *value*. For example:

  ```
  ISSUE.PRIORITY=1
  ```

  The PRIORITY keyword is defined in text_api.cfg so that it performs a lookup to convert the value you specify to match the corresponding value that is stored in the database. Here, value 1 is converted to 5, which is the underlying database value for the priority symbol 1. This feature lets users specify the value just as they would in the web interface.

- table_name**.PROPERTY={{**property_label**}}**value
  The *property_label* must be defined as a property in your database.

In both formats, the *table_name* must be one of the values defined by VALID_TABLE_LIST in the [OPTIONS] section, such as Issue, Request, or Contact.

Ignore Incoming

There are several [..._IGNORE_INCOMING] sections in the text_api.cfg file, one for each interface that uses the Text API (for example [TNG_IGNORE_INCOMING] for the CA NSM interface and [EXT_IGNORE_INCOMING] for the external interface used by other CA products). These sections define fields and properties that are ignored in the input (the format is the same as described in Defaults, except no "**=***value*" is specified). This feature lets you prevent users from setting certain values, which in turn, provides you with more security for such times as letting customers use the email interface.

The IGNORE sections work well when used in conjunction with the corresponding [..._DEFAULTS] sections because you can prevent the user from setting a particular value and supply a default value at the same time. For example, if you want to prevent email interface users from setting the priority of an issue, you could set the following values:

```
[EMAIL_DEFAULTS]
ISSUE.PRIORITY=2
[EMAIL_IGNORE_INCOMING]
ISSUE.PRIORITY
```

In this case, any priority that the user specifies in the email message body is ignored, and all issues created by the email interface are automatically assigned a priority of 2.

Example Input

The following examples show input that you can use in the body of an email message or in a file serving as input to the command-line interface.

Example: First Line Does Not Include a Keyword

In this example, because the first line is missing a %keyword in the first column, the literal % DESCRIPTION= is added to the beginning of the message. This addition sets the description field to "This entire text goes to the description field" (with the line break intact, because ISSUE.DESCRIPTION is included in the list of fields for the LINEFEEDS_ALLOWED entry in the [OPTIONS] section of text_api.cfg).

```
This entire text goes
into the description field
%PRIORITY=None
```

Example: First Line Includes a Keyword

In this example, the PRIORITY keyword is defined in text_api.cfg so that it performs a lookup to convert the value you specify to match the corresponding value that is stored in the database. Here, the value None is converted to 0, which is the underlying database value for the priority symbol 1. This feature lets users specify the value as they would in the web interface.

```
%description=This is my description
%priority=None
%CATEGORY=Upgrade.PC
%PROPERTY={{Current CPU}}266 mhz
%PROPERTY={{Current Harddrive}}1 gig
%PROPERTY={{Requested Upgrade}}4 gig harddrive
```

The specified values are used to set the description and priority fields for the ticket, similar to the previous example (notice that keyword case is unimportant).

The value of Upgrade.PC is searched, and the category field for the ticket is set appropriately.

Matching the following labels sets the three property values:

- Current CPU
- Current Hard drive
- Requested Upgrade

View Field Descriptions

This article contains the following topics:

You can use the field description information in the basic and advanced views that are supplied with CA SDM.

The following points apply to many of the tables:

- You must turn on audit logging, found in Administration, Options Manager, Audit Log, to see data in the advanced views.
- pdmtime refers to date/time fields that are in GMT format (the number of elapsed seconds since 1/1/1970).
- The terms change request and change order are used interchangeably.

View_Act_Log

The following is a basic view of the request activity log table. Activity type and the analyst's full name are also listed in the view. The activity log table (act_log) was joined with the activity type table (act_type) and the contact table (ca_contact) to give the actual activity type of each activity log entry, and the analyst who performed the activity. Extracted fields from the joins that might be useful are located at the end of this list.

Field	Remarks
id	act_log.id: The unique identifier for this record in the act_log table.

Field	Remarks
persid	act_log.persid: The unique identifier for this record in the act_log table, preceeded by the object identifier (alg for act_log) and a colon.
call_req_id	act_log.call_req_id: Pointer to call request persid to which this activity belongs. act_log.call_req_id = call_req.persid.
last_mod_dt	act_log.last_mod_dt: The last modify date/time (pdmtime).
time_spent	act_log.time_spent: The duration of time spent on this activity, stored as the total number of seconds. For example, 80 = 1 minute, 20 seconds.
time_stamp	act_log.time_stamp: User modifiable date/time of activity (pdmtime).
system_time	act_log.system_time: The date/time of record creation (pdmtime).
analyst	act_log.analyst: The uuid pointer to the contact uuid to get the analyst who performed the activity. act_log.analyst = ca_contact.contact_uuid.
description	act_log.description: The text description of this activity, which can be modified by the user.
action_desc	act_log.action_desc: The text description of automated action, which cannot be modified by the user.
type	act_log.type: The text pointer to a record in the activity type table. For example, act_log.type = act_type.code.
knowledge_session	act_log.knowledge_session: An identifier for a particular session of a particular user.
knowledge_tool	act_log.knowledge_tool: An indicator of the knowledge management tool used for the search, such as NLS_FAQ or EXPERT, etc.
internal	act_log.internal: An integer flag (1 or 0), which indicates if this log entry is intended for all to see or just for internal use.
activity_type	act_type.symActivity: The type derived from act_log.type = act_type.code.
analyst_lastname	View_Contact_Full.last_name: The analyst's last name, derived from act_log.analyst = ca_contact.contact_uuid.
analyst_firstname	View_Contact_Full.first_name: The analyst's first name.
analyst_middlename	View_Contact_Full.middle_name: The analyst's middle name.

View_Audit_Assignee

The following is an advanced view of the audit log where assignee is tracked. This view shows the duration of time between assignee changes for every request and change order. Requests or change orders that are changed from a particular assignee to a null assignee, and then from null assignee back to a particular assignee, do not have the duration of the null assignee listed in this view. This view lists the following fields for both requests and change orders. There may be more than one entry for each audobj_uniqueid (request or change order).

Field	Remarks
audobj_uniqueid	audit_log.audobj_uniqueid: The audit log object unique id representing the chg.id or the call_req.id.
from_val	audit_log.attr_after_val: The 'changed from' assignee value.
to_val	audit_log.attr_after_val: The 'changed to' assignee value.
from_time	audit_log.attr_from_time: The beginning time an assignee was assigned (pdmtime).
to_time	audit_log.attr_from_time: The ending time the same assignee was assigned (pdmtime).

View_Audit_Group

The following is an advanced view of the audit log where group is tracked. This view shows the duration of time between group changes for every request and change order. Requests or change orders that are changed from a particular group to null group, and then from null group back to a particular group, do not have the duration of the null group listed in this view. This view lists the following fields for both requests and change orders. There may be more than one entry for each audobj_uniqueid (request or change order).

Field	Remarks
audobj_uniqueid	audit_log.audobj_uniqueid: The audit log object unique id which represents chg.id or call_req.id.
from_val	audit_log.attr_after_val: The 'changed from' group value.
to_val	audit_log.attr_after_val: The 'changed to' group value.
from_time	audit_log.attr_from_time: The beginning time group was assigned (pdmtime).
to_time	audit_log.attr_from_time: The ending time same group was assigned (pdmtime).

View_Audit_Priority

The following is an advanced view of the audit log where priority is tracked. This view shows the duration of time between priority changes for every request and change order. This view lists the following fields for both requests and change orders. There may be more than one entry for each audobj_uniqueid (request or change order).

Field	Remarks
audobj_uniqueid	audit_log.audobj_uniqueid: The audit object unique id, represents a request call_req.id or change order chg.id.
from_val	audit_log.attr_after_val: The 'changed from' value of priority.
to_val	audit_log.attr_after_val: The 'changed to' value of priority.
from_time	audit_log.attr_from_time: The beginning time priority was in a particular state (pdmtime).
to_time	audit_log.attr_from_time: The ending time priority was in the same state (pdmtime).

View_Audit_Status

The following is an advanced view of the audit log where status is tracked. This view shows the duration of time between status changes for every request and change order. This view lists the following fields for both requests and change orders. There may be more than one entry for each audobj_uniqueid (request or change order).

Field	Remarks
audobj_uniqueid	audit_log.audobj_uniqueid: The audit object unique id, which represents a request call_req.id or change order chg.id.
from_val	audit_log.attr_after_val: The 'changed from' value of priority.
to_val	audit_log.attr_after_val: The 'changed to' value of priority.
from_time	audit_log.attr_after_time: The beginning time status was in a particular state (pdmtime).
to_time	audit_log.attr_after_time: The ending time status was in the same state (pdmtime).

View_Change_Act_Log

The following is a basic view of all change order activity logs. This is a view of the change request activity log table (chgalg) joined with the activity type table (act_type) and the contact table (ca_contact) to give more meaningful data, such as the actual activity type description and full name of the analyst who performed the activity.

Field	Remarks
id	chgalg.id: The unique identifier for this record in the chgalg table.
persid	chgalg.persid: The unique identifier for this record in the chgalg table, preceded by the object identifier (chgalg for chgalg) and a colon.
change_id	chgalg.change_id: The pointer to the change order id to which this activity belongs. chgalg.change_id = chgalg.id
last_mod_dt	chgalg.last_mod_dt: The last modify date/time (pdmtime).
time_spent	chgalg.time_spent: The duration of time spent on this activity, stored as the total number of seconds. For example, 80 = 1 minute, 20 seconds.
time_stamp	chgalg.time_stamp: The user modifiable date/time of activity (pdmtime).
system_time	chgalg.system_time: The date/time of record creation (pdmtime).
analyst	chgalg.analyst: The uuid pointer to the contact uuid to get the analyst who performed the activity.chgalg.analyst = ca_contact.contact_uuid
description	chgalg.description: The text description of this activity, which can be modified by the user.
action_desc	chgalg.action_desc: The text description of the automated action, which cannot be modified by the user.
type	chgalg.type: The text pointer to a record in the activity type table.chgalg.type = act_type.code
internal	chgalg.internal: The integer flag (1 or 0), which indicates if this log entry is intended for all to see or just for internal use.

Field	Remarks
knowledge_session	chgalg.knowledge_session: An identifier for a particular session of a particular user.
knowledge_tool	chgalg.knowledge_tool: An indicator of the knowledge management tool used for the search, such as NLS_FAQ or EXPERT, and so on.
analyst_last name	View_Contact_Full.last_name: The analyst's last name, derived from chgalg.analyst = ca_contact.contact_uuid.
analyst_first name	View_Contact_Full.first_name: The first name of the analyst.
analyst_middlename	View_Contact_Full.middle_name: The middle name of the analyst.
activity_type	act_type.sym: The activity type referenced by chgalg.type = act_type.code.

View_Change

The following is a basic view of all change orders, listing the status, priority, category, organizations, the affected end user's full name, the requester's full name, the assignee's full name, the group name and ID, and so on. Here, the change request table (chg) was joined with many other tables to give some more meaningful data about the change order.

Field	Remarks
id	chg.id: The unique identifier for this record in the chg table.
persid	chg.persid: The unique identifier for this record in the chg table, preceded by the object identifier (chg for table chg) and a colon.
chg_ref_num	chg.chg_ref_num: The change order reference number, which is used by analysts and customers to refer to a particular change order.
description	chg.description: The long description of a change order, as dictated by an analyst or customer.
status	chg.status: The unique identifier of a change order status, which is a pointer to the chgstat table.chg.status = chgstat.code.
active_flag	chg.active_flag: The integer flag to determine whether this change record is active or not (1 or 0).
start_date	chg.start_date: The date the first task goes to a pending status (pdmtime).
open_date	chg.open_date: The change order creation date (pdmtime).
last_mod_dt	chg.last_mod_dt: The last modified date (pdmtime).
last_mod_by	chg.last_mod_by: The pointer to the contact uuid who was the last contact to modify this change order.chg.last_mod_by = ca_contact.contact_uuid.
close_date	chg.close_date: The date the change order was set to inactive (pdmtime).
resolve_date	chg.resolve_date: The date the change order was set to a status configured to indicate the change was resolved (pdmtime).
rootcause	chg.rootcause: A pointer to a record in the rootcause table, which represents the original situation which required this change order to be executed.chg.rootcause = rootcause.id.

Field	Remarks
est_total_time	chg.est_total_time: The estimated total time (pdmtime) it will take to complete this change.
actual_total_time	chg.actual_total_time: The actual total time (pdmtime) it took to complete this change.
log_agent	chg.log_agent: A binary unique identifier referencing the ca_contact table, referencing the person who was the change's original creator.chg.log_agent = ca_contact. contact_uuid.
assignee	chg.assignee: The pointer to the contact uuid who is currently assigned to the change order.chg.assignee = ca_contact.contact_uuid.
organization	chg.organization: The pointer to internal organization uuid, which represents the organization to whom this change order belongs.chg.organization = ca_organization. organization_uuid.
group_id	chg.group_id: The pointer to contact uuid, which represents the group currently assigned to the change order.chg.group_id = ca_contact.contact_uuid
affected_contact	chg.affected_contact: The pointer to the contact uuid, which represents the affected contact for this change order.chg.affected_contact = ca_contact.contact_uuid
requestor	chg.requrestor: The pointer to the contact uuid, which represents the person who ordered the change.chg.requestor = ca_contact.contact_uuid
category	chg.category: The pointer to the change category code to get the category into which this change falls.chg.category = chgcat.code
priority	chg.priority: The pointer to priority enum, which represents the priority into which this change falls.chg.priority = pri.enum
need_by	chg.need_by: The date which indicates when the affected_end_user needs to have the change completed (pdmtime).
est_comp_date	chg.est_comp_date: The estimated completion date (pdmtime) for this Change Order.
actual_comp_date	chg.actual_comp_date:The actual completion date (pdmtime) of this change order.
est_cost	chg.est_cost: The estimated cost of this change order.
actual_cost	chg.actual_cost: The actual cost to implement this change order.
justification	chg.justification: A text field which allows a requestor to document the reason(s) this change is required.
backout_plan	chg.backout_plan: A text field that allows an analyst to document a backout plan for this change.
impact	chg.impact: A pointer to an impact table record, which indicates the scope of resources that this change affects.chg.impact = impact.enum
parent	chg.parent: A pointer to another change request id, which allows creation of a hierarchy of change orders.chg.parent = chg.id
effort	chg.effort: A text field which explains the plan for implementing this change order.
support_lev	chg.support_lev: A pointer to a service desc record, which automates some constraints for which this change must be completed.chg.support_lev = srv_desc.code
template_name	chg.template_name: The name of and pointer to a change order template.chg. template_name = chg_template.template_name

Field	Remarks
sla_violation	chg.sla_violation: The integer to count the number of times slas attached to this "change has been violated".
predicted_sla_viol	chg.predicted_sla_viol: (r5.5) Neugent related technology field.
macro_predict_viol	chg.macro_predict_viol: (r5.5) Neugent related technology field.
created_via	chg.created_via: A pointer to a record in the interface table, which indicates from which interface the change order originated. chg.created_via = interface.id
call_back_date	chg.call_back_date:A date/time field (pdmtime), which indicates a future date/time the requestor is to be contacted.
call_back_flag	chg.call_back_flag: A boolean indicator displayed as a checkbox to the user, indicating whether or not to notify the analyst at the chg.call_back_date.
string1	This is a user-definable text field.
string2	This is a user-definable text field.
string3	This is a user-definable text field.
string4	This is a user-definable text field.
string5	This is a user-definable text field.
string6	This is a user-definable text field.
service_date	chg.service_date: The Date/ Time (pdmtime) that an outside vendor is expected to spend to service this change order.
service_num	chg.service_num: The text field to document an outside vendor's service or purchase order number.
product	chg.product: A pointer to a record in the product table, which indicates the product that is affected by this change.chg.product = product.id
actions	chg.actions: A big text field for documenting actions.
type_of_contact	chg.type_of_contact: A pointer to a record in the toc table, which indicates a general categorization of the affected_end_user's perspective of the change order.chg. type_of_contact = toc.id
reporting_method	chg.reporting_method: A pointer to a record in the repmeth table, which classifies the origination of the change order, and is selected by the person creating the change order.chg.reporting_method = repmeth.id
person_contacting	chg.person_contacting: A pointer to a record in the perscon table, which indicates the role of the affected_end_user or requestor.chg.person_contacting = perscon.id
status_name	chgstat.sym: The description of the status as seen by a user.chg.status = chgstat.code
priority_num	pri.sym: The description of the priority as seen by a user.chg.priority = pri.enum
category_name	chgcat.sym: The name of the Change Category as viewed by a user.chg.category = chgcat.code
organization_name	ca_organization.org_name: The name of an organization as viewed by a user.chg. organization = ca_organization.organization_uuid
affected_end_user_lastname	ca_contact.last_name: The affected end user's last name.chg.affected_end_user = ca_contact.contact_uuid

Field	Remarks
affected_end_user_firstname	ca_contact.first_name: The affected end user's first name.chg.affected_end_user = ca_contact.contact_uuid
affected_end_user_middlename	ca_contact.middle_name: The affected end user's middle name.chg.affected_end_user = ca_contact.contact_uuid
requester_lastname	ca_contact.last_name: The requestor's last name.chg.requestor = ca_contact.contact_uuid
requester_firstname	ca_contact.first_name: The requestor's first name.chg.requestor = ca_contact.contact_uuid
requester_middlename	ca_contact.middle_name: The requestor's middle name.chg.requestor = ca_contact.contact_uuid
business	ca_organization.org_name: The name of the Requester's organization as seen by users.chg.requestor = ca_organization.organization_uuid
assignee_lastname	ca_contact.last_name: The assignee's last name.chg.assignee = ca_contact.contact_uuid
assignee_firstname	ca_contact.first_name: The assignee's first name.chg.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name: The assignee's middle name.chg.assignee = ca_contact.contact_uuid
groupID	ca_contact.contact_uuid: A binary representation of the internal id used for the group assigned to this change order.chg.group_id = ca_contact.contact_uuid
group_name	ca_contact.last_name: The name of the group assigned to this change order.chg.group = ca_contact.contact_uuid
service_type	srv_desc.sym: The name of the service type applied to this change order.chg.support_lev = srv_desc.code
impact_num	impact.sym: The description of the impact as seen by users.chg.impact = impact.enum
product_sym	product.sym: The product description as seen by users.chg.product = product.id
type_of_contact_sym	toc.sym: The Type Of Contact description as seen by users.chg.type_of_contact = toc.id
rpting_method_sym	repmeth.sym: The Reporting method description as seen by users.chg.reporting_method = repmeth.id
person_contacting_sym	perscon.sym: The Person Contacting description as seen by users.chg.person_contacting = perscon.id

View_Change_to_Assets

The following list of fields is a basic view of change orders and their assets. The change request table (chg) is indirectly joined with the network resource table (ca_owned_resource) to get a list of each change order's assets. This view may not list all change orders, particularly those that have no assets.

Field	Remarks
	All fields listed in the View_Change view defined earlier in this document.

Field	Remarks
View_Change.*	
assetID	ca_owned_resource.own_resource_uuid: The binary field which serves as the internal, unchanging unique identifier for an asset record.
asset_serial_num	ca_owned_resource.serial_number: The serial number for an asset record.
asset_class	ca_resource_class.name: A short description of the class to which an asset belongs. ca_owned_resource.resource_class = ca_resource_class.id
asset_family	ca_resource_family.name: The family of assets to which this asset belongs. ca_owned_resource.resource_class = ca_resource_class.id AND ca_resource_class.family_id = ca_resource_family.id
asset_name	ca_owned_resource.resource_name: The network name by which this asset is known.

View_Change_to_Change_Act_Log

The following is a basic view of all change orders and the activity logs that go with them. This view joins the View_Change view with the Change Order Activity Log (chgalg) to give detailed information about change orders and their activity logs.

Field	Remarks
View_Change.*	This shows all fields listed in the View_Change view defined earlier in this document.
chgalg_id	chgalg.id: The unique identifier for this record in the chgalg table.
chgalg_persid	chgalg.persid: The unique identifier for this record in the chgalg table, preceded by the object identifier (chgalg for chgalg) and a colon.
change_id	chgalg.change_id: This is a pointer to change the order id to which this activity belongs. chgalg.change_id = chgalg.id
chgalg_last_mod_dt	chgalg.last_mod_dt: The last modify date/time (pdmtime).
time_spent	chgalg.time_spent: The duration of time spent on this activity, stored as the total number of seconds. For example, 80 = 1 minute, 20 seconds.
time_stamp	chgalg.time_stamp: The user modifiable date/time of activity (pdmtime).
system_time	chgalg.system_time: The date/time of record creation (pdmtime).
analyst	chgalg.analyst: The uuid pointer to contact uuid to get the analyst who performed the activity.chgalg.analyst = ca_contact.contact_uuid
chgalg_description	chgalg.description: The text description of this activity, which can be modified by the user.
action_desc	chgalg.action_desc: The text description of automated action, which cannot be modified by the user.

Field	Remarks
type	chgalg.type: The text pointer to a record in the activity type table.chgalg.type = act_type.code
internal	chgalg.internal: The integer flag (1 or 0), which indicates if this log entry is intended for all to see or just for internal use.
knowledge_session	chgalg.knowledge_session: This is an identifier for a particular session of a particular user.
knowledge_tool	chgalg.knowledge_tool: This is an indicator of the knowledge management tool used for the search, such as NLS_FAQ or EXPERT, and so on.
chgalg_analyst_id	chgalg.analyst: This is the uuid pointer to contact uuid to get the analyst who performed the activity.chgalg.analyst = ca_contact.contact_uuid

View_Change_to_Change_WF

This view is a result of the View_Change view joined with the Workflow task table (wf) to give a basic view of change orders and their workflow tasks. This may not list all change orders, particularly when there are no workflow tasks assigned.

Field	Remarks
View_Change.*	This shows all fields listed in the View_Change view defined earlier in this document.
wf_id	wf.id: The unique identifier for a record in the wf table.
wf_persid	wf.persid: This is a unique identifier for this record in the wf table, preceded by the object identifier (wf for wf) and a colon.
del	wf.del: This is a boolean indicator. It specifies whether this record is to be displayed to the user.
object_type	wf.object_type: This is the factory name, which is used to identify the type of record (for example, chg) to which this workflow task is attached.
object_id	wf.object_id: This is the unique identifier used to identify the specific record to which this workflow task is attached.wf.object_id = chg.id
task	wf.task: This is an identifier, which references the type of task this record represents.wf.task = tskty.code
wf_template	wf.wf_template: This is an identifier, which references from which template this workflow task record was created.wf.wf_template = wftpl.id
sequence	wf.sequence: This is an integer, which indicates the order this particular workflow task record should be displayed and executed by CA SDM (for example, Ascending).
wf_status	wf.status: This is an identifier, which references a tskstat record that indicates the current status of this workflow task.wf.status = tskstat.code
group_task	wf.group_task: This is a Boolean, which indicates whether this task belongs to a group.
asset	wf.asset: This is a UUID (binary) identifier, which references a record in the ca_owned_resource table.wf.asset = ca_owned_resource.own_resource_uuid
creator	

Field	Remarks
	wf.creator: This is a UUID (binary) identifier, which references a record in the ca_contact table. It indicates the person who created this workflow task.wf.creator = ca_contact. contact_uuid
date_created	wf.date_created: This is the Date/timestampe this workflow task was created (pdmtime).
wf_assignee	wf.assignee: This is the UUID (binary) identifier, which references a record in the ca_contact table. It indicates the person who is currently assigned to this workflow task.wf.assignee = ca_contact.contact_uuid
done_by	wf.done_by: This is the UUID (binary) identifier, which references a record in the ca_contact table. It indicates the person who completed or approved this workflow task.wf.done_by = ca_contact.contact_uuid
wf_start_date	wf_start_date: This is the timestamp when the workflow task moved into an active status (pdmtime).
wf_est_comp_date	wf.est_comp_date: This is the timestamp (pdmtime) when users believe this task will be completed.
est_duration	wf.est_duration: This is the estimated duration for this workflow task.
completion_date	wf.completion_dat: This is the timestamp (pdmtime) when this workflow task was completed.
actual_duration	wf.actual_duration: This is the actual amount of time it took to complete this workflow task.
wf_est_cost	wf.est_cost: This is the estimated cost of this workflow task.
cost	wf.cost: This is the actual cost required to complete this workflow task.
wf_description	wf.description: This is the description of the workflow task.
wf_last_mod_dt	wf.last_mod_dt: This is the timestamp (pdmtime) when this workflow task was last changed.
wf_last_mod_by	wf.last_mod_by: This is the UUID (binary) unique identifier referencing a record in the contact table, which indicates the last person to make changes to this workflow task.wf. last_mod_by = ca_contact.contact_uuid

View_Change_to_Properties

This view is a result of the View_Change view joined with the Properties table (prp) to give a basic view of change orders and their assigned properties. This may not list all change orders, particularly when there are no properties assigned.

Field	Remarks
	This shows all fields listed in the View_Change view defined earlier in this document.

Field	Remarks
View_Change.*	
prp_id	prp.id: This is an integer unique identifier for the property record.
prp_persid	prp.persid: This is a unique identifier for this record in the wf table, preceded by the object identifier (prp for prp) and a colon.
object_type	prp.object_type: This is the factory name, which is used to identify the type of record (for example, chg) to which this property record is attached.
object_id	prp.object_id: This is the unique identifier used to identify the specific record to which this property is attached.prp.object_id = chg.id
sequence	prp.sequence: This is an integer that indicates the order for which this particular property record should be displayed by CA SDM (for example, Ascending).
property	prp.property: This is an identifier, which references a record in the prptpl table. It represents the template from which this property was created.prp.property=prptpl.code
value	prp.value: This is the value entered by the user in response to the prp_description and prp.label fields.
prp_last_mod_dt	prp.last_mod_dt: This is the timestamp (pdmtime) when this property was last modified.
prp_last_mod_by	prp.last_mod_by: This is a binary identifier, which references a record in the ca_contact table. It represents the person who last modified this record.prp.last_mod_by = ca_contact.contact_uuid
required	prp.required: This is a Boolean indicating whether this property must have a prp.value before the record is saved.
sample	prp.sample: This is a text field, which displays example values to guide the user in typing the most useful value in prp.value.
prp_description	prp.description: This is a text field, which explains what kind of value should be entered in prp.value.
label	prp.label: This is a short description of what should be placed in the prp.value field.

View_Change_to_Request

The following is a basic view of change orders that have assigned requests only. This view is a result of the View_Change view joined with the request table (call_req) to give details about the change order and its associated request.

Field	Remarks
View_Change.*	This shows all fields listed in the View_Change view defined earlier in this document.
cr_id	call_req.id: This is the unique identifier for this record in the call_req table.
ref_num	call_req.ref_num: This is the Request reference number, which is used by analysts and customers to refer to a particular Request.
	call_req.summary: This is a brief description of the request for quick reference.

Field	Remarks
cr_summary	
cr_persid	call_req.persid: This is a unique identifier for this record in the call_req table, preceded by the object identifier (cr for table call_req) and a colon.
cr_description	call_req.description: This is the long description of a request, as dictated by an analyst or customer.
cr_status	call_req.status: This is a unique identifier referencing a record in the cr_stat table. It indicates the status of this request:call_req.status = cr_stat.code
cr_active_flag	call_req.active_flag: This is the Integer flag used to determine whether this request record is active (1 or 0).
time_spent_sum	call_req.time_spent_sum: This is the derived total of all act_log records' time_spent fields, stored in seconds (i.e. 80 = 1 minute 20 seconds).
cr_open_date	call_req.open_date: This is the Request creation timestamp (pdmtime).
cr_last_mod_dt	call_req.last_mod_dt: This is the last modified timestamp (pdmtime).
cr_close_date	call_req.close_date: This is the Timstamp for when the request was set to inactive (pdmtime).
cr_log_agent	call_req.log_agent: This is a binary unique identifier referencing the ca_contact table. It references the person who was the request's original creator.call_req.log_agent = ca_contact.contact_uuid
cr_group_id	call_req.group_id: This is a binary unique identifier referencing a record in the ca_contact table. It represents the group currently assigned to the request.call_req.group_id = ca_contact.contact_uuid
cr_assignee	call_req.assignee: This is a binary unique identifier referencing a record in the ca_contact table. It represents the person currently assigned to the request.call_req.assignee = ca_contact.contact_uuid
customer	call_req.customer: This is a binary unique identifier referencing a record in the ca_contact table. It represents the affected end user for this request.call_req.customer = ca_contact.contact_uuid
charge_back_id	charge_back_id: This is a text field available for use as an indicator of accounting jargon for expensing this request to the appropriate cost center.
affected_rc	call_req.affected_rc: This is a binary unique identifier referencing a row in the ca_owned_resource table. It represents the asset to which this request applies.call_req.affected_rc = ca_owned_resource.own_resource_uuid.
cr_support_lev	call_req.support_lev: This is a pointer to a service desc record, which automates some constraints under which this request must be completed.call_req.support_lev = srv_desc.code
cr_category	call_req.category: This is a unique identifier referencing a record in the prob_ctg table,. It represents the category to which this request belongs.call_req.category = prob_ctg.persid
solution	call_req.solution: This is a pointer to call solution to get solution.call_req.solution = crsol.persid

Field	Remarks
cr_impact	call_req.impact: This is an integer unique identifier referencing a row in the impact table. It indicates the scope this request is affecting.call_req.impact = impact.enum
cr_priority	call_req.priority: This is an integer unique identifier referencing a record in the pri table. It indicates how analysts will prioritize the work associated with this request.call_req.priority = pri.enum
urgency	call_req.urgency: This is an integer unique identifier referencing a row in the urgncy table. It documents the user's feeling of urgency for having this request resolved.call_req.urgency = urgncy.enum
severity	call_req.severity: This is an integer unique identifier referencing a row in the severity table. It indicates the severity of the consequences of this unresolved request.call_req.severity = sevrty.enum
extern_ref	This specifies an associated ticket.
last_act_id	This is the id of the last activity.
cr_tticket	This is a pointer to a trouble ticket to get the associated ticket.
cr_parent	call_req.parent: This is a persid pointer to another request persid, which facilitates creation of a hierarchy of change orders.call_req.parent = call_req.persid
cr_template_name	call_req.template_name: This is a text value, which indicates this request is designated for and can be chosen from a list as a template for other similar requests.cr_template.template = call_req.persid
cr_sla_violation	call_req.sla_violation: This is an integer, which counts number of times slas attached to this request have been violated.
cr_predicted_sla_viol	call_req.predicted_sla_viol: (r5.5) Neugent related technology field.
cr_created_via	call_req.created_via: This is an integer pointer to a record in the interface table. It indicates from which interface the change order originated.call_req.created_via = interface.id
cr_call_back_date	call_req.call_back_date: This is a timestamp field (pdmtime), which indicates a future date /time the affected_end_user is to be contacted.
cr_call_back_flag	call_req.call_back_flag: This is a Boolean indicator displayed as a checkbox to the user, indicating whether to notify the analyst at the call_req.call_back_date.
event_token	call_req.event_token: This is used by CA NSM for message matching.
type	call_req.type: This is a text field referencing a record in the crt table. It indicates the ITIL type of this request.call_req.type = crt.code
cr_string1	This is a user-definable string.
cr_string2	This is a user-definable string.
	This is a user-definable string.

Field	Remarks
cr_string3	
cr_string4	This is a user-definable string.
cr_string5	This is a user-definable string.
cr_string6	This is a user-definable string.
change	call_req.change: This is an integer unique identifier, referencing a row in the chg table. It indicates the change order that was created as a result of this request.call_req.change = chg.id.

View_Contact_Full

The following of fields is a basic view of all contacts. This view lists all fields in the ca_contact table, plus referenced fields such as short descriptions for contact type, location name, organization names, and service type for each contact. This view has already been joined with the ca_location, ca_organization, srv_desc, and ca_contact_type tables to get the actual names and symbols for some of the fields in the ca_contact table. The actual names and symbols are located at the end of this view's field list.

Field	Remark
contact_uuid	ca_contact.contact_uuid: A binary-unique identifier for each ca_contact record.
middle_name	ca_contact. middle_name: The middle name of this contact.
alias	ca_contact.alias: The alternate, often informal name for this contact.
last_name	ca_contact.last_name: This contact's surname.
first_name	ca_contact.first_name: This contact's formal first name.
pri_phone_number	ca_contact.pri_phone_number: The contact's primary phone number.
alt_phone_number	ca_contact.alt_phone_number: The contact's alternate phone number.
fax_number	ca_contact.fax_number: The contact's facsimile number.
mobile_phone	ca_contact.mobile_phone: The contact's mobile phone number.
pager_number	ca_contact.pager_number: The number for issuing a page to the contact's page.
	ca_contact.email_address: The contact's email address.

Field	Remark
email_address	
location_uuid	ca_contact.location_uuid: A binary-unique identifier referencing a record in the ca_location table, which indicates the contact's static location.ca_contact.location_uuid = ca_location.location_uuid
floor_location	ca_contact.floor_location: A contact's floor number.
pager_email_address	ca_contact.pager_email_address: A contact's email address for their pager.
room_location	ca_contact.room_location: The contact's specific room on the floor at the static location.
contact_type	ca_contact.contact_type: An unique integer-identifier, referring to a row in the ca_contact_type table, which indicates the general function of this contact within the service desk application.ca_contact.contact_type = ca_contact_type.id
inactive	ca_contact.inactive: A boolean indicator of the state of this record, determining its inclusion or exclusion from standard searches within service desk.
creation_user	ca_contact.creation_user: The userid of the contact who created this record.ca_contact.creation_user = ca_contact.userid
creation_date	ca_contact.creation_date: A timestamp (pdmtime), indicating the date and time this contact was created.
last_update_user	ca_contact.last_update_user: The userid of the contact who last updated this contact record.ca_contact.last_update_user = ca_contact.userid
last_update_date	ca_contact.last_update_date: A timestamp (pdmtime), indicating the date and time this record was last modified.
version_number	ca_contact.version number: The internal version indicator.
department	ca_contact.department: An integer-unique identifier, referencing a row in the ca_resource_department table, that indicates the contact's department.ca_contact.department = ca_resource_department.id
comment	ca_contact.comment: A freeform text comment field for analysts to document important facts that influence the handling of this particular contact.
company_uuid	ca_contact.company_uuid: A binary-unique identifier, which references a row in the ca_company table. It indicates this contact's affiliation with a company.ca_contact.company_uuid = ca_company.company_uuid
organization_uuid	ca_contact.organizaiton_uuid: A binary-unique identifier which references a row in the ca_organization table. It indicates this contact's working organization.ca_contact.organizaiton_uuid = ca_organization.organization_uuid
admin_organization_uuid	ca_contact.admin_organization_uuid: A binary-unique identifier, which references a row in the ca_organization table. It indicates this contact's administrative organization.ca_contact.admin_organization_uuid = ca_organization.organization_uuid

Field	Remark
alternate_identifier	ca_contact.alternate_identifier: A user-defined identifier, usually an entity used by human resources to uniquely identify this contact.
job_title	ca_contact.job_title: An integer-unique identifier, which references the ca_job_title table. It indicates the standardized job title for this contact.ca_contact.job_title = ca_job_title.id
job_function	ca_contact.job_function: An integer-unique identifier, which references the ca_job_function table. It indicates a standardized general description of the contact's job function. ca_contact.job_function = ca_job_function.id
mail_stop	ca_contact.mail_stop: Mail Stop.
cost_center	ca_contact.cost_center: An integer-unique identifier, which references the ca_resource_cost_center table. It indicates this contact's primary cost center.ca_contact. cost_center = ca_cost_center.id
userid	ca_contact.userid: The user identifier this contact will use for logging into service desk.
supervisor_contact_uuid	ca_contact.supervisor_contact_uuid: A binary-unique identifier, referencing a row in the ca_contact table, that creates a hierarchy of contacts to indicate the reporting structure of each contact.ca_contact.supervisor_contact_uuid = ca_contact.contact_uuid
exclude_registration	ca_contact.exclude registration: An internal flag.
delete_time	ca_contact.delete_time: A timestamp indicating when the inactive flag was set to 1.
contact_type_name	ca_contact_type.name: A short description of this contact's ca_contact.contact_type.
location_name	ca_location.name: A short description of this contact's static location.
organization	ca_organization.org_name: A short description of this contact's ca_contact. organizaiton_uuid.
admin_organization	ca_organization.org_name: A short description of this contact's organization name. ca_contact.admin_organization_uuid
service_type	srv_desc.sym: A short description of this contact's usp_contact.c_service_type.ca_contact. contact_uuid = usp_contact.contact_uuid AND usp_contact.c_service_type = srv_desc.code
state_sym	ca_location.state: An integer-unique identifier, referencing a row in the ca_state_provice table, that indicates the State, Province, or other artificially defined geographic region. ca_contact.location_uuid = ca_location.location_uuid AND ca_location.state = ca_state_province.id

View_Contact_to_Environment

The following list of fields is a basic view of contacts and their environment (assets). This view is a view of the contact table (ca_contact), but is also joined with the owned resource table (ca_owned_resource) to get a list of all assets associated with a contact. This view may be joined with the View_Contact_Full view to get the contact type, service type, organizations and location of each contact. Or, this view may be joined with the individual tables to get that same information.

Field	Remarks
ca_contact.*	The ca_contact fields that are defined in the View_Contact_Full view definition.
asset_uuid	ca_owned_resource.own_resource_uuid: A binary-unique identifier for an asset in the ca_owned_resource table.
asset_name	ca_owned_resource.resource_name: The designated network name of this asset.

View_Group

The following list of fields is a basic view of the contact table, but lists only group contacts. Contact type id = 2308, which is for group types. You may want to join this view with other CA SDM tables to get more meaningful data for reporting. For example, you can join it with the Location (ca_location) table to find the name and address for the group's location. You can also join this view with the Organization (ca_organization) table to get the functional and administrative organization names for the group.

Field	Remarks
ca_contact.*	The ca_contact fields that are defined in the View_Contact_Full view definition.

The following example shows how joining tables works, and how reporting fields are extracted. The field from one table (on the right) is joined (->) with a field from another table (on the left). To join properly between tables and views, you need to understand the differences in joins for the database. The field defined in the parentheses, as follows, is what you may want to use in your reports if the previous tables are joined with the View_Group view:

- View_Group.contact_type -> ca_contact_type.id (ca_contact_type.sym)
- View_Group.location_uuid -> ca_location.location_uuid (ca_location.location_name)
- View_Group.organization_uuid -> ca_organization.organization_uuid (ca_organization.org_name)
- View_Group.admin_organization_uuid -> ca_organization(2).organization_uuid (ca_organization (2). org_name)

View_Group_to_Contact

The following list of fields is a basic view of all group contacts (members). It also includes managers. Here, View_Group is joined with the Group_Member table, and then joined with the ca_contact table. All fields in View_Group are listed, as well as the first, middle and last name from the ca_contact table. The Group_Member manager flag is also listed. The group member manager flag is

1 or 0, which means that the member is either (yes - 1) a manager, or (no - 0) not a manager. Most of the information in this view pertains to the group itself, not the actual members. This view is used to find information on a particular group, including the names of its members.

Field	Remarks
View_Group.*	The View_Group fields that are defined in the View_Group definition.
member_lastname	ca_contact.last_name: The surname of the group member.
member_firstname	ca_contact.first_name: The formal first name of the group member.
member_middlename	ca_contact.middle_name: The middle name of the group member.
grpmem_manager_flag	ca_contact.manager_flag: The Group Member Manager (1 or 0) indicator.

View_Issue

The following is a basic view of all issues, listing the status, priority, category, organizations, the requester's full name, the assignee's full name, the group name and ID, and so on. Here, the issue table is joined with many other tables to give some more meaningful data about the issue.

Field	Remarks
id	issue.id: The unique identifier for this record in the issue table.
persid	issue.persid: The unique identifier for this record in the issue table, preceded by the object identifier (iss for table issue) and a colon.
issue_ref_num	issue.iss_ref_num: The Issue reference number, which is used by analysts and customers to refer to a particular issue.
description	issue.description: The long description of an issue as dictated by an analyst or customer.
status	issue.status: The unique identifier of an issue status, which is a pointer to the issstat table.issue.status = issstat.code
active_flag	issue.active_flag: The integer flag used to determine whether this issue is active (1 or 0).
start_date	issue.start_date: The date the first task goes to a pending status (pdmtime).
open_date	issue.open_date: The issue creation date (pdmtime).
last_mod_dt	issue.last_mod_dt: The last modified date (pdmtime).
last_mod_by	issue.last_mod_by: The pointer to the contact uuid, which indicates the last contact to modify this issue.issue.last_mod_by = ca_contact.contact_uuid
close_date	issue.close_date: The date the issue was set to inactive (pdmtime).
resolve_date	issue.resolve_date: The date the issue was set to a status configured to indicate the issue was resolved (pdmtime).
rootcause	issue.rootcause: A pointer to a record in the rootcause table, which represents the original situation that required this issue to be logged.issue.rootcause = rootcause.id
est_total_time	issue.est_total_time: The estimated total time (pdmtime) it will take to complete this issue.
actual_total_time	issue.actual_total_time actual: The total time (pdmtime) it took to complete this issue.

Field	Remarks
log_agent	issue.log_agent: A binary-unique identifier, this references the ca_contact table, which in turn references the person who was the issue's original creator.issue.log_agent = ca_contact.contact_uuid
assignee	issue.assignee: A pointer to the contact uuid who is currently assigned to the change order.issue.assignee = ca_contact.contact_uuid
organization	issue.organization: A pointer to the internal organization uuid, which represents the organization to whom this issue belongs.issue.organization = ca_organization. organization_uuid
group_id	issue.group_id: A pointer to the contact uuid, which represents the group currently assigned to the issue.issue.group_id = ca_contact.contact_uuid
affected_contact	issue.affected_contact: A pointer to the contact uuid, which represents the affected contact for this issue.issue.affected_contact = ca_contact.contact_uuid
requestor	issue.requrestor: A pointer to the contact uuid, which represents the person who asked this issue to be logged.issue.requestor = ca_contact.contact_uuid
category	issue.category: A pointer to the issue category code to reference the category into which this issue falls.issue.category = isscat.code
priority	issue.priority: A pointer to priority enum, which represents the priority into which this issue falls.issue.priority = pri.enum
need_by	issue.need_by: The date, which indicates when the affected_end_user needs to have the issue completed (pdmtime).
est_comp_date	issue.est_comp_date: The estimated completion date (pdmtime) for this Issue.
actual_comp_date	issue.actual_comp_date: The actual completion date (pdmtime) of this issue.
est_cost	issue.est_cost: The estimated cost of this issue.
actual_cost	issue.actual_cost: The actual cost to implement this issue.
justification	issue.justification: A text field, which allows a requester to document the reason(s) this issue is required.
backout_plan	issue.backout_plan: A text field that allows an analyst to document a backout plan for this issue.
impact	issue.impact: A pointer to an impact table record, which indicates the scope of resources that this issue affects.issue.impact = impact.enum
parent	issue.parent: A pointer to another issue id, which allows creation of a hierarchy of issues.issue.parent = issue.id
effort	issue.effort: A text field which explains the plan for implementing this issue.
support_lev	issue.support_lev: A pointer to a service desc record, which automates some constraints under which this issue must be completed.issue.support_lev = srv_desc. code
template_name	issue.template_name: The name of and pointer to an issue template.issue. template_name = iss_template.template_name
sla_violation	issue.sla_violation: The integer to count the number of times slas attached to this issue have been violated.
	issue.predicted_sla_viol: (r5.5) Neugent related technology field.

Field	Remarks
predicted_sla_viol	
macro_predict_viol	issue.macro_predict_viol: (r5.5) Neugent related technology field.
created_via	issue.created_via: A pointer to a record in the interface table. This indicates from which interface the issue originated.issue.created_via = interface.id
call_back_date	issue.call_back_date: A date/time field (pdmtime), which indicates a future date/time the requester is to be contacted.
call_back_flag	issue.call_back_flag: A boolean indicator displayed as a checkbox to the user, to indicate whether to notify the analyst at the issue.call_back_date.
string1	This is a user-definable text field.
string2	This is a user-definable text field.
string3	This is a user-definable text field.
string4	This is a user-definable text field.
string5	This is a user-definable text field.
string6	This is a user-definable text field.
service_date	issue.service_date: The Date/ Time (pdmtime) that an outside vendor is expected to service this issue.
service_num	issue.service_num: The text field to document an outside vendor's service or purchase order number.
product	issue.product: A pointer to a record in the product table, which indicates the product that is affected by this issue.issue.product = product.id
actions	issue.actions: A big text field for documenting actions.
type_of_contact	issue.type_of_contact: A pointer to a record in the toc table, which indicates a general categorization of the affected_end_user's perspective of the issue.issue. type_of_contact = toc.id
reporting_method	issue.reporting_method: A pointer to a record in the repmeth table, which classifies the origination of the issue, and is selected by the person creating the issue.issue. reporting_method = repmeth.id
person_contacting	issue.person_contacting: A pointer to a record in the perscon table, which indicates the role of the affected_end_user or requester.issue.person_contacting = perscon.id
status_name	issstat.sym: The description of the status as seen by a user.issue.status = issstat.code
priority_num	pri.sym: The description of the priority as seen by a user.issue.priority = pri.enum
category_name	isscat.sym: The name of the issue category as viewed by a user.issue.category = isscat. code
organization_name	ca_organization.org_name: The name of an organization as viewed by a user.issue. organization = ca_organization.organization_uuid
affected_end_user_lastname	ca_contact.last_name: The affected End User's last name.issue.affected_end_user = ca_contact.contact_uuid
	ca_contact.first_name: The affected End User's first name.issue.affected_end_user = ca_contact.contact_uuid

Field	Remarks
affected_end_user_firstname	
affected_end_user_middlename	ca_contact.middle_name: The affected End User's middle name.issue.affected_end_user = ca_contact.contact_uuid
assignee_lastname	ca_contact.last_name: The assignee's last name.issue.assignee = ca_contact.contact_uuid
assignee_firstname	ca_contact.first_name: The assignee's first name.issue.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name: The assignee's middle name.issue.assignee = ca_contact.contact_uuid
groupID	View_Group.contact_uuid: A binary representation of the internal id used for the group assigned to this issue.issue.group_id = ca_contact.contact_uuid
group_name	View_Group.last_name: The name of the group assigned to this issue.issue.group = ca_contact.contact_uuid
service_type	srv_desc.sym: The name of the service type applied to this issue.issue.support_lev = srv_desc.code
impact_num	impact.sym: The description of the impact as seen by users.issue.impact = impact.enum
product_sym	product.sym: The product description as seen by users.issue.product = product.id
type_of_contact_sym	toc.sym: The Type Of Contact description as seen by users.issue.type_of_contact = toc.id
rpting_method_sym	repmeth.sym: The Reporting method description as seen by users.issue.reporting_method = repmeth.id
person_contacting_sym	perscon.sym: The Person Contacting description as seen by users.issue.person_contacting = perscon.id
created_via_sym	interface.sym: issue.created_via = interface.id.
rootcause_sym	rootcause.sym: issue.rootcause = rootcause.id.

View_Issue_Act_Log

The following is a basic view of all issue activity logs. This is a view of the issue activity log table (issalg) joined with the activity type table (act_type) and the contact table (ca_contact) to give more meaningful data, such as the actual activity type and full name of the analyst who performed the activity.

Field	Remarks
id	issalg.id: The unique identifier for this record in the issalg table.
persid	issalg.persid: The unique identifier for this record in the issalg table, preceded by the object identifier (issalg for issalg) and a colon.
issue_id	

Field	Remarks
	issalg.issue_id: The pointer to issue id to which this activity belongs.issalg.issue_id = issalg.id
last_mod_dt	issalg.last_mod_dt: The last modify date/time (pdmtime).
time_spent	issalg.time_spent: The duration of time spent on this activity, stored as the total number of seconds. For example, 80 = 1 minute, 20 seconds.
time_stamp	issalg.time_stamp: The user modifiable date/time of activity (pdmtime).
system_time	issalg.system_time: The date/time of record creation (pdmtime).
analyst	issalg.analyst: A binary-unique identifier referring to the contact uuid to get the analyst who performed the activity.issalg.analyst = ca_contact.contact_uuid
description	issalg.description: The text description of this activity, which can be modified by the user.
action_desc	issalg.action_desc: The text description of the automated action, which cannot be modified by the user.
type	issalg.type: The text pointer to a record in the activity type table.issalg.type = act_type.code
internal	issalg.internal: The integer flag (1 or 0), which indicates if this log entry is intended for all to see or just for internal use.
knowledge_session	issalg.knowledge_session: An identifier for a particular session of a particular user.
knowledge_tool	issalg.knowledge_tool: An indicator of the knowledge management tool used for the search, such as NLS_FAQ or EXPERT, and so on.
analyst_lastname	View_Contact_Full.last_name: The Analyst's last name, derived from issalg.analyst = ca_contact.contact_uuid.
analyst_firstname	View_Contact_Full.first_name: The analyst's first name.
analyst_middlename	View_Contact_Full.middle_name: The middle name of the analyst.
activity_type	act_type.sym: The activity type referenced by issalg.type = act_type.code.

View_Issue_to_Assets

The following list of fields is a basic view of issues and their assets. The issue table (issue) is indirectly joined with the owned resource table (ca_owned_resource), and other asset-related tables, to get a list of each issue's assets. This may not list all issues, particularly those that have no assets.

Field	Remarks
View_Issue.*	The View_Issue view which defines all fields listed in the View_Issue view.
assetID	

Field	Remarks
	ca_owned_resource.own_resource_uuid: The binary field which serves as the internal, unchanging unique identifier for an asset record.
asset_serial_num	ca_owned_resource.serial_number: The serial number for an asset record.
asset_class	ca_resource_class.name: A short description of the class to which an asset belongs. ca_owned_resource.resource_class = ca_resource_class.id
asset_family	ca_resource_family.name: The family of assets to which this asset belongs. ca_owned_resource.resource_class = ca_resource_class.id AND ca_resource_class.family_id = ca_resource_family.id
asset_name	ca_owned_resource.resource_name: The network name by which this asset is known.

View_Issue_to_Issue_Act_Log

The following is a basic view of all issues and the activity logs that go with them. This view joins the View_Issue view with the View_Issue_Act_Log view to give detailed information about issues and their activity logs. Actual data is at the end of the fields list.

Field	Remarks
View_Issue.*	Please refer to the View_Issue view defined earlier in this document.
issalg_id	issalg.id: The unique identifier for this record in the issalg table.
issalg_persid	issalg.persid: The unique identifier for this record in the issalg table, preceded by the object identifier (issalg for issalg) and a colon.
issue_id	issalg.issue_id: The pointer to issue id to which this activity belongs.issalg.issue_id = issalg.id
issalg_last_mod_dt	issalg.last_mod_dt: The last modify date/time (pdmtime).
time_spent	issalg.time_spent: The duration of time spent on this activity, stored as the total number of seconds. For example, 80 = 1 minute, 20 seconds.
time_stamp	issalg.time_stamp: The user modifiable date/time of activity (pdmtime).
system_time	issalg.system_time: The date/time of record creation (pdmtime).
analyst	issalg.analyst: The unique binary pointer to the contact uuid to get the analyst who performed the activity.issalg.analyst = ca_contact.contact_uuid
issalg_description	issalg.description: The text description of this activity, which can be modified by the user.
action_desc	issalg.action_desc: The text description of the automated action, which cannot be modified by the user.
type	issalg.type: The text pointer to a record in the activity type table.issalg.type = act_type.code
internal	

Field	Remarks
	issalg.internal: The integer flag (1 or 0), which indicates if this log entry is intended for all to see or just for internal use.
knowledge_session	issalg.knowledge_session: An identifier for a particular session of a particular user.
knowledge_tool	issalg.knowledge_tool: An indicator of the knowledge management tool used for the search, such as NLS_FAQ or EXPERT, and so on.
issalg_analyst_id	issalg.analyst: The unique binary pointer to the contact uuid to get the analyst who performed the activity.issalg.analyst = ca_contact.contact_uuid

View_Issue_to_Issue_WF

This view is a result of the View_Issue view joined with the workflow task table (isswf) to give a basic view of issues and their workflow tasks. This may not list all issues, particularly if there are no workflow tasks assigned to them.

Field	Remarks
View_Issue.*	Please refer to the View_Issue definition earlier in this document for a description of each field.
wf_id	isswf.id: This is a unique identifier for a record in the isswf table.
wf_persid	isswf.persid: This is a unique identifier for this record in the isswf table, preceded by the object identifier (isswf) and a colon.
del	isswf.del: This is a boolean indicator of whether this record is to be displayed to the user.
object_type	isswf.object_type: This is the factory name, which is used to identify the type of record (for example, iss) to which this workflow task is attached.
object_id	isswf.object_id: This is a unique identifier used to identify the specific record to which this workflow task is attached.isswf.object_id = issue.id
task	isswf.task: This is an identifier, which references the type of task this record represents.isswf.task = tskty.code
wf_template	isswf.wf_template: This is an identifier, which references from which template this workflow task record was created.isswf.wf_template = wftpl.id
sequence	isswf.sequence: This is an integer that indicates the order for which this particular workflow task record should be displayed and executed by CA SDM (for example, Ascending).
wf_status	isswf.status: This is an identifier, which references a tskstat record. It indicates the current status of this workflow task.isswf.status = tskstat.code
group_task	isswf.group_task: This is a boolean, which indicates whether this task belongs to a group.
asset	isswf.asset: This is a unique binary identifier, which references a record in the ca_owned_resource table.isswf.asset = ca_owned_resource.own_resource_uuid
creator	isswf.creator: This is a unique binary identifier, which references a record in the ca_contact table. It indicates the person who created this workflow task.isswf.creator = ca_contact.contact_uuid
date_created	isswf.date_created: This is the date/timestamp that this workflow task was created (pdmtime).

Field	Remarks
wf_assignee	isswf.assignee: This is a unique binary identifier, which references a record in the ca_contact table. It indicates the person who is currently assigned to this workflow task.isswf.assignee = ca_contact.contact_uuid
done_by	isswf.done_by: This is a unique binary identifier, which references a record in the ca_contact table. It indicates the person who completed or approved this workflow task.isswf.done_by = ca_contact.contact_uuid
wf_start_date	wf_start_date: This is the timestamp when the workflow task moved into an active status (pdmtime).
wf_est_comp_date	isswf.est_comp_date: This is a timestamp (pdmtime) indicating when users believe this task will be completed.
est_duration	isswf.est_duration: This is the estimated duration for this workflow task.
completion_date	isswf.completion_date: This is a timestamp (pdmtime) indicating when this workflow task was completed.
actual_duration	isswf.actual_duration: This is the actual amount of time it took to complete this workflow task.
wf_est_cost	isswf.est_cost: This is the estimated cost of this workflow task
cost	isswf.cost: This is the actual cost required to complete this workflow task.
wf_description	isswf.description: This is a description of the workflow task.
wf_last_mod_dt	isswf.last_mod_dt: This is the timestamp (pdmtime) indicating when this workflow task was last changed.
wf_last_mod_by	isswf.last_mod_by: This is the unique binary identifier, which references a record in the contact table. It indicates the last person to make changes to this workflow task.isswf. last_mod_by = ca_contact.contact_uuid

View_Issue_to_Properties

This view is a result of the View_Issue view joined with the issue properties table (issprp) to give a basic view of issues and their assigned properties. This may not list all issues, particularly if there are no properties assigned to them.

Field	Remarks
View_Issue.*	Please refer to the View_Issue definition earlier in this document, for a description of each field.
prp_id	issprp.id: This is an integer-unique identifier for the property record.
prp_persid	issprp.persid: This is a unique identifier for this record in the prp table, preceded by the object identifier (prp) and a colon.

Field	Remarks
sequence	issprp.sequence: This is an integer that indicates the order for which this particular property record should be displayed by CA SDM (for example, Ascending).
label	issprp.label: This is a short description of what should be placed in the issprp.value field.
value	issprp.value: This is a value entered by the user in response to the prp_description and issprp.label fields.
prp_last_mod_dt	issprp.last_mod_dt: This is the timestamp (pdmtime) indicating when this property was last modified.
prp_last_mod_by	issprp.last_mod_by: This is a binary identifier, which references a record in the ca_contact table. It represents the person who last modified this record.issprp.last_mod_by = ca_contact.contact_uuid
required	issprp.required: This is a boolean, indicating whether this property must have a issprp.value before the record is saved.
sample	issprp.sample: This is a text field, which displays example values to guide the user in entering the most useful value in issprp.value.
owning_iss	issprp.owning_iss: This is a unique identifier used to identify the specific record to which this property is attached.issprp.object_id = issue.persid
prp_description	issprp.description: This is a text field, which explains the type of value that should be entered in issprp.value.

View_Request

The following is a basic view of all requests. Here, the Request table has been joined with other CA SDM tables to give you more specific information, such as the request service type, severity, urgency, category, and priority. There is some additional information about the request listed, as well. All fields from the Request (call_req) table are selected. The extracted fields that are a result of the joined tables are listed at the end of this fields list.

Field	Remarks
id	call_req.id: This is the unique identifier for this record in the call_req table.
persid	call_req.persid: This is a unique identifier for this record in the call_req table, preceded by the object identifier (cr for table call_req) and a colon.
ref_num	call_req.ref_num: This is a Request reference number, which is used by analysts and customers to refer to a particular Request.
summary	call_req.summary: This is a brief description of the request for quick reference.
description	call_req.description: This is the long description of a request, as dictated by an analyst or customer.
status	call_req.status: This is a unique identifier referencing a record in the cr_stat table. It indicates the status of this request. call_req.status = cr_stat.code
active_flag	call_req.active_flag: This is an integer flag to determine whether this request record is active (1 or 0).
	call_req.open_date: This is the Request creation timestamp (pdmtime).

Field	Remarks
open_date	
time_spent_sum	call_req.time_spent_sum: This is the derived total of all of the act_log records' time_spent fields, stored in seconds (i.e. 80 = 1 minute 20 seconds).
last_mod_dt	call_req.last_mod_dt: This is the last modified timestamp (pdmtime).
close_date	call_req.close_date: This is the timstamp when the request was set to inactive (pdmtime).
resolve_date	This is the date for when the request was resolved (pdmtime).
rootcause	This is a pointer to the rootcause.id.
log_agent	call_req.log_agent: This is a binary-unique identifier, referencing the ca_contact table. It references the person who was the request's original creator.call_req.log_agent = ca_contact.contact_uuid
assignee	call_req.assignee: This is a binary-unique identifier, referencing a record in the ca_contact table. It represents the person currently assigned to the request.call_req.assignee = ca_contact.contact_uuid
group_id	call_req.group_id: This is a binary-unique identifier, referencing a record in the ca_contact table. It represents the group currently assigned to the request.call_req. group_id = ca_contact.contact_uuid
customer	call_req.customer: This is a binary-unique identifier, referencing a record in the ca_contact table. It represents the affected end user for this request.call_req.customer = ca_contact.contact_uuid
charge_back_id	charge_back_id: This is a text field available for use as an indicator of accounting jargon for expensing this request to the appropriate cost center.
affected_rc	call_req.affected_rc: This is a binary-unique identifier, referencing a row in the ca_owned_resource table. It represents the asset to which this request applies.call_req. affected_rc = ca_owned_resource.own_resource_uuid.
support_lev	call_req.support_lev: This is a pointer to a service desc record, which automates some constraints under which this request must be completed.call_req.support_lev = srv_desc. code.
category	call_req.category: This is a unique identifier, referencing a record in the prob_ctg table. It represents the category to which this request belongs.call_req.category = prob_ctg.persid
solution	call_req.solution: This is a pointer to call solution to get solution.call_req.solution = crsol. persid
impact	call_req.impact: This is an integer-unique identifier, referencing a row in the impact table. It indicates the impact scope of the request.call_req.impact = impact.enum
priority	call_req.priority: This is an integer-unique identifier, referencing a record in the pri table. It indicates how analysts will prioritize the work associated with this request.call_req. priority = pri.enum
urgency	call_req.urgency: This is an integer-unique identifier, referencing a row in the urgency table. It indicates the user's feeling of urgency for having this request resolved.call_req. urgency = urgncy.enum
severity	

Field	Remarks
	call_req.severity: This is an integer-unique identifier, referencing a row in the severity table. It indicates the severity of the consequences of this unresolved request.call_req. severity = sevrty.enum
extern_ref	This is an external reference to an associated ticket.
last_act_id	This identifies the id of the last activity.
cr_tticket	This is a pointer to the trouble ticket to get the associated ticket.
parent	call_req.parent: This is a ersid pointer to another request persid, which facilitates creation of a hierarchy of change orders.call_req.parent = call_req.persid
template_name	call_req.template_name: This is a text value, which indicates this request is designated for and can be chosen from a list as a template for other similar requests.cr_template. template = call_req.persid
sla_violation	call_req.sla_violation: This is an integer, which counts the number of times that slas attached to this request have been violated.
predicted_sla_viol	This specifies that a request has been predicted by neugents to likely violate SLA.
macro_predicted_violation	This indicates that the request has been predicted by neugents to likely violate SLA.
created_via	call_req.created_via: This is an integer pointer to a record in the interface table that indicates from which interface the change order originated.call_req.created_via = interface.id
call_back_date	call_req.call_back_date: This is a timestamp field (pdmtime), which indicates a future date /time that the affected_end_user is to be contacted.
call_back_flag	call_req.call_back_flag: This is a boolean indicator, displayed as a checkbox to the user, indicating whether to notify the analyst at the call_req.call_back_date.
event_token	call_req.event_token: This is used by CA NSM for message matching.
sched_token	call_req.sched_token: This is used by CA NSM for message matching.
type	call_req.type: This is a text field referencing a record in the crt table. It indicates the ITIL type for this request.call_req.type = crt.code
string1	This is a user-definable string.
string2	This is a user-definable string.
string3	This is a user-definable string.
string4	This is a user-definable string.
string5	This is a user-definable string.
string6	This is a user-definable string.
problem	This is an ITIL problem.
incident_priority	This is an ITIL incident priority.
change	

Field	Remarks
	call_req.change: This is an integer-unique identifier, referencing a row in the chg table. It indicates the change order that was created as a result of this request.call_req.change = chg.id.
service_type	srv_desc.sym: This indicates the actual Service Type.call_req.support_lev = srv_desc.code
severity_num	sevrty.sym: This is the actual Severity number.call_req.severity = sevrty.enum
urgency_num	urgncy.sym: This indicates the actual Urgency number.call_req.urgency = urgncy.enum
category_name	prob_ctg.sym: This is the actual Request Area (problem category).call_req.category = prob_ctg.id
asset	ca_owned_resource.resource_name: This is the actual Asset name.call_req.affected_rc = ca_owned_resource.own_resource_uuid
impact_num	impact.sym: This is the actual Impact number.call_req.impact = impact.enum
assignee_lastname	ca_contact.last_name: This is the actual Assignee last name.call_req.assignee = ca_contact.contact_uuid
assignee_firstname	ca_contact.first_name: This is the actual Assignee first name.call_req.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name: This is the actual Assignee middle name.call_req.assignee = ca_contact.contact_uuid
customer_lastname	ca_contact.last_name: This is the actual last name of the Affected End User.call_req. customer = ca_contact.contact_uuid
customer_firstname	ca_contact.first_name: This is the actual first name of the Affected End User.call_req. customer.ca_contact.contact_uuid
customer_middlename	ca_contact.middle_name: This is the actual middle name of the Affected End User. call_req.customer = ca_contact.contact_uuid
group_name	View_Group.last_name: This is the actual Group name.
GroupID	View_Group.contact_uuid: This is the actual Group key ID.
status_name	cr_stat.sym: This is the actual status.
priority_num	pri.sym: This is the actual Priority number.

View_Request_to_Act_Log

The following is a basic view of all requests with their activity logs. The View_Request view is joined with the View_Act_Log view to give more detailed information about each activity per request.

Field	Remarks
View_Request.*	Please refer to the field defined in the View_Request section earlier in this document.
View_Act_Log.*	Please refer to the fields defined in the View_Act_Log section earlier in this document.

View_Request_to_Properties

The following is a basic view of call requests and their properties. This view lists everything from the call request (call_req) table and the request property (cr_prp) table.

Field	Remarks
View_Request.*	Please refer to the fields defined in the View_Request section of this document.
crprp_id	cr_prp.id: This is an integer-unique identifier for the property record.
crprp_persid	cr_prp.persid: This is a unique identifier for this record in the cr_prp table, preceded by the object identifier (cr_prp) and a colon.
sequence	cr_prp.sequence: This is an integer that indicates the order for which this particular property record should be displayed by CA SDM (for example, Ascending).
label	cr_prp.label: This is a short description of what should be placed in the cr_prp.value field.
value	cr_prp.value: This is a value entered by the user in response to the prp_description and cr_prp.label fields.
crprp_last_mod_dt	cr_prp.last_mod_dt: This is the timestamp (pdmtime) identifying when this property was last modified.
crprp_last_mod_by	cr_prp.last_mod_by: This is a binary identifier, which references a record in the ca_contact table. It represents the person who last modified this record.cr_prp.last_mod_by = ca_contact.contact_uuid
required	cr_prp.required: This is the boolean, indicating whether this property must have a cr_prp. value before the record is saved.
sample	cr_prp.sample: This is a text field, which displays example values to guide the user in entering the most useful value in cr_prp.value.
owning_cr	cr_prp.owning_cr: This is the unique identifier used to identify the specific record to which this property is attached.cr_prp.object_id = call_req.persid
crprp_description	cr_prp.description: This is a text field, which explains the type of value that should be entered in cr_prp.value.

View_Request_to_Request_WF

Note: This feature will only be available if you apply a patch for CA Service Management Release 14.1.01. Find the patch and the download details from CA Support Online.

This view is a result of the View_Request view joined with the workflow task table (crwf) to give a basic view of requests and their workflow tasks. This may not list all requests, particularly if there are no workflow tasks assigned to them.

Field	Remarks
View_Request.*	Please refer to the View_Request definition earlier in this document for a description of each field.
wf_id	crwf.id: This is a unique identifier for a record in the crwf table.
wf_persid	crwf.persid: This is a unique identifier for this record in the crwf table, preceded by the object identifier (crwf) and a colon.
del	crwf.del: This is a boolean indicator of whether this record is to be displayed to the user.
object_type	crwf.object_type: This is the factory name, which is used to identify the type of record (for example, cr) to which this workflow task is attached.
object_id	crwf.object_id: This is a unique identifier used to identify the specific record to which this workflow task is attached.cr.object_id = issue.id
task	crwf.task: This is an identifier, which references the type of task this record represents.crwf.task = tskty.code
wf_template	crwf.wf_template: This is an identifier, which references from which template this workflow task record was created.crwf.wf_template = wftpl.id
sequence	crwf.sequence: This is an integer that indicates the order for which this particular workflow task record should be displayed and executed by CA SDM (for example, Ascending).
wf_status	crwf.status: This is an identifier, which references a tskstat record. It indicates the current status of this workflow task.crwf.status = tskstat.code
group_task	crwf.group_task: This is a boolean, which indicates whether this task belongs to a group.
creator	crwf.creator: This is a unique binary identifier, which references a record in the ca_contact table. It indicates the person who created this workflow task.crwf.creator = ca_contact.contact_uuid
date_created	crwf.date_created: This is the date/timestamp that this workflow task was created (pdmtime).
wf_assignee	crwf.assignee: This is a unique binary identifier, which references a record in the ca_contact table. It indicates the person who is currently assigned to this workflow task.crwf.assignee = ca_contact.contact_uuid
done_by	isswf.done_by: This is a unique binary identifier, which references a record in the ca_contact table. It indicates the person who completed or approved this workflow task.isswf.done_by = ca_contact.contact_uuid
wf_start_date	wf_start_date: This is the timestamp when the workflow task moved into an active status (pdmtime).
wf_est_comp_date	crwf.est_comp_date: This is a timestamp (pdmtime) indicating when users believe this task will be completed.
est_duration	crwf.est_duration: This is the estimated duration for this workflow task.

Field	Remarks
completion_date	crwf.completion_date: This is a timestamp (pdmtime) indicating when this workflow task was completed.
actual_duration	crwf.actual_duration: This is the actual amount of time it took to complete this workflow task.
wf_est_cost	crwf.est_cost: This is the estimated cost of this workflow task
cost	crwf.cost: This is the actual cost required to complete this workflow task.
wf_description	crwf.description: This is a description of the workflow task.
wf_last_mod_dt	crwf.last_mod_dt: This is the timestamp (pdmtime) indicating when this workflow task was last changed.
wf_last_mod_by	crwf.last_mod_by: This is the unique binary identifier, which references a record in the contact table. It indicates the last person to make changes to this workflow task.crwf. last_mod_by = ca_contact.contact_uuid

View_Request_to_Request_WF

RFC 2251 LDAP Result Codes

This article contains the following topics:

LDAP Return Codes

LDAP has a set of operation result codes that may be generated by the LDAP server in response to various LDAP requests. These codes indicate the status of the protocol operation and are categorized by server or client return code categories.

LDAP Server Return Codes

The following table lists the server return codes:

Hex	Decimal	Description
0x00	0	LDAP_SUCCESS Indicates the requested client operation completed successfully.
0x01	1	

Hex	Decimal	Description
		LDAP_OPERATIONS_ERROR Indicates an internal error occurred. The server is unable to respond with a more specific error and is also unable to properly respond to a request. It does not indicate that the client has sent an erroneous message.
0x02	2	LDAP_PROTOCOL_ERROR Indicates that the server has received an invalid or malformed request from the client.
0x03	3	LDAP_TIMELIMIT_EXCEEDED Indicates that the operation's time limit specified by either the client or the server has been exceeded. On search operations, incomplete results are returned.
0x04	4	LDAP_SIZELIMIT_EXCEEDED Indicates that in a search operation, the size limit specified by the client or the server has been exceeded. Incomplete results are returned.
0x05	5	LDAP_COMPARE_FALSE Does not indicate an error condition. Indicates that the results of a compare operation are false.
0x06	6	LDAP_COMPARE_TRUE Does not indicate an error condition. Indicates that the results of a compare operation are true.
0x07	7	LDAP_AUTH_METHOD_NOT_SUPPORTED Indicates that during a bind operation the client requested an authentication method not supported by the LDAP server.
0x08	8	LDAP_STRONG_AUTH_REQUIRED Indicates one of the following: In bind requests, the LDAP server accepts only strong authentication. In a client request, the client requested an operation, such as delete, that requires strong authentication. In an unsolicited notice of disconnection, the LDAP server discovers the security protecting the communication between the client and server has unexpectedly failed or been compromised.
0x09	9	Reserved.
0x0A	10	LDAP_REFERRAL Does not indicate an error condition. In LDAPv3, indicates that the server does not hold the target entry of the request, but that the servers in the referral field may.
0x0B	11	LDAP_ADMINLIMIT_EXCEEDED Indicates that an LDAP server limit set by an administrative authority has been exceeded.
0x0C	12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION Indicates that the LDAP server was unable to satisfy a request because one or more critical extensions were not available. Either the server does not support the control or the control is not appropriate for the operation type.
0x0D	13	LDAP_CONFIDENTIALITY_REQUIRED Indicates that the session is not protected by a protocol, such as Transport Layer Security (TLS), which provides session confidentiality.
0x0E	14	

Hex	Decimal	Description
		LDAP_SASL_BIND_IN_PROGRESS Does not indicate an error condition, but indicates that the server is ready for the next step in the process. The client must send the server the same SASL mechanism to continue the process.
0x0 F	15	Not used.
0x1 0	16	LDAP_NO_SUCH_ATTRIBUTE Indicates that the attribute specified in the modify or compare operation does not exist in the entry.
0x1 1	17	LDAP_UNDEFINED_TYPE Indicates that the attribute specified in the modify or add operation does not exist in the LDAP server's schema.
0x1 2	18	LDAP_INAPPROPRIATE_MATCHING Indicates that the matching rule specified in the search filter does not match a rule defined for the attribute's syntax.
0x1 3	19	LDAP_CONSTRAINT_VIOLATION Indicates that the attribute value specified in a modify, add, or modify DN operation violates constraints placed on the attribute. The constraint can be one of size or content (string only, no binary).
0x1 4	20	LDAP_TYPE_OR_VALUE_EXISTS Indicates that the attribute value specified in a modify or add operation already exists as a value for that attribute.
0x1 5	21	LDAP_INVALID_SYNTAX Indicates that the attribute value specified in an add, compare, or modify operation is an unrecognized or invalid syntax for the attribute.
	22-31	Not used.
0x2 0	32	LDAP_NO_SUCH_OBJECT Indicates that the target object cannot be found. This code is not returned on the following operations: Search operations that find the search base but cannot find any entries that match the search filter. Bind operations
0x2 1	33	LDAP_ALIAS_PROBLEM Indicates that an error occurred when an alias was dereferenced.
0x2 2	34	LDAP_INVALID_DN_SYNTAX Indicates that the syntax of the DN is incorrect. However, if the DN syntax is correct, but the LDAP server's structure rules do not permit the operation, the server returns the following: LDAP_UNWILLING_TO_PERFORM
0x2 3	35	LDAP_IS_LEAF Indicates that the specified operation cannot be performed on a leaf entry. (This code is not currently in the LDAP specifications, but is reserved for this constant.)
0x2 4	36	LDAP_ALIAS_DEREF_PROBLEM Indicates that during a search operation, either the client does not have access rights to read the aliased object's name or dereferencing is not allowed.
	37-47	Not used.

Hex	Decimal	Description
0x30	48	LDAP_INAPPROPRIATE_AUTH Indicates that during a bind operation, the client is attempting to use an authentication method that the client cannot use correctly. For example, either of the following causes this error: The client returns simple credentials when strong credentials are required. The client returns a DN and a password for a simple bind when the entry does not have a password defined.
0x31	49	LDAP_INVALID_CREDENTIALS Indicates that during a bind operation, one of the following occurred: The client passed either an incorrect DN or password. The password is incorrect because it has expired; intruder detection has locked the account, or some other similar reason.
0x32	50	LDAP_INSUFFICIENT_ACCESS Indicates that the caller does not have sufficient rights to perform the requested operation.
0x33	51	LDAP_BUSY Indicates that the LDAP server is too busy to process the client request at this time, but if the client waits and resubmits the request, the server may be able to process it then.
0x34	52	LDAP_UNAVAILABLE Indicates that the LDAP server cannot process the client's bind request, usually because it is shutting down.
0x35	53	LDAP_UNWILLING_TO_PERFORM Indicates that the LDAP server cannot process the request because of server-defined restrictions. This error is returned for the following reasons: The add entry request violates the server's structure rules. The modify attribute request specifies attributes that users cannot modify. Password restrictions prevent the action. Connection restrictions prevent the action.
0x36	54	LDAP_LOOP_DETECT Indicates that the client discovered an alias or referral loop, and is thus unable to complete this request.
	55-63	Not used.
0x40	64	LDAP_NAMING_VIOLATION Indicates that the add or modify DN operation violates the schema's structure rules. For example: The request places the entry subordinate to an alias. The request places the entry subordinate to a container that is forbidden by the containment rules. The RDN for the entry uses a forbidden attribute type.
0x41	65	LDAP_OBJECT_CLASS_VIOLATION Indicates that the add, modify, or modify DN operation violates the object class rules for the entry. For example, the following types of request return this error: The add or modify operation tries to add an entry without a value for a required attribute. The add or modify operation tries to add an entry with a value for an attribute which the class definition does not contain. The modify operation tries to remove a required attribute without removing the auxiliary class that defines the attribute, as required.

Hex	Decimal	Description
0x42	66	LDAP_NOT_ALLOWED_ON_NONLEAF Indicates that the requested operation is permitted only on leaf entries. For example, the following types of requests return this error: The client requests a delete operation on a parent entry. The client request a modify DN operation on a parent entry.
0x43	67	LDAP_NOT_ALLOWED_ON_RDN Indicates that the modify operation attempted to remove an attribute value that forms the entry's relative distinguished name.
0x44	68	LDAP_ALREADY_EXISTS Indicates that the add operation attempted to add an entry that already exists, or that the modify operation attempted to rename an entry with the name of an entry that already exists.
0x45	69	LDAP_NO_OBJECT_CLASS_MODS Indicates that the modify operation attempted to modify the structure rules of an object class.
0x46	70	LDAP_RESULTS_TOO_LARGE Reserved for CLDAP.
0x47	71	LDAP_AFFECTS_MULTIPLE_DSAS Indicates that the modify DN operation moves the entry from one LDAP server to another and thus requires more than one LDAP server.
	72-79	Not used.
0x50	80	LDAP_OTHER Indicates an unknown error condition. This is the default value for NDS error codes which do not map to other LDAP error codes.

LDAP Client Return Codes

The following table lists the client return codes:

Hex	Decimal	Description
0x51	81	LDAP_SERVER_DOWN Indicates that the LDAP libraries cannot establish an initial connection with the LDAP server. Either the LDAP server is down, or the specified host name or port number is incorrect.
0x52	82	LDAP_LOCAL_ERROR Indicates that the LDAP client has an error. This is usually a failed dynamic memory allocation error.
0x53	83	LDAP_ENCODING_ERROR Indicates that the LDAP client encountered errors when encoding an LDAP request intended for the LDAP server.
0x54	84	LDAP_DECODING_ERROR Indicates that the LDAP client encountered errors when decoding an LDAP response from the LDAP server.
0x55	85	LDAP_TIMEOUT Indicates that the time limit of the LDAP client was exceeded while waiting for a result.

Hex	Decimal	Description
0x56	86	LDAP_AUTH_UNKNOWN Indicates that the ldap_bind or ldap_bind_s function was called with an unknown authentication method.
0x57	87	LDAP_FILTER_ERROR Indicates that the ldap_search function was called with an invalid search filter.
0x58	88	LDAP_USER_CANCELLED Indicates that the user cancelled the LDAP operation.
0x59	89	LDAP_PARAM_ERROR Indicates that an LDAP function was called with an invalid parameter value (for example, the ID parameter is NULL).
0x5A	90	LDAP_NO_MEMORY: Indicates that a dynamic memory allocation function failed when calling an LDAP function.
0B	91	LDAP_CONNECT_ERROR Indicates that the LDAP client has lost either its connection or cannot establish a connection to the LDAP server.
0x5C	92	LDAP_NOT_SUPPORTED Indicates that the client does not support the requested functionality. For example, if the LDAP client is established as an LDAPv2 client, the libraries set this error code when the client requests LDAPv3 functionality.
0x5D	93	LDAP_CONTROL_NOT_FOUND Indicates that the client requested a control that the libraries cannot find in the list of supported controls sent by the LDAP server.
0x5E	94	LDAP_NO_RESULTS_RETURNED Indicates that the LDAP server sent no results. When the ldap_parse_result function is called, no result code is included in the server's response.
0x5F	95	LDAP_MORE_RESULTS_TO_RETURN Indicates that more results are chained in the result message. The libraries set this code when the call to the ldap_parse_result function reveals that additional result codes are available.
0x60	96	LDAP_CLIENT_LOOP Indicates the LDAP libraries detected a loop. Usually, this happens when following referrals.
0x61	97	LDAP_REFERRAL_LIMIT_EXCEEDED Indicates that the referral exceeds the hop limit. The hop limit determines how many servers the client can hop through to retrieve data. For example, suppose the following conditions: The hop limit is two. The referral is to server D which can be contacted only through server B (1 hop) which contacts server C (2 hops) which contacts server D (3 hops) With these conditions, the hop limit is exceeded and the LDAP libraries set this code.

LDAP-Associated RFC Standards

The following table describes the LDAP-associated RFC standards available for your use:

RFC	Description
1274	The COSINE and Internet X.500 Schema
1275	Replication Requirements to provide an Internet Directory using X.500
1276	Replication and Distributed Operations extensions to provide an Internet Directory using X.500
1308	Executive Introduction to Directory Services Using the X.500 Protocol
1309	Technical Overview of Directory Services Using the X.500 Protocol
1430	A Strategic Plan for Deploying an Internet X.500 Directory Service
1488	The X.500 String Representation of Standard Attribute Syntaxes
1558	A String Representation of LDAP Search Filters
1617	Naming and Structuring Guidelines for X.500 Directory Pilots
1777	Lightweight Directory Access Protocol v2
1778	The String Representation of Standard Attribute Syntaxes
1779	A String Representation of Distinguished Names
1804	Schema Publishing in X.500 Directory
1823	The LDAP Application Program Interface
1959	An LDAP URL Format
1960	A String Representation of LDAP Search Filters
2044	UTF -8, a transformation format of Unicode and ISO 10646
2164	Use of an X.500/LDAP Directory to support MIXER address mapping
2218	A Common Schema for the Internet White Pages Service
2247	Using Domains in LDAP/X.500 Distinguished Names
2251	Lightweight Directory Access Protocol (v3)
2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
2253	Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names
2254	The String Representation of LDAP Search Filters
2255	The LDAP URL Format
2256	A Summary of the X.500(96) User Schema for use with LDAPv3
2279	UTF-8, a transformation format of ISO 10646
2293	Representing Tables and Subtrees in the X.500 Directory
2294	Representing the O/R Address hierarchy in the X.500 Directory Information Tree
2307	An Approach for Using LDAP as a Network Information Service
2377	Naming Plan for Internet Directory-Enabled Applications
2531	Content Feature Schema for Internet Fax
2559	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2
2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema
2589	Lightweight Directory Access Protocol (v3): Extensions for Dynamic Directory Services
2596	Use of Language Codes in LDAP

RFC	Description
2649	An LDAP Control and Schema for Holding Operation Signatures
2657	RFC 2657 - LDAPv2 Client vs. the Index Mesh
2696	LDAP Control Extension for Simple Paged Results Manipulation
2713	Schema for Representing Java(tm) Objects in an LDAP Directory
2714	Schema for Representing CORBA Object References in an LDAP Directory
2739	Calendar Attributes for vCard and LDAP
2798	Definition of the inetOrgPerson LDAP Object Class
2820	Access Control Requirements for LDAP
2829	Authentication Methods for LDAP
2830	Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security
2849	The LDAP Data Interchange Format (LDIF) - Technical Specification
2879	Content Feature Schema for Internet Fax (V2)
2891	LDAP Control Extension for Server Side Sorting of Search Results
3045	Storing Vendor Information in the LDAP root DSE
3062	LDAP Password Modify Extended Operation
3112	LDAP Authentication Password Schema
3296	Named Subordinate References in Lightweight Directory Access Protocol Directories
3377	Lightweight Directory Access Protocol (v3): Technical Specification
3384	Lightweight Directory Access Protocol (version 3) Replication Requirements

pdm_configure--Open the Configuration Window

pdm_configure opens a window containing the CA SDM configuration window. Use this window to set the CA SDM configuration after installing CA SDM, or to change the CA SDM configuration after CA SDM is running. Following are the possible reasons to change the CA SDM configuration:

- Changing the database type or server
- Reload default data
- Change passwords for the CA SDM system accounts
- Rebuild schema files to incorporate changes
- Reconfigure the following server, depending on your CA SDM configuration:
  - Conventional: Primary or secondary server
  - Advanced availability: Application or background server

Syntax

This command has the following format:

```
pdm_configure
```

Restrictions

pdm_configure can be run on any CA SDM server or a CA SDM Linux client. You must be the privileged user or root to run pdm_configure.

pdm_key_refresh--Refresh Cached Key Information

The pdm_key_refresh utility refreshes cached key information from the key control table in the database. If key control information is updated, this utility can be executed instead of stopping and restarting the system to force CA SDM to use the new keyid base value.

Important! Changing the key control table may cause data corruption. You should not attempt to change the key control without specific instructions from CA Technical Support.

Syntax

This command has the following format:

```
pdm_key_refresh
```

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

pdm_lexutil--Modify CA SDM Lexicons

The pdm_lexutil utility allows you to modify Service Desk lexicons, to add or delete words for the spell check dictionary.

Syntax

This command has the following format:

```
pdm_lexutil -a | -d [-f] [-l] wordlist
```

- **-a**
  Add words.
- **-d**
  Delete words.

- **-f**
  File or lexicon containing list of words to be added or deleted.

- **-l**
  Lexicon name.
  Default: userdict.tlx

- **wordlist**
  Words to be added or deleted.

> **Important!** On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

pdm_listconn--List Active Connections

The pdm_listconn utility can be used to list active connections for both clients and servers.

Syntax

This command has the following format:

```
pdm_listconn [-c] [-s] [ - s -c] [ - t nn] [proc1 [proc2...]]
```

The default command has the following format if no parameters are specified:

```
pdm_listconn -s -t 2
```

-c

Lists connections by client. The utility displays two lines for each client:

```
(n secs) client_type node|cproc
connected to alias (sproc) at time
```

n is the number of seconds it took for the client to respond.

client_type is "vbop," "animator daemon," or "web engine."

node is the IP address of the client's node.

cproc is the client's slump procname.

alias is the alias of the server the client is connected with.

sproc is the server's slump procname.

time is the connection time.

For example:

```
(0 secs) vbop client 141.202.211.34|vbop-0x40120000:anthill:0
         connected to CMD40120 on anthill (domsrvr) at 02/19/1999 10:44:16
```

-s

Lists connections by server (default). The utility displays two lines for each server:

```
(n secs) server  alias (node|sproc) willingness willingness
count connected clients (use pdm_listconn -c -s to list clients by server)
```

n is the number of seconds it took for the server to respond.

node is the IP address of the server's node.

alias is the alias of the server the client is connected with.

sproc is the server's slump procname.

willingness is the server's willingness to accept new clients (0 - 100).

count is the number of connected clients.

For example:

```
(0 secs) server CMD40120 on anthill (domsrvr) willingness 98
2 connected clients (use pdm_listconn -c -s to list clients by server)
   vbop client 141.202.211.34|vbop2 connected 02/19/1999 10:53:16
   vbop client 141.202.211.34|vbop-0x40120000:anthill:0 connected 02/19/1999 10:44:17
```

-s -c

Lists connections by server, including client detail for each server. The utility displays several lines for each server:

```
(n secs) server  alias (node|sproc) willingness willingness
count connected clients:
client_type node|cproc connected time
```

where:

n is the number of seconds it took for the server to respond.

node is the IP address of the server's node.

alias is the alias of the server the client is connected with.

sproc is the server's slump procname.

willingness is the server's willingness to accept new clients (0 - 100).

count is the number of connected clients.

client_type is "vbop," "animator daemon," or "web engine."

node is the IP address of the client's node.

cproc is the client's slump procname.

time is the connection time.

For example:

```
(0 secs) server CMD40120 on anthill (domsrvr) willingness 98
2 connected clients:
    vbop client 141.202.211.34|vbop2 connected 02/19/1999 10:53:16
    vbop client 141.202.211.34|vbop-0x40120000:anthill:0 connected 02/19/1999 10:44:17
```

-t nn

Specifies a timeout interval in seconds. Because pdm_listconn receives information from an unknown number of clients and servers, it terminates when the specified timeout interval elapses after the last message received.

Default: 2

proc1

Specifies one or more slump procnames, separated by spaces. The utility displays client or server information from them, as appropriate.

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

pdm_logfile--Change stdlog Cutover Size

pdm_logfile lets you change your stdlog.*x* cutover size. The cutover can occur after a specified number of bytes are written. On UNIX, this value is reset with each pdm_init. On Windows, the settings are retained with each pdm_halt and pdm_init.

Syntax

This command has the following format:

```
pdm_logfile [-L|-h]
```

or

```
pdm_logfile [-g -h] [-b bytes]
```

Example

To change your stdlog.*x* files to cutover at 500,000 bytes, issue the following command:

```
pdm_logfile -f STD -b 500000
```

-L

Creates a listing of current cutovers.

-q

Runs pdm_logfile in quiet mode.

-b bytes

Specifies the number of bytes written before cutover occurs.

Restrictions

You can run pdm_load while CA SDM is active, but performance can become very slow. It is best to run pdm_load when no one is using CA SDM.

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

pdm_task--Set Environment Variables

Applies to UNIX only

The pdm_task utility sets environment variables for commands that do not have wrappers. For example, the pdm_task command must precede the report command on the same command line **only** when the command is invoked through a script or the command line. If you issue the report command from a menu, you do not need to include pdm_task, because all environment variables are set by the application.

Note: Reports cannot be generated from the command line on a client.

Syntax

This command has the following format:

```
pdm_task command
```

command

Specifies a command that does not have a wrapper and, therefore, does not automatically set environment variables. See report--Generate Reports (see page 3912) for more information about issuing pdm_task with a command.

pdm_uconv--Convert Local Charset to UTF-8

The pdm_uconv utility assists you in converting data from previous releases of CA SDM or integrations with other CA Technologies products. The most common usage of this utility is to convert from a local charset to UTF-8 and from UTF-8 to a local charset.

Syntax

This command has the following format:

```
pdm_uconv -h [-V] [-s] [-v] [-l | --list-code
| --default-code | -L] [--cannon] [-x] [--to-callback | -c] [--from-callback | -i] [--
fallback | --no-fallback] [-b] [-f] [--t] [--add-signature] [--remove-signature] [-o]
[file ...]
```

- **-h**
  Opens the help menu.
- **-V**
  Prints the program version.
- **-s**
  Uses silent operation and suppresses messages.
- **-v**
  Displays the progress information of the utility.
- **-l**
  Lists all available encoding. The following are valid:
  - **--list-code**
    Lists only the given encoding.
  - **--default-code**
    Lists only the default encoding.
  - **-L**
    Lists all available transliterators.
- **--cannon**
  Prints the list in cnvrtrs.txt(5) format.
- **-x**
  Runs the progress through transliteration.
- **--to-callback *callback***
  Uses callback on destination encoding.

- **-c**
  Omits invalid characters from the output.

- **--from-callback *callback***
  Uses callback on original encoding.

- **-i**
  Ignores invalid sequences in the input.

- **--callback *callback***
  Uses callback on both encoding.s.

- **-b**
  Specifies the block size.
  Default: 4096

- **--fallback**
  Uses fallback mapping.

- **--no-fallback**
  Does not use fallback mapping.

- **-f**
  Sets theoriginal encoding.

- **-t**
  Sets the destination encoding.

- **--add-signature**
  Adds U+FEFF Unicode signature character (BOM).

- **--remove-signature**
  Removes U+FEFF Unicode signature character (BOM)

- **-o**
  Writes output to file.

Examples:

- **From local charset to UTF-8**
  pdm_uconv -t utf-8 inputfile.txt > outputfile.txt

- **From specific charset (iso-2022-jp) to UTF-8**
  pdm_uconv -f iso-2022-jp -t utf-8 inputfile.txt > outputfile.txt

- **From UTF-8 to local charset**
  pdm_uconv -f utf-8 inputfile.txt > outputfile.txt

- **From UTF-8 to specific charset**
  pdm_uconv -f utf-8 -t iso-2022-jp inputfile.txt > outputfile.txt

The pdm_uconv utility has the following are valid callbacks:

- substitute
- skip
- stop
- escape
- escape-icu
- escape-java
- escape-c
- escape-xml
- escape-xml-hex
- escape-xml-dec
- escape-unicode

pdm_webstat--Return Web Usage Statistics

Use pdm_webstat to return CA SDM session and user statistics for one or more web engine processes. The pdm_webstat command shows cumulative sessions, most sessions at a time, and current active sessions. It can also provide information about the individual users.

Syntax

This command has the following format:

```
pdm_webstat [-r] [-d | -D] [-i] [-t timeout] [-p webengine process] [-n] [-h]
```

-r

Specifies raw text mode, without titles and other formatting. Within the output for a single web engine process there are no line breaks; however, the output for each web engine process always starts on a new line.

Raw text mode displays data in exactly the same order as when you use pdm_webstat without the -r option. Use raw text mode if you want to use the resulting data in a spreadsheet or other type of report. For example, the following syntax:

```
pdm_webstat -r
```

shows the following output:

```
10/11/2005 10:31:49 web:local:0 12 4 2
10/11/2005 10:31:49 web:local:1 9 2 2
```

-d

Specifies detailed output that displays user sessions. The -d option lists all current sessions in the form of *userid@IPaddress*. If a session is displayed without a user ID, it usually means that the session has not logged on yet. For example, the following syntax:

```
pdm_webstat -d
```

shows the following output:

```
PDM_Webstat: Invoked at 10/11/2005 10:27:31
=======================================
Report from Webengine: web:local:0
=======================================
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
  @192.168.1.16
  usery@192.168.1.20
=======================================
Report from Webengine: web:local:1
=======================================
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
  SrvcPlus@192.168.1.14
  userx@192.168.1.8
```

-D

Provides more detailed output for debugging purposes. This option should be specified only when specifically requested by CA support. It adds internal information about each session to the detailed output. For example, the following syntax:

```
pdm_webstat -D
```

shows the following output:

```
PDM_Webstat: Invoked at 10/11/2007 10:28:10
=========================================
Report from Webengine: web:local:0
=========================================
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
  @192.168.1.16            SessionStat   1
  userx@192.168.1.20       SessionStat   5
=========================================
Report from Webengine: web:local:1
=========================================
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
  SrvcPlus@192.168.1.14    SessionStat   7
  userx@192.168.1.8        SessionStat  13
```

- **-i**
  Specifies an interval in seconds between successive reports. When the -i argument is specified, pdm_webstat runs continuously. The pdm_webstat command outputs its report in the format requested by other arguments, waits for the interval specified, and outputs the report again. With - i, pdm_webstat terminates only when explicitly cancelled, normally with Ctrl+C. For example, the following syntax:

  ```
  pdm_webstat  - i 5  - p web:local  - r
  ```

  shows the following output:

  ```
  09/21/2007 16:27:25 web:local 14 10 6

  09/21/2007 16:27:30 web:local 17 10 9

  09/21/2007 16:27:35 web:local 18 10 10

  09/21/2007 16:27:41 web:local 21 13 13
  ```

-t timeout

Specifies a time-out value in seconds. This parameter causes pdm_webstat to wait for a number of seconds for a response before terminating. The default is 30 seconds.

-p webengine_process

Specifies the process name of the web engine for which you want to report. By default, all web engine processes are reported. The process name (also called slump-name) is the same name that would be viewed in an slstat output and always starts with "web:".

-n

Suppresses the normal log entry for each reported web engine. By default, a log entry summarizing each web engine is created.

> **Note:** By default, if you do not specify any parameters, pdm_webstat displays summary data for all running processes.

pdm_webstat returns zero if the command completes successfully, and a nonzero value if errors occur (for example, a time-out or no active web engine processes).

Example: pdm_webstat Output When No Parameters Are Specified

The following example shows the output of pdm_webstat when it is executed with no parameters:

```
PDM_Webstat: Invoked at 10/11/2007 10:26:42
=========================================
Report from Webengine: web:local:0
=========================================
Cumulative sessions so far = 12
Most sessions at a time    = 4
```

```
Currently active sessions  = 2
=======================================
Report from Webengine: web:local:1
=======================================
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
```

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

pdm_mail Utility--Send Email Information

The pdm_mail utility is used in notifications to send emails by sending email information to the pdm_mail_nxd process. The pdm_mail utility can also be used for commands, but not to both. If no parameters are used, then the default behavior of using the NX_NTF_xxxx variable to pass parameters is in effect.

For email, the utility is invoked as follows:

```
pdm_mail [-i [-s subject] [-e email_address] [-q]] [-p] [-M] [-F] [-T] [-B] [-H] [-N]
[-R] [-h]
```

- **-i**
  Uses STDIN instead of NTF variables. The following parameters are used for STDIN email behavior only:
  - **-e**
    Specifies the email address (for recipient).
  - **-s**
    Specifies the subject for the email.
  - **-q**
    Disables the display prompt for STDIN.
- **-p**
  Utilizes pager logic. This option includes using the pager email address instead of the regular email address. Only the plain text version of the notification is used (no HTML).
- **-M**
  Uses plain text only (no MIME) in body.
- **-F**
  Specifies the From address of the email.
- **-T**
  Specifies the Reply-To address of the email.

- **-B**
  Specifies the body charset. This might be useful for pagers that do not support the UTF-8.
- **-H**
  Specifies the header charset. This might be useful for pagers that do not support the UTF-8.
- **-N**
  Specifies the Delivery Status Notification (DSN) Notify option.
- **-R**
  Specifies the Delivery Status Notification (DSN) Return option.
- **-h**
  Displays help on the utility.

For commands, the utility is invoked as follows:

Command to mail server

```
pdm_mail -c option [parameter]
```

Command to mail eater

```
pdm_mail -x option [parameter]
```

- **check_interval**
  (-x only) Changes the check mail interval to a specified value (in seconds).
- **report_interval**
  Changes the report interval to a specified value (in seconds).
- **report_now**
  Forces a report to the logs. The counter is not reset.
- **send_q**
  (-c only) Sends local mail queue to remote mail server.
- **trace**
  Turns tracing on or off.

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

CA SDM PDM Database Commands

This article contains the following topics:

pdm_replace--Replace a Database Table

pdm_replace deletes a table in a CA SDM database and replaces it with a table from a temporary file you specify with the -f option; the data from the input file is the only data that is in that table after running pdm_replace. Back up your table before running pdm_replace.

Note: As part of its processing, pdm_replace first shuts down the daemons (UNIX) or services (Windows).

pdm_replace accepts a text file as input, which is the same file format used by pdm_userload. You can create an input file for pdm_replace using pdm_extract; however, you cannot use the output of pdm_backup as input to pdm_replace.

Important! Be sure to name your input file with a name different from the table name you are attempting to replace. For example, if you are replacing a table named ca_contacts and you name the input file ca_contacts.dat, after you execute the pdm_replace command to point to the input file (ca_contacts.dat), it deletes the file after execution because it has the same name as the table.

Restrictions

- pdm_replace can be run only on the following servers, depending on your CA SDM configuration:
  - Conventional: Primary server
  - Advanced availability: Background server

    Important! Ensure that you have stopped all application and standby servers before running this command on the background server.
- Only the privileged user or root can run pdm_replace.
- Do not run pdm_replace when users are logged in to CA SDM.

Syntax

This command has the following format:

```
pdm_replace [-v] -f filename
```

-v

Specifies verbose mode.

-f *filename*

Specifies an ASCII file with the following format:

```
TABLE table_name
fieldname1 fieldname2 . . . . fieldnameN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
```

```
.
.
.
{ "valueN1", "valueN2", . . . "valueNN" }
```

This format is the same file format used by pdm_userload. You can create an input file for pdm_replace using pdm_extract; however, you cannot use the output of pdm_backup as input to pdm_replace.

pdm_restore--Restore a Database

pdm_restore stops CA SDM and then deletes all records from a CA SDM database and replaces them with records from a file you specify with the -f option. The data from the input file is the only data that will be in the CA SDM database after running pdm_restore.

The input file must be created using pdm_extract or pdm_backup, or otherwise formatted for pdm_restore. pdm_backup can back up non-database data, and pdm_restore can restore this data also. pdm_backup and pdm_restore are not recommended when other backup and restoration tools are available.

Note: As part of its processing, pdm_restore first shuts down the daemons (UNIX) or services (Windows).

Syntax

This command has the following format:

```
pdm_restore [-d] [-g] [-n] [-w] [-v]  - f filename
```

Restrictions

pdm_restore can be run only on a CA SDM server. Only the privileged user or root can run pdm_restore. The following restrictions are applicable if you are using the advanced availability configuration:

If you are restoring the database, run the pdm_restore command only on the background server.

- Ensure that you have stopped all servers (application, background, and standby) before you run the pdm_restore command.

Important! Use pdm_restore only with a full database backup created by pdm_backup, because your current database is deleted and replaced by the backup file. Do not run pdm_restore when users are logged in to CA SDM.

- **-d**
  Specifies that only database data is restored.

- **-g**
  Specifies that only non-database data be restored. Only windows (forms) and other non-database data are restored.

- **-n**
  Specifies that NX.env is restored if restoring non-database data. By default, NX.env is not restored. We recommend that the NX.env file not be restored unless the restore is to the same server the backup came from. Restoring an incorrect NX.env can affect unintended databases.

- **-w**
  Specifies that web.cfg is restored if restoring non-database data. By default, web.cfg is not restored.

- **-v**
  Specifies verbose mode.

-f *filename*

Specifies an input file that contains a full backup created by pdm_backup.

pdm_load--Add, Update, and Delete Database Records

Important! Using pdm_load can be destructive so always back up your database before you perform a pdm_load, and use pdm_userload unless instructed to use pdm_load.

pdm_load updates a CA SDM database using an input file you specify, up to a maximum of 112 attributes.

Whenever you upload tickets (such as requests or issues), your ticket number should include a unique prefix or suffix in its string. CA SDM views this number as a string of characters not as a sequential number, and thus cannot guarantee that it will assign a unique number to the uploaded tickets. As long as you assign a unique prefix or suffix using awk or another text processor, you can upload tickets without CA SDM writing over previously assigned numbers.

Syntax

This command has the following format:

```
pdm_load [-c] [-h] [-m] [-r] [-u] [-v]  - f filename
```

The input file entries follow this format:

```
TABLE table_name
fieldname1 fieldname2 . . . . fieldnameN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
.
.
.
```

```
{ "valueN1", "valueN2", . . . "valueNN" }
```

table_name is the name of the table to be loaded, as listed in the CA SDM database schema file, which is located in $NX_ROOT/site/sch/schema.sch (UNIX) or *installation-directory*\site\sch\schema.sch (Windows). $NX_ROOT or *installation-directory* is the directory where you installed CA SDM.

-f *filename*

Specifies an input ASCII file.

-c

Checks the input file against the database and reports on the updates that would be made, but does not make the updates.

-m

Specifies mass update. Specify when you are using pdm_load to add or delete a large number of records. This option suppresses all client notifications of updates and sends a cache refresh message for a table when pdm_load finishes processing the table.

-r

Removes database records that match input records.

Important! Make a backup copy of the database before running pdm_load with this option. After old database records are removed, you must restore the CA SDM database with this backup copy if you want to recover any deleted records.

-u

Updates existing records, but does not insert new records into the database.

CA SDM PDM Daemon Commands

pdm_halt--Terminate Daemons or Stop Services

pdm_halt cleanly terminates all CA SDM daemons (UNIX) or the System Server Service (Windows) on the system from which pdm_halt is executed. The pdm_halt utility usually takes about 30 seconds to complete. If it hangs for more than two minutes, press Ctrl+C to stop pdm_halt, and try again.

Syntax

This command has the following format:

```
pdm_halt [-w] [-a] [time]
```

- **-w**
  Waits for the daemons to stop.

- **-a**
  Stops all proctors defined in the pdm_startup file.

- **[time]**
  Specifies the number of seconds to wait until the command executes.

Restrictions

pdm_halt can be run on a CA SDM server or a CA SDM UNIX client. You must be the privileged user to run pdm_halt.

pdm_init--Start Daemons

Applies to UNIX only

pdm_init starts all CA SDM automatic processes on the system from which pdm_init is executed. These automatic processes are called *daemons* and run continually in the background while you work. Not all of the daemons are started; some are applicable only to certain operating systems.

Note: Use pdm_d_refresh to start daemons that failed to start the first time after remedying the problem that caused them not to start initially. In most cases you do not need to terminate the daemons running to start ones that initially failed.

Syntax

```
pdm_init
```

Restrictions

pdm_init can be run on a CA SDM server or a CA SDM UNIX client. You must be the privileged user to run pdm_init.

pdm_d_refresh--Start Failed Daemons

The pdm_d_refresh command line utility is used primarily for remote daemon configurations. It tells the daemon manager to try to start daemons that have failed to start ten times and that the daemon manager has flagged as "not runnable.". Running this utility flags all daemons as able to run and resets the restart counter. Then, the daemon manager tries to start all stopped daemons.

Syntax

This command has the following format:

```
pdm_d_refresh
```

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

pdm_status--Show Status of Daemons or Processes

pdm_status shows the status of all CA SDM daemons (UNIX) or processes (Windows) on the system from which the command is executed.

Output is displayed in this format:

```
DAEMON                          STATUS      HOST      PID   SLUMP CONNECT TIME
-------------------------------------------------------------------------------
Agent anthill                   Running     anthill   455   Tue Feb 17 17:55:12
Ddict_rd             (ddictrd) Completed   anthill
Data Dictionary   (ddictbuild) Completed   anthill
...
User Validation      (boplgin) Running     anthill   456   Tue Feb 17 17:55:21
```

Syntax

This command has the following format:

```
pdm_status
```

uniconv--Start UNIX CA NSM Event Converter Daemon

Applies to UNIX only

When CA SDM is integrated with CA NSM, you can use uniconv to send generic event data to filter daemons in CA SDM. uniconv is used in a message action in CA NSM Event Management.

Syntax

This command has the following format:

```
uniconv  - h &opnode  - e &'text' [-n &
nodeid] [-u &userid] [-d &datem] [-t &'
time']
```

Restrictions

uniconv must be run from $NX_ROOT/bin on UNIX. Your site must be integrated with CA NSM to use this utility.

- **-h &opnode**
  Specifies the node name of the machine on which you are executing uniconv (required).
- **-e &'text'**
  Specifies the full text of the message (required).
- **-n &nodeid**
  Specifies the node name from which the message originated (required).

- **-u &userid**
  Specifies the login ID of the person who originated the message.

- **-d &datem**
  Specifies the system date in *mm*/*dd*/*yy* format.

- **-t &'time'**
  Specifies the system time.

CA SDM PDM Server Commands

pdm_proctor_init--Start Proctor on Secondary Servers

Applies to UNIX only

Use pdm_proctor_init to start the proctor on secondary servers. All secondary servers should be started prior to starting the daemons from the primary server. After all daemons have been stopped from the primary server, use pdm_halt on the secondary server to stop this proctor.

Note: Do not use pdm_proctor_init on the primary server.

Syntax

This command has the following format:

```
pdm_proctor_init
```

pdm_server_control Utility--Identify Servers

The pdm_server_utility commands identify the server as background or standby in an advance availability configuration.

Execute the following command from the command prompt:

```
pdm_server_control -h | -b | -q interval [-s server_name] | -t | -c [-server_name]
```

- **-h**
  Displays the help page.

- **-b**
  Notifies a local standby server to become the background server. The standby server must be running. If the server is not running, it is started but no failover is performed. To start a failover, run the command again.

- **-q interval [-s server_name]**
  Notifies a local or remote application server to quiesce in a specified time interval. This interval is the number of seconds before the server shutdowns. When using this option without a server_name, the local server is notified to quiesce. This option cannot be used for a background or a standby server.

- **-t**
  Displays the type of this CA SDM advance availability Server.

- **-c [-s server_name]**
  Notifies a local or remote application server to cancel the previous quiesce the request.

pdm_rest_util--Manage the CA SDM RESTful Web Services Application

CA SDM uses this utility automatically. You can run it manually if you require the utility, such as after an unexpected error occurs. This REST web services utility deploys the REST services web application. This utility deploys the REST application to the dedicated REST Tomcat instance. A batch file in the NX_ROOT\bin directory (pdm_rest_util.bat for Windows or ./pdm_rest_util.sh for UNIX) lets you invoke the utility.

This command has the following formats and options:

```
pdm_rest_util  - h | [-deploy] | [-undeploy]
```

- **-h**
  Prints command-line help.

- **-deploy**
  Generates, compiles, and deploys all Majic factories.

- **-undeploy**
  Undeploys REST Web Services on the local server.

Undeploy the REST Web Services Application

You can undeploy the REST Web Services application with the pdm_rest_util utility. For example, you want to perform CA SDM maintenance and prefer to undeploy REST during this operation.

Follow these steps:

1. Open a command prompt.
2. Execute the following command:

   ```
   pdm_rest_util -undeploy
   ```

   The REST Web Services application is undeployed.

Important! If you undeploy the REST application with this utility, REST can redeploy automatically when CA SDM restarts. We recommend that you use the CA SDM configuration to disable REST indefinitely.

pdm_k_reindex -- Knowledge Re-Index Utility

The Knowledge reindex utility, pdm_k_reindex.exe, is located under the Knowledge Management installation directory.

Note: Reindexing the documents in the knowledge base can be a time-consuming operation, depending upon the size of your database. We recommend that you run the Knowledge Reindex utility after all the changes have been added. For advanced availability configuration, you cannot execute the knowledge re-index utility during failover.

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use pdm_task to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

Follow these steps:

1. Open the command prompt.
2. Enter the following command at the command prompt to run the knowledge reindex:

For example:

```
pdm_k_reindex
```

The following options are available with this command.

- **-D**
  Defines the debug mode, such as printing to the command window.
- **-v**
  Defines the verbose mode, such as printing to the stdlog file.
- **-i**
  Does not create table indexes in the reindex table after reindexing.

Note: Parameters with a dash as a prefix, such as " - D", must precede other parameters that do not have this prefix.

The other option is as follow:

- ***File*:reindex.txt**
  Documents are reindexed to the specified file.

- **+i**
  Creates the indexes of the reindexed table only, which is the search table after reindexing. The old indexes are dropped before reindexing.

- **+t**
  Switches the names of search and reindex tables only.

> **Note:** A “+” prefix denotes only this parameter applies.

- **sdtout**
  Defines the frequency of statistic appearing in the command window. By default the knowledge reindex utility provides statistics into the command window for every 1000 documents processed. However, sometimes statistics are required to be provided more often. Use the following parameter:

  ```
  pdm_k_reindex -i sdtout:10
  ```

  In this case, statistics display in the command window for every ten documents.

The documents are reindexed in the knowledge base.

When to Use pdm_k_reindex

Run the pdm_k_reindex utility when one or more of the following search settings were changed:

- Noise words
- Synonyms
- Special terms
- Language
- Remove Similar Words
- Remove Noise Words
- Valid Character Range
- Recognize Special Terms

An appropriate message appears on Knowledge node of Administration tab when a change occurs.

Re-Index Tracking

While the re-index is running, you can view the status of the process in the Re-Index Tracking section in the lower half of the page. Each field is described as follows:

- **Document #**
  Specifies the number of documents already processed.

- **Average Size (Words)**
  Specifies the size of the current documents, calculated by the number of words minus the number of noise words.

- **Rate (Docs/Sec)**
  Specifies the number of documents processed, per second.

- **Time from Start**
  Indicates the duration of the re-index process since start.

- **Time Remaining**
  Specifies the estimated amount of time remaining for the process, based on the current rate and the remaining number of documents.

- **Failures #**
  Represents the number of failed documents (maximum=100). When the maximum number of failures is reached, the administrator is prompted to either continue or cancel the process.

> **Note:** If changes have been made to Noise Words, Special Terms, Synonyms or Parse Settings and you do not re-index, you are prompted the next time you access the Knowledge node of the Administration tab. Changes will take effect only after the Knowledge Re-index utility is run.

Import and Re-Indexing

When pdm_kit.exe is invoked from the command line, the pdm_kit utility imports the documents into the database. After pdm_kit is completed, assuming document indexing or re-indexing has not been disabled using the command-line options, the re-index utility (pdm_k_reindex.exe) is automatically invoked. The status and output of the re-indexing operation is automatically written to the "EBR_REINDEX.LOG" in the $NX_ROOT\log directory.

Index and De-Index Queue Settings for Batch and Instant Processing

Indexing and De-Indexing both run a batch process to include a predefined number of documents at one run. These batch processes are used for performance optimization. If more documents are included in the batch, system performance increases.

The number of documents you can process is limited; the limit depends on the size of the documents and the linked attachments. The document size is calculated based on the pure text and its attachments. Imagine and format elements are not calculated.

> **Note:** You can limit the size of attachments by navigating to Attachments Library, Repositories on the Administration tab and editing the repository to set the File Limit Size (KB).

The recommended batch maximum size is between 2-12 MB (per the EBR_MAX_INDEX_BATCH_SIZE parameter of the NX.env file and the average document size).

- If the average size of your document (including attachments) is approximately 0.1 MB, keep the default setting in NX.env:

```
@EBR_MAX_INDEX_BATCH_SIZE=128

@NX_EBR_INDEX_QUEUE_TIMEOUT=10

@NX_EBR_REINDEX_QUEUE_TIMEOUT=1

@NX_EBR_INDEX_QUEUE_ONLINE=Yes

@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=Yes
```

  This setting means that one batch processes 128 documents, that batch executions have ten second intervals, and when in reindex, the wait interval between two batches is one second.

- If the average size of your document (including attachments) is approximately 0.5 MB, keep the default setting in NX.env

```
@EBR_MAX_INDEX_BATCH_SIZE=25

@NX_EBR_INDEX_QUEUE_TIMEOUT=10

@NX_EBR_REINDEX_QUEUE_TIMEOUT=10

@NX_EBR_INDEX_QUEUE_ONLINE=No

@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=No
```

  This setting means that one batch processes 25 documents, that batch executions have ten second intervals, and when in reindex, the wait interval between two batches is ten seconds.

PDM-Discovered Asset Commands

pdm_discupd -- Discovered Asset Update

Batch update of non-CA SDM Discovered Assets. Use this utility to update assets that were imported by the pdm_discimp command.

Syntax

```
pdm_discupd [-t] [-v] [-d domsrvr]
```

Where

- **t**
  Test
- **v**
  Verbose/diagnostic mode.
- **d**
  Object manager (domsrvr) to use for processing.

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

pdm_discimp -- Discovered Asset Import

Batch registration of non-CA SDM Discovered Assets. Use this to search the MDB for assets that were registered by other software products and register them as CA SDM assets, so they can be used in CA SDM.

Logic is similar to Discovered Assets dialog that can be launched from Asset Search/List web form. That is an interactive and batch process.

This program will query the ca_logical_asset, ca_asset, and ca_logical_asset_property tables, using various parameters, and attempt to register new CA SDM Assets from the discovered values.

Syntax

```
pdm_discimp [-l label] [-s serial number] [-t asset tag] [-n hostname] [-d dns name]
[-m mac address] [-c asset class] [-v] [-r] [-o object manager]
```

Asset selection criteria (use % for wild card):

- **l**
  Match this asset label.
- **s**
  Match this serial number.
- **t**
  Match this asset tag.
- **n**
  Match this hostname.

Asset property selection criteria (use % for wild card):

- **d**
  Match this dns name.
- **m**
  Match this mac address.

Other options:

- **c**
  Asset class to assign when registering new owned assets defaults to Discovered Hardware.
- **v**
  Verbose/diagnostic mode.

- **r**
  Register assets, otherwise runs in simulate mode.
- **h**
  Displays this information.
- **o**
  Object manager (domsrvr) to use for processing.

Note: If processing results in a blank Asset Label, the value found for the host name or DNS Name will be used as the Asset Label. Assets must have at least a Label and Asset Class to be registered for use in CA SDM.

Because of the structure of the MDB and CA SDM architecture limitations, two queries are performed to select the appropriate records to process. It is important to understand this as it could affect performance. The first query retrieves the rows from a join between the ca_logical_asset and ca_asset tables that match label, serial number, tag and hostname. Then for each resulting row, a query is performed against ca_logical_asset_property to match dns_name and mac_address. The asset from the first query is chosen for registration if the second query results in rows being returned.

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

pdm_text_cmd--Text API Command Line Interface

Use the pdm_text_cmd command for the Text API, which you can use to create and update various objects such as requests, change orders, issues, assets, and contacts.

Important! You cannot use a single or double quote as the parameter of the pdm_text_nxd or bop_cmd commands.

Syntax

This command has the following format:

```
pdm_text_cmd  - t table {-u from_userid  - p from_persid} [-o operation] [-f input
file] [-T timeout] [-h]
```

-t *table*

(Required) Specifies the table to process. The *table* name can be one of the following values (not case sensitive):

- Asset
- Contact
- Change
- Issue
- Request

Note: See the [OPTIONS] section of the text_api.cfg file for a complete list of valid table names.

-u *from_userid* **| -p** *from_persid*

(One option required) Identifies the contact for this operation:

- **-u *from_userid***
  Identifies the contact using the User ID value.
- **-p *from_persid***
  Identifies the contact using the unique object identifier for the contact record. *from_persid* must be of the form **cnt:***xxxx. xxxx* is the persistent ID of the object.

Note: The value that you specify with this option is appended to the end of the input for the pdm_text_cmd command using the appropriate keyword, %FROM_USERID or % FROM_PERSID.

-o *operation*

Specifies the operation to perform. The *operation* must be one of the following values (not case sensitive):

- NEW -- Creates an object. This value is the default if no operation is specified.
- UPDATE | UPD -- Creates an object if not found or updates an existing object if found.
- UPDATE_ONLY | UPDO -- Updates object if found; otherwise, does nothing.

Both UPDATE and UPDATE_ONLY require the %SEARCH keyword in the command input. You can perform only one operation transaction with each invocation of pdm_text_cmd.

-f *input_file*

Specifies the full path of the file to process, which is a text file containing valid Text API commands. If you omit this parameter, commands are used from STDIN. The Text API uses the following basic format for input:

```
%keyword=value
```

You can issue multiple commands within the input by separating the command request by at least five percent signs (%%%%%).

Note: For more information about valid keywords and about formatting input to the Text API, see the file text_api.cfg.

-T *timeout*

Specifies the number of seconds to wait for a response from the server before timing out. The default is 30 seconds.

Note: pdm_text_cmd shows the text-based replies received back from the Text API, which include success or error messages, and the original text sent using the API for processing. pdm_text_cmd returns zero if the command completes successfully without warnings or errors or one if the command completes successfully, but with warnings. Any other return value indicates that an error occurred.

Important! On UNIX, the LIBPATH must be set before running several CA SDM utilities. Use *pdm_task* to set the LIBPATH before running a utility. For example, input "pdm_task pdm_clean_attachments ...".

Note: When passing the parameters from command prompt, use Ctrl+Z in Windows and Ctrl+D in POSIX.

Input Examples

pdm_text_cmd is the command line interface for the Text API that you can use to create and update various objects such as requests, change orders, issues, assets, and contacts.

Example: Use an Input File to Create an Issue

The following example demonstrates how to use a pdm_text_cmd input file to create an issue:

```
%DESCRIPTION=This is my Test.
%PRIORITY=3
```

To process this file, assuming its full path is c:\input.txt, issue the following command:

```
pdm_text_cmd -t Issue  - u user01 -f c:\input.txt
```

Example: Use an Input File to Update an Issue

The following example demonstrates an input file to update issue 123 to a priority of 2:

```
%SEARCH=ISSUE_ID
%ISSUE_ID=123
%PRIORITY=2
```

To process this file, assuming its full path is c:\update.txt, issue the following command:

```
pdm_text_cmd -t Issue -o UPDATE_ONLY  - u user01 -f c:\update.txt
```

Example: Use an Input File to Create Multiple Requests

The following example demonstrates creating multiple requests with one input file. This command can be helpful creating test data on a test system.

```
%DESCRIPTION=This is Test 1.
%PRIORITY=3
%%%%%
%DESCRIPTION=This is Test 2.
%PRIORITY=2
%%%%%
%DESCRIPTION=This is Test 3.
%PRIORITY=None
```

To process this file, assuming its full path is c:\testdata.txt, issue the following command:

```
pdm_text_cmd -t Request  - u user01-f c:\testdata.txt
```

pdm_log4j_config Utility--Modify the log4j properties File

The pdm_log4j_config.pl utility lets you configure the log4j properties file of CA SDM, web components, PDM_RPC, Support Automation, Rest, and CMDB Visualizer. Execute the utility batch script that is based on your environment. For Windows, execute pdm_log4j_config from the command line. For UNIX, execute the pdm_log4j_config.sh file.

This command has the following format:

```
pdm_log4j_config  - f <component> -d
pdm_log4j_config -h
pdm_log4j_config  - f <component>  [-a | -n <name>] [-l <log level>] [I <max # of log
files>] [-s <max size of log files>] [-t <log level threshold>]
```

- **-f**
  Specifies the log4j configuration of CA SDM or the component of CA SDM that you want to change. Enter one of the following values:
  SDM_WEB, SDM_RPC, REST, SA, or Viz.
  Note: Use the mandatory option along with the other options.

- **-d**
  Displays the current log4j.properties configuration.

- **-h**
  Displays help for the utility.

- **-a**
  Completes all changes to log4j.properties globally.

- **-n**
  Specifies that you only want to modify a specific class or package name.
  Specify a specific class name, such as bop_logging, or a complete package name, such as com.ca.ServicePlus.

- **-l**
  Specifies the log level that you want to set.

  Note: For the -l, -l, -s, and -t parameters, specify the -a or -n option.

- **-i**
  Specifies the max file number index that you want to set.
  -s
  Specifies the max file size that you want to set.

  Important! Change the appender in the log4j.properties file of Visualizer to Rolling File Appender before you execute the command with this parameter. If you do not change the appender, MaxFileSize generates logs in the same file.

- **-t**
  Specifies the log level threshold.

Utility Usage Examples

The following list provides examples of using the pdm_log4j_config utility:

- Modify the log verbosity level for all loggers configured in the properties file by using the -l and -a variables.
  For example, set all of the loggers configured in Support Automation to a level of DEBUG:

```
pdm_log4j_config  - f SA -a -l DEBUG
```

- Modify the log verbosity level for a specific logger class or package name in the CA SDM log4j properties file by using the -l and -n variables.
  For example, set the logger for the pdm_rpc package to DEBUG using one of the following code samples:

```
pdm_log4j_config  - f SDM_RPC -n pdm_rpc -l DEBUG

pdm_log4j_config  - f SDM_RPC -n com.ca.ServicePlus.pdm_rpc -l DEBUG
```

- Modify the maximum number of log files to create for all the appenders (MaxBackupIndex property) by using the -i and -a variables in the log4j properties file of REST.
  For example, set the maximum number of files for all appenders to 9.

```
pdm_log4j_config  - f REST -a -i 9
```

- Modify the maximum number of log files configured in the CA SDM log4j properties file to create for an appender for a specific class or set of classes (MaxBackupIndex property) by using the -i and -n variables.
  For example, set the maximum number of files for bop_logging to 7.

```
pdm_log4j_config  - f SDM_WEB -n bop_logging -i 7
```

- Modify the maximum size of each log file configured in the REST log4j properties file to create for any appender (MaxFileSize property) by using the -s and -a variables.
  For example, set the maximum size of files for all appenders to 9 MB.

```
pdm_log4j_config  - f REST -a -s 9MB
```

- Modify the maximum size of each log file configured in the CA SDM log4j properties file to create for an appender for a specific class or set of classes (MaxFileSize property) by using the -s and -n variables.
  For example, set the maximum size of files for bop_logging to 7 MB.

```
pdm_log4j_config  - f SDM_WEB -n bop_logging -s 7MB
```

- Modify the log level threshold for all the appenders configured in the Support Automation log4j properties file (Threshold property) by using the -t and -a variables.
  For example, set the log level threshold to DEBUG.

```
pdm_log4j_config  - f SA -a -t DEBUG
```

> **Note:** The -t parameter log level threshold overrides the -l parameter log level. If you modify the log level and the threshold level, the DEBUG logs from the servlet do not appear in the file.

- Modify the log level threshold for an appender for a specific class or set of classes (Threshold property) configured in the CA SDM log4j properties file by using the -t and -n variables.
  For example, set the log level threshold to WARN.

```
pdm_log4j_config  - f SDM_WEB -n bop_logging -t WARN
```

- Execute the following command to view the current logger and appender configuration of the REST log4j properties file:

```
pdm_log4j_config  - f REST -d
```

Important! Use -l, -i, -s, and -t variables together with one of the -a or -n options, Do not use both the options. The -f option is mandatory. The -h and -d options are mutually exclusive to any other option.

Modify the Log File Refresh Interval Manually

Administrators can modify how often CA SDM monitors the log4j.properties file for changes. By default, the refresh interval is set to 60 seconds. CA SDM components including SDM Servlets, PDM_RPC, Support Automation, CMDB Visualizer, and REST use log4j for logging.

Follow these steps:

1. Open the following directory on the CA SDM server:

   NX_ROOT

2. Open the NX.env file for editing.
3. Modify the NX_LOG4J_REFRESH_INTERVAL variable with a value in milliseconds.

   Note: If you enter a negative or nonnumeric value, the value defaults to 60 seconds.

4. Save the NX.env file.

Modify the jsrvr.log Appender

By default, servlets such as PDMContextListener, pdmweb, UploadServlet, and pdm_report log INFO level messages to the jsrvr.log file. You change the threshold level of the jsrvr.log appender to log any messages under the INFO level.

Follow these steps:

1. Modify the level in the log4j.properties file to the following threshold:

   ```
   log4j.appender.jsrvrlog.Threshold=debug
   ```

2. Modify the log level of UploadServlet:

   ```
   log4j.logger.com.ca.ServicePlus.uploadservlet=debug, jsrvrlog
   ```

3. Open the jsrvr.log file.

4. Confirm that the DEBUG log messages of UploadServlet appear.

Note: If you modify the log level without modifying the threshold level, the DEBUG logs from the servlet do not appear in the file. Not all servlets have explicit loggers attached. For example, the log4j.properties file does include pdmweb, BOServlet, pdm_export, pdm_report, and pdm_cache, which are part of the pdmweb servlet. To see DEBUG logs from these servlets, modify the pdmweb log level.

Modify the jstd.log Appender

All logs from nonwebapp applications dump into the jstd.log file separately. You can display logs for any of these applications, such as pdm_rpc by changing the log level of that specific application.

Follow these steps:

1. Modify the following log level:

```
log4j.logger.com.ca.ServicePlus.pdm_rpc=debug
```

2. Open log4j.properties and confirm that the log entries appear.

CA SDM Report Command

This article contains the following topics:

rpt_srv--Generate Reports

Valid for Windows only

The report program lets you generate a report from the command line on the server. To issue the report command at the command line or in a script, you must include pdm_task. The pdm_task command sets up environment variables for commands that do not have a wrapper. Enter pdm_task with the report command on the same command line only when the report is invoked through a script or the command line. If you issue the report command from a menu, you do not need to include pdm_task, because all environment variables are set by the application.

Syntax

This command has the following format:

```
rpt_srv  - m [-h] [-e] [-f] [-F ffstring] [-p pagelength] [-C] [-B] filename [
command line arguments]
```

- **-m**
  Signifies that the report is manually being run from the command line.

- **-e**
  Echoes compiled script (for debugging purposes).

- **-f**
  Uses form feeds between pages.

- **-F *ffstring***
  Sets the optional form-feed string.

- **-p *pagelength***
  Sets the page length. The default page length is 66.

- **-C**
  Changes encoding from UTF-8 to another charset. The default output is UTF-8.
  Example: To convert the output to JIS, you would run "-C iso-2022-jp"
  Example: To encode to the operating system's native charset, use "DEFAULT" or "NATIVE".

- **-B**
  Suppresses the Byte Order Mark if the variable NX_ADD_UTF8_BYTE_ORDER_MARK is set.
  The NX_ADD_UTF8_BYTE_ORDER_MARK option is a signature into a file. It allows editors that support UTF-8 to maintain the UTF-8 integrity of the file.

  Note: This is only needed for non-ASCII data. If this is not installed, the default behavior omits the Byte Order Mark (BOM). If installed, set it to "1" or "Yes".

- ***filename***
  Specifies the report template. If you are not running the report command from the directory in which the template file is located, include the complete file path name. The command sends the output as standard output (stdout).

- **command line arguments**
  Specifies parameters received by the report template. If the report is designed to accept command line arguments, you must enter a command line argument for each parameter in the report template. If the argument is empty, enter the null string.
  For example, the following command supplies the command line arguments Smith, Jane, and L. The report template requires these three parameters to generate the Affected Contacts Report. For example, enter the following command:

  ```
  rpt_srv  - m c:\reports\affected.rpt Smith Jane L
  ```

  In the next example, Jane Smith does not have a middle initial:

  ```
  rpt_srv  - m c:\reports\affected.rpt Smith Jane "
  ```

report--Generate Reports

Applies to UNIX only

The report program lets you generate a report from the command line on the server. To issue the report command at the command line or in a script, you must include pdm_task. The pdm_task command sets up environment variables for commands that do not have a wrapper. Enter pdm_task with the report command on the same command line *only* when the report is invoked through a script or the command line. If you issue the report command from a menu, you do not need to include pdm_task, because all environment variables are set by the application.

Syntax

This command has the following format:

```
pdm_task report [-h] [-e] [-f] [-F ffstring] [-p pagelength] filename [ command line arguments]
```

-e

Echoes compiled script (for debugging purposes).

-f

Uses form feeds between pages.

-F ffstring

Sets the optional form-feed string.

-p pagelength

Sets the page length. The default page length is 66.

filename

The report template. If you are not running the report command from the directory in which the template file is located, include the complete file path name. The command sends the output as standard output (stdout).

command line arguments

Specifies parameters received by the report template. If the report is designed to accept command line arguments, you must enter a command line argument for each parameter in the report template. If the argument is empty, enter the null string.

For example, the following command supplies the command line arguments Smith, Jane, and L. The report template requires these three parameters to generate the Affected Contacts Report.

For example, enter:

```
pdm_task report /opt/CAisd/samples/sdk/reports/affected.rpt
```

In the next example, Jane Smith does not have a middle initial:

```
pdm_task report /opt/CAisd/samples/sdk/reports/affected.rpt Smith Jane "
```

CA SDM Form Groups

This article contains the following topics:

Customer Forms Group

The following web forms are included in the Customer forms groups:

- about.htmpl
- bin_form_np.htmpl
- chg_lr.htmpl
- cr_lr.htmpl
- detail_iss.htmpl
- detail_issalg.htmpl
- detail_KD.htmpl
- generic.htmpl
- home.htmpl
- iss_lr.htmpl
- issue_status_change.htmpl
- list_iss.htmpl
- list_isscat.htmpl
- list_KD.htmpl
- menu_frames.htmpl
- std_body.htmpl
- std_body_site.htmpl
- std_footer.htmpl
- std_footer_site.htmpl

- std_head.htmpl
- std_header.htmpl
- std_head_site.htmpl

Employee Forms Group

The following web forms are included in the Employee forms groups:

- about.htmpl
- bin_form_np.htmpl
- buttons.htmpl
- change_status_change.htmpl
- chg_lr.htmpl
- cr_lr.htmpl
- detail_alg.htmpl
- detail_chg.htmpl
- detail_chgalg.htmpl
- detail_cr.htmpl
- detail_in.htmpl
- detail_KD.htmpl
- generic.htmpl
- home.htmpl
- iss_lr.htmpl
- list_chg.htmpl
- list_chgcat.htmpl
- list_cr.htmpl
- list_in.htmpl
- list_KD.htmpl
- list_pcat.htmpl
- list_pcat_cr.htmpl

- list_pcat_in.htmpl
- menu_frames.htmpl
- request_status_change.htmpl
- show_error.htmpl
- std_body.htmpl
- std_body_site.htmpl
- std_footer.htmpl
- std_footer_site.htmpl
- std_head.htmpl
- std_header.htmpl
- std_head_site.htmpl

Analyst Forms Group

The following web forms are included in the Analyst forms groups:

A

- about.htmpl
- acctyp_role_tab.htmpl
- acctyp_web_auth_tab.htmpl
- acctyp_wsp_tab.htmpl
- admin_empty.htmpl
- admin_main_role.htmpl
- admin_tab_dflt.htmpl
- admin_tree.htmpl
- attmnt_content_tab.htmpl
- attmnt_fields.htmpl
- attmnt_permissions_tab.htmpl
- attmnt_upload_popup.htmpl
- att_mgs_event.htmpl

- att_stype_event.htmpl
- aty_chg_ntfr_tab.htmpl
- aty_chg_svy_tab.htmpl
- aty_cr_ntfr_tab.htmpl
- aty_cr_svy_tab.htmpl
- aty_iss_ntfr_tab.htmpl
- aty_iss_svy_tab.htmpl
- aty_kdComment_ntfr_tab.htmpl
- aty_kd_ntfr_tab.htmpl
- aty_mgs_ntfr_tab.htmpl

B

- bhvtpl_todo_tab.htmpl
- bhvtpl_trans_info_tab.htmpl
- bin_form_np.htmpl

C

- cancel.htmpl
- cancel_empty.htmpl
- category_content_tab.htmpl
- category_permissions_tab.htmpl
- chgcat_auto_assignment_tab.htmpl
- chgcat_prptpl_tab.htmpl
- chgcat_wftpl_tab.htmpl
- chg_accumulate.htmpl
- chg_causedreq_tab.htmpl
- chg_close_all_child.htmpl
- chg_expedite.htmpl
- chg_lr.htmpl

- chg_relchg_tab.htmpl
- chg_relreq_tab.htmpl
- cia_bmhier_tab.htmpl
- cia_export_bmhier.htmpl
- cia_export_nr.htmpl
- cia_nr_tab.htmpl
- cia_pwd_tab.htmpl
- cia_sync_stat.htmpl
- cnote_tracker.htmpl
- cnt_addr_tab.htmpl
- cnt_auto_assignment_tab.htmpl
- cnt_env_tab.htmpl
- cnt_grp_tab.htmpl
- cnt_mem_tab.htmpl
- cnt_notif_tab.htmpl
- cnt_org_tab.htmpl
- cnt_rem_tab.htmpl
- cnt_role_tab.htmpl
- cr_attach_chg.htmpl
- cr_close_all_child.htmpl
- cr_detach_chg.htmpl
- cr_lr.htmpl
- cr_relreq_tab.htmpl

D

- dcon_constraint_tab.htmpl
- dcon_sql_tab.htmpl
- detail.template

- detail_acctyp.htmpl
- detail_act_type_assoc.htmpl
- detail_ADMIN_TREE.htmpl
- detail_alg.htmpl
- detail_arcpur_rule.htmpl
- detail_asset.htmpl
- detail_atev.htmpl
- detail_atomic_cond.htmpl
- detail_attmnt_edit.htmpl
- detail_attmnt_error.htmpl
- detail_attmnt_folder.htmpl
- detail_attmnt_ro.htmpl
- detail_attr_alias.htmpl
- detail_aty.htmpl
- detail_audlog.htmpl
- detail_bhvtpl.htmpl
- detail_bmcls.htmpl
- detail_bmhier.htmpl
- detail_bmrep.htmpl
- detail_BU_TRANS.htmpl
- detail_ca_cmpny.htmpl
- detail_chg.htmpl
- detail_chgalg.htmpl
- detail_chgcat.htmpl
- detail_chgstat.htmpl
- detail_chgtype.htmpl
- detail_CI_ACTIONS.htmpl

- detail_CI_ACTIONS_ALTERNATE.htmpl
- detail_CI_DOC_TEMPLATES.htmpl
- detail_CI_STATUSES.htmpl
- detail_CI_WF_TEMPLATES.htmpl
- detail_cmth.htmpl
- detail_cnote.htmpl
- detail_cnt.htmpl
- detail_cost_cntr.htmpl
- detail_country.htmpl
- detail_cr.htmpl
- detail_crs.htmpl
- detail_crsq.htmpl
- detail_cr_prptpl.htmpl
- detail_ctab.htmpl
- detail_ctimer.htmpl
- detail_ctp.htmpl
- detail_dcon.htmpl
- detail_dept.htmpl
- detail_dmn.htmpl
- detail_doc_rep.htmpl
- detail_DOC_VERSIONS.htmpl
- detail_EBR_ACRONYMS.htmpl
- detail_EBR_LOG.htmpl
- detail_EBR_NOISE_WORDS.htmpl
- detail_EBR_SYNONYMS_ADM.htmpl
- detail_event_log.htmpl
- detail_evt.htmpl

- detail_fmgrp.htmpl
- detail_grc.htmpl
- detail_g_cnt.htmpl
- detail_g_loc.htmpl
- detail_g_org.htmpl
- detail_g_prod.htmpl
- detail_g_qname.htmpl
- detail_g_srvrs.htmpl
- detail_g_tblmap.htmpl
- detail_g_tblrule.htmpl
- detail_help_set.htmpl
- detail_hier_edit.htmpl
- detail_hier_ro.htmpl
- detail_ical_event_template.htmpl
- detail_imp.htmpl
- detail_in.htmpl
- detail_iss.htmpl
- detail_issalg.htmpl
- detail_isscat.htmpl
- detail_issstat.htmpl
- detail_iss_wf.htmpl
- detail_kc.htmpl
- detail_KCAT.htmpl
- detail_KD.htmpl
- detail_KD_FILE.htmpl
- detail_KD_QA.htmpl
- detail_KD_SAVE_AS.htmpl

- detail_KD_TASK.htmpl
- detail_KD_TASK_cancel_rework.htmpl
- detail_KD_TASK_retire.htmpl
- detail_KD_template.htmpl
- detail_KEIT_TEMPLATES.htmpl
- detail_KT_ACT_CONTENT.htmpl
- detail_KT_BLC.htmpl
- detail_KT_FILE_TYPE.htmpl
- detail_KT_FLG_TYPE.htmpl
- detail_ldap.htmpl
- detail_ldap_group.htmpl
- detail_loc.htmpl
- detail_LONG_TEXTS.htmpl
- detail_lr_ro.htmpl
- detail_macro.htmpl
- detail_macro_type.htmpl
- detail_menu_bar.htmpl
- detail_menu_tree_name.htmpl
- detail_mfrmod.htmpl
- detail_mgs.htmpl
- detail_mgsalg.htmpl
- detail_mgsstat.htmpl
- detail_NOTIFICATION.htmpl
- detail_no_contract_sdsc.htmpl
- detail_nr.htmpl
- detail_nrf.htmpl
- detail_nr_com.htmpl

- detail_ntfl.htmpl
- detail_ntfm.htmpl
- detail_ntfr.htmpl
- detail_options.htmpl
- detail_org.htmpl
- detail_O_COMMENTS.htmpl
- detail_O_EVENTS.htmpl
- detail_pcat.htmpl
- detail_perscnt.htmpl
- detail_position.htmpl
- detail_pr.htmpl
- detail_prefs.htmpl
- detail_pri.htmpl
- detail_prod.htmpl
- detail_projex.htmpl
- detail_prptpl.htmpl
- detail_prpval.htmpl
- detail_prpval_rule.htmpl
- detail_prp_edit.htmpl
- detail_QUERY_POLICY.htmpl
- detail_rc.htmpl
- detail_response.htmpl
- detail_role.htmpl
- detail_role_go_form.htmpl
- detail_rptmeth.htmpl
- detail_rrf.htmpl
- detail_rss.htmpl

- detail_sapolicy.htmpl
- detail_saprobtyp.htmpl
- detail_sdsc.htmpl
- detail_sdsc_map.htmpl
- detail_seq.htmpl
- detail_sev.htmpl
- detail_site.htmpl
- detail_slatpl.htmpl
- detail_srvr_aliases.htmpl
- detail_srvr_zones.htmpl
- detail_state.htmpl
- detail_svc_contract.htmpl
- detail_svy_atpl.htmpl
- detail_svy_qtpl.htmpl
- detail_svy_tpl.htmpl
- detail_tab.htmpl
- detail_tenant.htmpl
- detail_tenant_group.htmpl
- detail_tskstat.htmpl
- detail_tskty.htmpl
- detail_tspan.htmpl
- detail_typecnt.htmpl
- detail_tz.htmpl
- detail_urg.htmpl
- detail_USP_PREFERENCES.htmpl
- detail_usp_servers.htmpl
- detail_vpt.htmpl

- detail_web_form.htmpl
- detail_wf.htmpl
- detail_wftpl.htmpl
- detail_wrkshft.htmpl
- dmn_dcon_tab.htmpl
- edit_prop_dyn.htmpl
- ed_image_pane.htmpl
- evt_action_info.htmpl
- evt_config_info.htmpl

G

- generic.htmpl
- get_comment.htmpl
- g_profile_browser.htmpl
- g_profile_browser2.htmpl
- g_profile_browser3.htmpl
- g_profile_browser_frameset.htmpl
- g_profile_jump.htmpl
- g_profile_scratchpad.htmpl

H

- hierload_admin_tree.htmpl
- hierload_KCAT.htmpl
- hiersel_admin_tree.htmpl
- hiersel_KCAT.htmpl
- hourglass.htmpl
- html_editor_create_change_order.htmpl
- html_editor_create_ticket.htmpl
- html_editor_frames.htmpl

- html_editor_insert_image.htmpl
- html_editor_insert_link.htmpl
- html_editor_insert_table.htmpl
- html_editor_tabs.htmpl
- html_editor_toolbar.htmpl

I

- insert_iss_wf.htmpl
- insert_wf.htmpl
- in_relreq_tab.htmpl
- isscat_auto_assignment_tab.htmpl
- isscat_prptpl_tab.htmpl
- isscat_wftpl_tab.htmpl
- issue_status_change.htmpl
- iss_accumulate.htmpl
- iss_close_all_child.htmpl
- iss_custfld_tab.htmpl
- iss_expedite.htmpl
- iss_lr.htmpl
- iss_reliss_tab.htmpl
- iss_resol_tab.htmpl

K

- kd_action_forward.htmpl
- kd_action_publish.htmpl
- kd_action_reject.htmpl
- kd_action_unpublish.htmpl
- kd_action_unretire.htmpl
- kd_attachments_tab.htmpl

- kd_attributes_tab.htmpl
- kd_categories_tab.htmpl
- kd_content_tab.htmpl
- kd_file_prop_tab.htmpl
- kd_permissions_tab.htmpl
- kd_qa_attributes_tab.htmpl
- kd_qa_content_tab.htmpl
- keit_tmpl_export_fields_tab.htmpl
- keit_tmpl_export_filter_tab.htmpl
- keit_tmpl_import_settings_tab.htmpl
- keit_tmpl_name_tab.htmpl
- kt_admin_attachments.htmpl
- kt_admin_automated_policies.htmpl
- kt_admin_document_settings.htmpl
- kt_admin_faq_options.htmpl
- kt_admin_general_settings.htmpl
- kt_admin_integration.htmpl
- kt_admin_knowledge.htmpl
- kt_admin_parse_settings.htmpl
- kt_admin_report_card.htmpl
- kt_admin_search_config_cr.htmpl
- kt_admin_search_config_iss.htmpl
- kt_admin_search_options.htmpl
- kt_admin_survey_settings.htmpl
- kt_admin_workflow_settings.htmpl
- kt_architect.htmpl
- kt_architect2.htmpl

- kt_architect3.htmpl
- kt_architect_delete_KCAT.htmpl
- kt_architect_delete_KD.htmpl
- kt_architect_frameset.htmpl
- kt_architect_init.htmpl
- kt_architect_javascript.htmpl
- kt_architect_KCATs.htmpl
- kt_architect_KCAT_path.htmpl
- kt_architect_KDs.htmpl
- kt_dtbuilder.htmpl
- kt_dtbuilder2.htmpl
- kt_dtbuilder3.htmpl
- kt_dtbuilder_frameset.htmpl
- kt_dtbuilder_node.htmpl
- kt_dtbuilder_prompt_window.htmpl
- kt_dtbuilder_save_dialog_window.htmpl
- kt_dtbuilder_save_tree_form.htmpl
- kt_dtbuilder_tree.htmpl
- kt_email_document.htmpl
- kt_faq_tree.htmpl
- kt_main.htmpl
- kt_main2.htmpl
- kt_main3.htmpl
- kt_main_role.htmpl
- kt_permissions.htmpl

L

- list.template

- list_acctyp.htmpl
- list_act_type_assoc.htmpl
- list_alg.htmpl
- list_all_fmgrp.htmpl
- list_all_lr.htmpl
- list_architect_KDs.htmpl
- list_architect_KDs_Pref.htmpl
- list_arcpur_hist.htmpl
- list_arcpur_rule.htmpl
- list_atev.htmpl
- list_atomic_cond.htmpl
- list_attmnt.htmpl
- list_attr_alias.htmpl
- list_aty.htmpl
- list_audlog.htmpl
- list_bmcls.htmpl
- list_bmhier.htmpl
- list_bmrep.htmpl
- list_bm_task.htmpl
- list_bool.htmpl
- list_ca_cmpny.htmpl
- list_ca_logical_asset.htmpl
- list_chg.htmpl
- list_chgalg.htmpl
- list_chgcat.htmpl
- list_chgsched.htmpl
- list_chgsched_config.htmpl

- list_chgstat.htmpl
- list_chgtype.htmpl
- list_CI_ACTIONS.htmpl
- list_CI_ACTIONS_ALTERNATE.htmpl
- list_CI_DOC_TEMPLATES.htmpl
- list_CI_STATUSES.htmpl
- list_CI_WF_TEMPLATES.htmpl
- list_cmth.htmpl
- list_cnote.htmpl
- list_cnt.htmpl
- list_cost_cntr.htmpl
- list_country.htmpl
- list_cr.htmpl
- list_crs.htmpl
- list_crsq.htmpl
- list_crs_cr.htmpl
- list_crs_in.htmpl
- list_crs_pr.htmpl
- list_crt.htmpl
- list_cr_kt.htmpl
- list_ctab.htmpl
- list_ctimer.htmpl
- list_ctp.htmpl
- list_dcon.htmpl
- list_dept.htmpl
- list_dmn.htmpl
- list_DOC_VERSIONS.htmpl

- list_EBR_ACRONYMS.htmpl
- list_EBR_LOG.htmpl
- list_EBR_NOISE_WORDS.htmpl
- list_EBR_SYNONYMS_ADM.htmpl
- list_event_log.htmpl
- list_evt.htmpl
- list_evtdly.htmpl
- list_grc.htmpl
- list_grpmem.htmpl
- list_g_chg_queue.htmpl
- list_g_cnt.htmpl
- list_g_cr_queue.htmpl
- list_g_iss_queue.htmpl
- list_g_loc.htmpl
- list_g_org.htmpl
- list_g_prod.htmpl
- list_g_qname.htmpl
- list_g_srvrs.htmpl
- list_g_tblmap.htmpl
- list_g_tblrule.htmpl
- list_g_tenant.htmpl
- list_help_item.htmpl
- list_help_set.htmpl
- list_ical_event_template.htmpl
- list_imp.htmpl
- list_in.htmpl
- list_iss.htmpl

- list_issalg.htmpl
- list_isscat.htmpl
- list_issstat.htmpl
- list_iss_kt.htmpl
- list_iss_wf.htmpl
- list_kc.htmpl
- list_KCAT_LINKED.htmpl
- list_KCAT_QA.htmpl
- list_KCAT_tree.htmpl
- list_KD.htmpl
- list_kdsched.htmpl
- list_kdsched_config.htmpl
- list_KD_ATTMNT.htmpl
- list_kd_CI_DOC_LINKS.htmpl
- list_KD_FILE.htmpl
- list_kd_INDEX_DOC_LINKS.htmpl
- list_KD_QA.htmpl
- list_KEIT_export_transactions.htmpl
- list_KEIT_IMPORT_PACKAGES.htmpl
- list_KEIT_import_transactions.htmpl
- list_KEIT_TEMPLATES.htmpl
- list_KT_ACT_CONTENT.htmpl
- list_KT_BLC.htmpl
- list_KT_FILE_TYPE.htmpl
- list_KT_FLG_TYPE.htmpl
- list_KT_FREE_TEXT.htmpl
- list_KT_LIFE_CYCLE_REP.htmpl

- list_ldap.htmpl
- list_ldap_group.htmpl
- list_loc.htmpl
- list_LONG_TEXTS.htmpl
- list_lr.htmpl
- list_macro.htmpl
- list_macro_type.htmpl
- list_menu_bar.htmpl
- list_menu_tree_name.htmpl
- list_mfrmod.htmpl
- list_mgs.htmpl
- list_mgsalg.htmpl
- list_mgsstat.htmpl
- list_NOTIFICATION.htmpl
- list_no_contract_sdsc.htmpl
- list_nr.htmpl
- list_nrf.htmpl
- list_nr_com.htmpl
- list_ntfl.htmpl
- list_ntfm.htmpl
- list_ntfr.htmpl
- list_OA_TABLES.htmpl
- list_options.htmpl
- list_org.htmpl
- list_O_EVENTS.htmpl
- list_pcat.htmpl
- list_pcat_cr.htmpl

- list_pcat_in.htmpl
- list_pcat_pr.htmpl
- list_perscnt.htmpl
- list_position.htmpl
- list_pr.htmpl
- list_pri.htmpl
- list_prod.htmpl
- list_prod_list.htmpl
- list_prpval.htmpl
- list_prpval_rule.htmpl
- list_QUERY_POLICY.htmpl
- list_QUERY_POLICY_ACTIONS.htmpl
- list_rc.htmpl
- list_rel_cat.htmpl
- list_response.htmpl
- list_role.htmpl
- list_role_tab.htmpl
- list_rptmeth.htmpl
- list_rrf.htmpl
- list_rss.htmpl
- list_sapolicy.htmpl
- list_saprobtyp.htmpl
- list_sdsc.htmpl
- list_sdsc_map.htmpl
- list_seq.htmpl
- list_sev.htmpl

- list_showgrp.htmpl
- list_site.htmpl
- list_srvr_aliases.htmpl
- list_srvr_zones.htmpl
- list_state.htmpl
- list_svc_contract.htmpl
- list_svy_atpl.htmpl
- list_svy_qtpl.htmpl
- list_svy_tpl.htmpl
- list_tab.htmpl
- list_tenant.htmpl
- list_tenant_group.htmpl
- list_tskstat.htmpl
- list_tskty.htmpl
- list_tspan.htmpl
- list_typecnt.htmpl
- list_tz.htmpl
- list_urg.htmpl
- list_usp_servers.htmpl
- list_vpt.htmpl
- list_web_form.htmpl
- list_wf.htmpl
- list_wrkshft.htmpl
- load_properties.htmpl
- load_wait.htmpl
- loc_address_tab.htmpl
- loc_auto_assignment_tab.htmpl

- log_reader.htmpl
- log_reader_banner.htmpl
- log_reader_fs.htmpl
- log_sol_4itil.htmpl

M

- macro_atomic_cond_tab.htmpl
- macro_cnt_tab.htmpl
- macro_ctp_tab.htmpl
- macro_ntfl_tab.htmpl
- macro_rrf_tab.htmpl
- mactyp_exescript_tab.htmpl
- mactyp_valscript_tab.htmpl
- mapped_contracts_tab.htmpl
- menubar.template
- menubar_admin.htmpl
- menubar_architect.htmpl
- menubar_chg_sched.htmpl
- menubar_dtbuilder.htmpl
- menubar_html_editor.htmpl
- menubar_kt.htmpl
- menubar_no.htmpl
- menubar_sd.htmpl
- menubar_sd_chg_manager.htmpl
- menubar_sd_cust_mgr.htmpl
- menubar_sd_cust_rep.htmpl
- menubar_sd_hd_manager.htmpl
- menubar_sd_inc_manager.htmpl

- menubar_sd_know_analyst.htmpl
- menubar_sd_know_manager.htmpl
- menubar_sd_l1_analyst.htmpl
- menubar_sd_l2_analyst.htmpl
- menubar_sd_prb_manager.htmpl
- menubar_sd_vendor_analyst.htmpl
- menu_frames.htmpl
- menu_tree_editor.htmpl
- menu_tree_editor2.htmpl
- menu_tree_editor3.htmpl
- mgs_cnt_tab.htmpl
- mgs_ctp_tab.htmpl
- mgs_ini_tab.htmpl
- mgs_ntfl_tab.htmpl
- mgs_rem_tab.htmpl
- multiframe.template
- multiframe_reports_admin.htmpl
- multiframe_reports_chg_manager.htmpl
- multiframe_reports_cust_mgr.htmpl
- multiframe_reports_inc_mgr.htmpl
- multiframe_reports_know_analyst.htmpl
- multiframe_reports_know_mgr.htmpl
- multiframe_reports_prb_mgr.htmpl
- multiframe_reports_sd_mgr.htmpl

N

- new_lr.htmpl
- nf.htmpl

- nosession.htmpl
- nr_bm_tab.htmpl
- nr_chg_tab.htmpl
- nr_contact_tab.htmpl
- nr_inc_tab.htmpl
- nr_inv_tab.htmpl
- nr_iss_tab.htmpl
- nr_loc_tab.htmpl
- nr_log_tab.htmpl
- nr_org_tab.htmpl
- nr_prb_tab.htmpl
- nr_projex_tab.htmpl
- nr_rel_tab.htmpl
- nr_reqitil_tab.htmpl
- nr_req_tab.htmpl
- nr_serv_tab.htmpl
- ntfl_ntfr_tab.htmpl
- ntfr_aty_tab.htmpl
- ntfr_cnt_tab.htmpl
- ntfr_ctp_tab.htmpl
- ntfr_ntfl_tab.htmpl

O

- order_status_change.htmpl
- org_address_tab.htmpl
- org_env_tab.htmpl

P

- pcat_auto_assignment_tab.htmpl

- pcat_prptpl_tab.htmpl
- pcat_wftpl_tab.htmpl
- power_user_tips.htmpl
- profile_browser.htmpl
- profile_browser2.htmpl
- profile_browser3.htmpl
- profile_browser_frameset.htmpl
- profile_envcnt.htmpl
- profile_envorg.htmpl
- profile_histcnt_chg.htmpl
- profile_histcnt_cr.htmpl
- profile_histcnt_in.htmpl
- profile_histcnt_iss.htmpl
- profile_histcnt_pr.htmpl
- profile_historg_chg.htmpl
- profile_historg_cr.htmpl
- profile_historg_in.htmpl
- profile_historg_iss.htmpl
- profile_historg_pr.htmpl
- profile_infocnt.htmpl
- profile_infoorg.htmpl
- profile_menu.htmpl
- profile_qtemplate.htmpl
- pr_attinc_tab.htmpl
- pr_relreq_tab.htmpl

R

- reports.htmpl

- reports.htmpl.tpl
- request_status_change.htmpl
- role_auth_tab.htmpl
- role_fnacc_tab.htmpl
- role_goform_tab.htmpl
- role_kt_ct_tab.htmpl
- role_kt_docs_tab.htmpl
- role_webform_tab.htmpl
- role_web_interface_tab.htmpl

S

- sapolicy_ac_tab.htmpl
- sapolicy_pt_tab.htmpl
- saprobtyp_dh_tab.htmpl
- saprobtyp_rd_tab.htmpl
- scoreboard.htmpl
- scratchpad.htmpl
- screen_reader_usage.htmpl
- sdsc_chg_slatpl_tab.htmpl
- sdsc_chg_wf_slatpl_tab.htmpl
- sdsc_cr_slatpl_tab.htmpl
- sdsc_iss_slatpl_tab.htmpl
- sdsc_iss_wf_slatpl_tab.htmpl
- sdsc_map_cnt_tab.htmpl
- sdsc_map_grp_tab.htmpl
- sdsc_map_nr_tab.htmpl
- sdsc_map_pri_tab.htmpl
- sdsc_map_urg_tab.htmpl

- sd_kt_admin.htmpl
- sd_main.htmpl
- sd_main_role.htmpl
- search_child_KCATs_filter.htmpl
- show_error.htmpl
- show_main_detail.htmpl
- std_body.htmpl
- std_body_site.htmpl
- std_footer.htmpl
- std_footer_site.htmpl
- std_head.htmpl
- std_head_site.htmpl
- suggest_knowledge_isscat.htmpl
- suggest_knowledge_list_isscat.htmpl
- suggest_knowledge_list_pcat.htmpl
- suggest_knowledge_pcat.htmpl
- sugggest_knowledge_search_options.htmpl

T

- tab_detail.template
- tenant_address_tab.htmpl
- tenant_groups_tab.htmpl
- tenant_group_members_tab.htmpl
- tskty_tskstat_tab.htmpl

U

- update_lrel_bmrep.htmpl
- update_lrel_chg.htmpl
- update_lrel_chgcat.htmpl

- update_lrel_cnt.htmpl
- update_lrel_cr.htmpl
- update_lrel_ctp.htmpl
- update_lrel_goform.htmpl
- update_lrel_help_content.htmpl
- update_lrel_in.htmpl
- update_lrel_iss.htmpl
- update_lrel_isscat.htmpl
- update_lrel_loc.htmpl
- update_lrel_macro.htmpl
- update_lrel_nr.htmpl
- update_lrel_ntfl.htmpl
- update_lrel_ntfr.htmpl
- update_lrel_org.htmpl
- update_lrel_pcat.htmpl
- update_lrel_pr.htmpl
- update_lrel_role.htmpl
- update_lrel_tab.htmpl
- update_lrel_tenant.htmpl
- update_lrel_tenant_group.htmpl
- update_lrel_tskstat.htmpl
- update_lrel_webform.htmpl
- update_lrel_wrkshft.htmpl
- upd_chg_sched.htmpl
- upload_file.htmpl
- upload_success.htmpl
- usq_update.htmpl

- usq_update_control.htmpl
- usq_update_fin.htmpl
- usq_update_select.htmpl
- usq_update_tree.htmpl

V

- v30_date_helper.htmpl

W

- wfdef.htmpl
- wftpl_auto_assignment_tab.htmpl
- wftpl_bhvtpl_tab.htmpl
- working.htmpl
- workitems.htmpl
- wrkshft_auto_assignment_tab.htmpl
- wrkshft_schedule_tab.htmpl
- wspmain.htmpl

X

- xfer_esc_chg.htmpl
- xfer_esc_cr.htmpl
- xfer_esc_iss.htmpl
- xx_attmnt_tab.htmpl
- xx_candp_tab.htmpl
- xx_nr_tab.htmpl
- xx_prop_tab.htmpl
- xx_solnalg_tab.htmpl
- xx_stype_tab.htmpl
- xx_template_tab.htmpl
- xx_wf_tab.htmpl

Contents of the Samples Directory

This article contains the following topics:

You can modify several files in the $NX_ROOT/samples directory for use with various external interfaces. These files are grouped into various subdirectories. None of the files in the samples directory are executable as originally shipped.

How to Modify the Message Catalog

To modify the message catalog, complete the following steps:

1. Refer to the format of pdm.xml that is located in $nx_root\bin.
2. Create a customized copy of pdm.xml and place it in the $nx_root\msg_catalog directory.
3. Add, modify, or add and modify messages in the XML message files from the previous step.

call_mgt

Contains samples for customization in request management.

- **gencr.frg**
  This file can be used in conjunction with bop_cmd to create requests from a command line. All notifications and activity log entries will occur, however no Request Form will display on the server when created. You must use the -u parameter to execute gencr.frg with the bob_cmd utility. Be sure to read the gencr_readme.txt file to learn the syntax, and how to modify it if necessary. The file should be placed in $NX_ROOT/site/mods/interp, if the directory does not exist, you should create it. Example: bop_cmd -d domsrvr -u nsm -f gencr.frg "gencr('My Description')"

- **iss_site.mod**
  This file can be used to enable activity logging of site-adapted fields in issues. This file should be placed in $NX_ROOT/site/mods/majic after it has been changed for the site-adapted fields.

- **cr_site.mod**
  This file can be used to enable activity logging of site-adapted fields in requests. This file should be placed in $NX_ROOT/site/mods/majic after it has been changed for the site-adapted fields.

- **chg_site.mod**
  This file can be used to enable activity logging of site-adapted fields in change orders. This file should be placed in $NX_ROOT/site/mods/majic after it has been changed for the site-adapted fields.

- **gencr_readme.txt**
  This file contains instructions on how to use the gencr.frg file.

- **chg_site.spl**
  This file may be modified to change the mapping of attributes when creating a change order from a request. This file should be placed in $NX_ROOT/site/mods/majic after the appropriate changes have been made.

- **audlog_site.mod**
  This file can be used to enable audit logging of site-adapted fields. This file should be placed in $NX_ROOT/site/mods/majic after it has been changed for the site-adapted fields.

- **Notify_add.spl (UNIX only)**
  This file can be used to add the request's log agent, assignee and group to the request notification list. This file should be placed in $NX_ROOT/site/mods/majic.

- **Notify_replace.spl (UNIX only)**
  This file can be used to add the request's log agent, assignee and group to the request notification list when they are changed. This file should be placed in $NX_ROOT/site/mods/majic.

data

This directory contains files depicting the Logical Data Model for most database tables in CA SDM. This data directory also includes sample data for Knowledge Management.

macro_lock

This file contains a spel fragment that can be run using a bop_cmd to turn off locks that are being held by macros.

multi-tenancy

This directory contains sample files for administering multi-tenancy.

pdmconf

- **web.xml.tpl**
- **pdm_startup.tpl**
- **pdm_edit_usage_notes.htm**
- **alias_install.bat**
- **web.cfg.tpl**
- **pdm_startup.i.tpl**

- **pdm_edit.pl**

- **README_files**
  All of these files are used by pdm_edit.pl to create startup files for a primary server and secondary servers that are configured to run a variety of daemons.

reporting

This directory contains documentation and samples for configuring offline reporting.

sdk

This directory contains a sample file for making CA SDM SOAP web service calls.

TableOfContents.doc further explains what is available, found in the following directory:

$NX_ROOT\samples\sdk\websvc

PKI_loginServiceManaged_JAVA_steps.doc and PKI_loginServiceManaged_PERL_steps.doc explain how to configure ServiceDesk for digital certificate logins in the following directory:

$NX_ROOT\samples\sdk\websvc\java\test1_pki

The following lists PERL and JAVA samples, examples, and locations:

- PERL samples
  $NX_ROOT\samples\sdk\websvc\perl\test1_pki
  Example: loginServiceManaged() web service call

- JAVA samples
  $NX_ROOT\samples\sdk\websvc\java\test1_pki
  Example: loginServiceManaged() and getBopsid() web service call
  $NX_ROOT\samples\sdk\websvc\java\test2_basic
  Example: Combined CreateRequest() and CreateChangeOrder() web service call

views

This directory contains database scripts uses for migration, multi-tenancy administration, and other processes.

Load Supplemental Content - sd_content.dat

Supplemental content for CA SDM is available in sd_content.dat. This data file contains Change Category and Root Cause records. To load the data from a command window, go to $NX_ROOT/data and run the following command:

```
pdm_load  - f sd_content.dat
```

Schema Files Syntax

This article contains the following topics:

The CA SDM database schema is defined in multiple .sch files in the $NX_ROOT/site (UNIX) or *installation-directory*/site (Windows) directory. During configuration, these .sch files along with any customized .sch files you may create are merged together into a single file called $NX_ROOT/site /ddict.sch (UNIX) or *installation-directory*/site/ddict.sch (Windows).

Review Using the Web Screen Painter (see page 1898) prior to making any changes to these files.

Note: Do not modify any .sch files in the $NX_ROOT/site (UNIX) or *installation-directory* /site (Windows) directory. Any changes you make to these files will be lost when upgrading to a new release or when certain patches are applied. If you want to make schema changes, you must create a file in the $NX_ROOT/site/mods (UNIX) or *installation-directory* /site/mods (Windows) directory with the file suffix .sch. Then add your changes to your . sch file, and your changes will then be merged with delivered schema during configuration. This is the only way to preserve your modifications when you upgrade to a new release.

TABLE Statement

Defines the logical tables in the CA SDM database schema and the logical columns (fields) in those tables. These logical tables and columns are then mapped to the physical tables and columns used by your database management system in a mapping statement that follows the TABLE statement.

Note: If you define a new table, you must define a mapping statement for that table. The Mapping Statement (see page 3950) is illustrated at the end of this chapter, followed by an example that combines the TABLE, TABLE_INFO, and mapping statements.

Syntax

TABLE *table_name* {*field value_type field_attributes*; [...]}

Arguments

- **TABLE**
  Introduces the TABLE statement. Must be uppercase. You must have one TABLE statement for each logical table in the schema.

- ***table_name***
  The name of the database table, for example, Call_Req. If adding a database table, you can specify any name beginning with a lowercase letter z. (This avoids possible conflict with existing and future CA SDM table names.) If changing an existing table, find the table in one of the .sch files and use the same name.

- ***field***
  The name of a logical column in the table, for example, id or desc. You must identify each column by name. If adding a table or adding a column to an existing table, you can specify any name beginning with a lowercase letter z; however, field names must not end with the characters "_f." (This avoids possible conflict with existing and future CA SDM column names.) If changing an existing column, find the column in one of the .sch files and use the same name.

- ***value_type***
  The field's data type. Valid values are:

Value	Description
STRING *nn*	A string that is *nn* characters long.
INTEGER	A 32-bit number.
LOCAL_TIME	The number of seconds since January 1, 1970. CA SDM automatically reformats this data type to the designated date format, for example: *mm*/*dd*/*yy hh*:*mm*:*ss*.
DURATION	A period of time, measured in seconds.
REAL	A floating point number
UUID	A 16 byte binary value.

field_attributes

A description of the field. Valid values are:

Value	Description
KEY	Identifies this field as the primary key to be used for identifying records to be updated with pdm_load. This is used if the default primary key, id, is not specified. Must be specified if the field is the primary key in the table.
NOT_NULL	Indicates that the field must contain a value. Must be specified if the field is the primary key in the table. Optional if the field is not the primary key.
REF other_table_name	Indicates that the field references another table. Optional whether the field is the primary key or not.
S_KEY	Optionally identifies this field as the secondary key to be used for identifying records to be updated with pdm_load.
UNIQUE	Indicates that the values in the field must be unique. Must be specified if the field is the primary key in the table. Optional if the field is not the primary key.

Macros are synonyms that will be converted during configuration to the value the macro represents. You can use macros for either data types or attributes. If you wish to use macros, you must add in #include statement to include the file that defines the macro including the path name (usually relative to your schema file). The include statement must be defined prior to using the macro. Example of an include statement:

```
#include "../schema.mac"
```

The following are some of the macros defined in .mac files located in the $ NX_ROOT/site (UNIX) or *installation-directory*/site (Windows) directory.

Data Type	Equivalent
nn	NOT_NULL
uniq	UNIQUE NOT_NULL
ADDR_LINE	STRING 30
EMAILADDR	STRING 120
ENT_DESC	STRING 40
ENT_NAME	STRING 30
OSI_NAME	STRING 80
OSI_TYPE_STRING	STRING 60
USERID	STRING 85
PHONENUM	STRING 32
SYMBOL	STRING 12
HIER_SYM	STRING 60
LONG_SYM	STRING 30
COMMENT	STRING 1000
LONG_STR	STRING 500
LONG_DESC	STRING 240
BOOL	INTEGER

Examples

This TABLE statement in the database schema defines severities. The macro nn indicates that a value is required in the del field. The macro uniq indicates that values are required and must be unique:

```
#include :../schema.mac"
TABLE Severity {
   id        INTEGER uniq KEY;    // key id
   del       INTEGER nn;          // 0=present,1=gone
   sym       SYMBOL uniq S_KEY; // type symbol
   desc      ENT_DESC;            // non-OSI specified column
}
```

This modified TABLE statement makes the Priority field on the Request Detail window required:

```
TABLE Call_Req {priority INTEGER NOT_NULL;}
```

This TABLE statement adds a resolution code field to the Call_Req table. The content of the field is numeric and references the Resolution_Code table. This reference allows users to double-click the Resolution Code field on the Request Detail window to display the values in the Resolution_Code table:

```
TABLE Call_Req {zres_code INTEGER REF Resolution_Code;}
```

TABLE_INFO Statement

This instructs your database management system how to store and index data in the logical tables. The extent to which these instructions are followed depends on the database management system. If no instructions are provided, the database management system follows its own storage and indexing instructions.

Syntax

```
TABLE_INFO table_name {
```

[STORAGE *storage_mtd Field* ;] [INDEX *ndx_props field1* [*field2* ...];] ...}

Arguments

- **TABLE_INFO**
  Introduces the TABLE_INFO statement. Must be uppercase. The TABLE_INFO statement is optional, but if specified, you can have only one TABLE_INFO for each TABLE statement, and it must follow the TABLE statement.

- ***table_name***
  The name of the database table in the TABLE statement.

- **STORAGE *storage_mtd***
  Identifies the storage method. Valid values are listed as follows, but note that some database management systems ignore these values:

Value	Description
BTREE	Indicates to use the balanced tree storage method.
HASH	Indicates to use the hash table storage method. This is valid only if the field is the primary key.
HEAP	Indicates to use the heap storage method.

- ***field***
  Identifies the column that is to be stored according to the specified storage method (STORAGE *storage_mtd*). Must be specified the same way as the name of the column in the TABLE statement.

- **INDEX *ndx_props***
  Identifies one or more properties for an index that consists of the fields specified. Valid values are:

Value	Description
SORT ASCENDING | DESCENDING	Indicates whether to sort the data in the fields in ascending or descending order. Data is sorted in ascending order by default; therefore, only SORT DESCENDING need be specified.
PRIMARY	Indicates to use this index as the default sort order for the table.
CLUSTER	Identifies this as a clustering index.

Value	Description
UNIQUE	Indicates that values in the index must be unique.

- ***field1* [*field2 . . .*]**

Identifies the column or columns that are to be indexed according to the specified index properties (INDEX *ndx_props*). Must be specified the same way as the name of the columns in the TABLE statement.

Examples

This TABLE_INFO statement instructs the database management system to use a hash table to store values in the id field in the Contact_Type table, and to sort the table in descending order according to the values in the sym field. It also indicates that values must be unique:

```
TABLE_INFO Contact_Type {
```

STORAGE HASH id; INDEX SORT DESCENDING PRIMARY UNIQUE sym;}

Mapping Statement

Defines the correspondence between the logical tables and columns in the CA SDM database schema and the physical tables and columns used by your database management system. This statement follows each TABLE statement in a.sch file. You must define it when you define a new table.

Syntax

```
p1 logical_table_name -> CURR_PROV physical_table_name
   [{logical_field -> physical_field ...] ;
```

Arguments

- **p1**
  Introduces the mapping statement. Must be specified as p1.
- ***logical_table_name***
  The name of the database table in the TABLE statement, for example, zManufacturer.
- **CURR_PROV**
  A required keyword.
- ***physical_table_name***
  The name of the table used by your database management system, for example, man. Short names improve performance and are required by some database management systems.
- ***logical_field***
  The name of the column in the CA SDM database schema, for example, desc. Must be the same as *field* in the TABLE statement. Omit this when the logical columns and physical columns have identical names. When omitted, the semicolon follows *physical_table_name*.
- ***physical_field***

The name of the column used by your database management system, for example, nx_desc. Omit this when the logical columns and physical columns have identical names. When omitted, the semicolon follows *physical_table_name*.

Examples

This example illustrates how TABLE, mapping (p1), and TABLE_INFO statements define a zManufacturer table:

```
TABLE zManufacturer {
        id       INTEGER  uniq KEY;       // key id
        del      INTEGER  nn;             // 0=present,1=gone
        sym      HIER_SYM uniq S_KEY;     // manufacturer name
        desc     ENT_DESC;                // manufacturer description
}

p1 zManufacturer -> CURR_PROV man   // maps logical table "zManufacturer"
{                                   // to physical table "man"
        desc -> nx_desc;            // maps logical column "desc"
}                                   // to physical column "nx_desc"

TABLE_INFO zManufacturer {
```

STORAGE HASH id; INDEX SORT ASCENDING PRIMARY UNIQUE sym;}

Object Definition Syntax

This article contains the following topics:

Many of the components of CA SDM consist of business objects. These objects are defined in a metalanguage named Majic. You can use Majic statements to create new objects and modify existing objects, thus customizing these objects to meet your needs.

Directories

The Majic files are organized in two directories:

Directory	Description
bopcfg/majic (UNIX) or bopcfg\majic (Windows)	Contains the .maj files that have been used to create windows defined in the database. These files should not be changed because changes will be overwritten by new releases of CA SDM.
site/mods/majic (UNIX) or site\mods\majic (Windows)	Contains the .mod files you use to customize windows.

Types of Statements

The following Majic statements are used in screen painter and database customization procedures.

Statement	Description
OBJECT	Defines a business object
MODIFY	Changes existing object attributes
MODIFY FACTORY	Changes existing factories

MODIFY Statement

Changes the way attributes are defined on OBJECT statements. MODIFY statements are read after OBJECT statements.

Syntax

```
MODIFY obj_name att_name [status_type;]
   [ON_NEW DEFAULT|SET value|NOW ;]|
   [ON_CI DEFAULT|SET value|NOW ;]|
   [ON_DB_INIT DEFAULT|SET value|NOW ;]
```

Arguments

- ***obj_name***
  Identifies the object whose attribute is being modified.
- ***att_name***
  Identifies the attribute being modified.
- ***status_type***
  Modifies the properties of the attribute to allow or prohibit null values. There are two valid options for this keyword:
  - **REQUIRED**
    Indicates that the attribute is required.
  - **NOT_REQUIRED**
    Indicates that the attribute is not required.
- **ON Statements**
  See ON Statements for a description of these statements.

Example

The following example changes the salary attribute in the emp object so that it is now a required attribute:

```
MODIFY emp salary REQUIRED;
```

Example

The following example changes the address2 attribute in the emp object so that is now not required.

```
MODIFY emp address2 NOT_REQUIRED;
```

MODIFY FACTORY Statement

Changes the way factories are defined on OBJECT statements. MODIFY statements are read after OBJECT statements.

Syntax

```
MODIFY FACTORY fac_name {
   [FUNCTION_GROUP name ;]
   [DISPLAY_NAME name ;]
   [STANDARD_LISTS {
       [SORT_BY index_att ;]
       [FETCH fetch_att ;]
       [WHERE string ;]
       [MLIST ON|OFF;]
       [RLIST ON|OFF;] } ;] };
```

Arguments

- ***fac_name***
  Identifies the factory, if included on the original OBJECT statement.

Optional Statements

At least one of these optional statements must be specified.

- **FUNCTION_GROUP *name***
  Indicates which security access groups are permitted to access the object. For example:

  ```
  FUNCTION_GROUP "admin" ;
  ```

- **DISPLAY_NAME name**
  Defines an external name for the table.
  DISPLAY_NAME "Call Request" ;

- **STANDARD_LISTS**
  Creates lists of objects that are kept in a cache. The parameters determine whether the lists are master lists or restricted lists, whether the objects included in the list must meet specified conditions, and how the lists can be sorted. Refer STANDARD_LISTS Optional Statements for a description of the syntax.

OBJECT Statement

Defines a business object.

Syntax

```
OBJECT obj_name {
```

```
    [ATTRIBUTES [table_name]{
        att_name [field_name] value_type [access_type[status_type]][DISPLAY_NAME
string][{
            [ON_NEW DEFAULT|SET value|NOW ;]
            [ON_CI DEFAULT|SET value|NOW ;]
            [ON_DB_INIT DEFAULT|SET value|NOW ;]} ;]};]


    [FACTORY [fac_name]{
        [REL_ATTR name ;]
        [COMMON_NAME name ;]
     [DISPLAY_NAME name ;]
        [FUNCTION_GROUP name ;]
        [STANDARD_LISTS {
           [SORT_BY index_att ;]
           [FETCH fetch_att ;]
           [WHERE string ;]
           [MLIST ON|OFF;]
           [RLIST ON|OFF;] } ;]};]
};
```

Arguments

- ***obj_name***
  The object's name (for example, cnt for contact or cr for request).

Optional Statements

Either ATTRIBUTES or FACTORY must be specified. Both can be specified.

- **ATTRIBUTES [*table_name*] { }**
  Defines the properties of the object. Most attributes map to a field (column) in a database table. The ATTRIBUTES Optional Statement describes its syntax.

- **FACTORY [*fac_name*] { }**
  Defines access to the object, like its relation attribute, a common name, the security group that can access it, the type of lists produced, and how those lists can be sorted. The FACTORY Optional Statement describes its syntax.

Example

This example defines an object named ctp. The ATTRIBUTES statement defines attributes named sym, delete_flag, and description whose values are stored in the Contact_Type table in the database. The FACTORY statement creates a master list of objects, sorted by values in the field that corresponds to the sym attribute, and specifies that the id attribute will represent ctp when it is referenced by an SREL:

```
OBJECT ctp {
   ATTRIBUTES Contact_Type {
       sym                STRING REQUIRED ;
       delete_flag del    INTEGER {
          ON_NEW DEFAULT 0 ;
       } ;
```

```
        description desc    STRING ;
    } ;
    FACTORY {
        STANDARD_LISTS {SORT_BY "sym"} ;
        REL_ATTR  id ;
    };
};
```

STANDARD_LISTS Optional Statement

This article contains the following topics:

The optional statement on the FACTORY statement that defines the object's standard lists.

Syntax (STANDARD_LISTS Optional Statement)

```
STANDARD_LISTS {
    [SORT_BY index_att ;]
    [FETCH fetch_att ;]
    [WHERE string ;]
    [MLIST ON|OFF;]
    [RLIST ON|OFF;] } ;
```

Optional Statements (STANDARD_LISTS Optional Statement)

At least one of these optional statements must be specified:

- **SORT_BY *index_att***
  Defines the attributes that can be used to sort the standard lists. If specified, a master list is produced. Attributes must be enclosed in quotes and separated by commas. When displayed in a list or select window, the list is sorted by the first attribute, by default. For example:

  ```
  SORT_BY "sym, code" ;
  ```

- **FETCH *fetch_att***
  Specifies additional attributes to keep in the cache, besides those used to sort the list. They must be enclosed in quotes and separated by commas. For example:

  ```
  FETCH "description" ;
  ```

- **WHERE *string***
  Specifies a condition, in SQL format and surrounded by quotes, that must be met for an object to be included in a restricted list. If specified, a restricted list is produced. This example specifies that the restricted list contain only records that were not deleted:

  ```
  WHERE "delete_flag = 0" ;
  ```

- **MLIST ON|OFF**
  Indicates whether to produce a master list, which includes all objects, using one of the following values:

Value	Description
ON	Produces a master list (default if SORT_BY is specified)
OFF	Does not produce a master list (default if SORT_BY is not specified or has no value defined)

Note: CA SDM web engine only uses the MLIST to populate the data in the web forms. MLIST is created on the domsrvr cache.

- **RLIST ON|OFF**
  Indicates whether to also produce a restricted list, which includes only the objects that meet the criteria in the WHERE clause, using one of the following values:

Value	Description
ON	Produces a restricted list (default if WHERE is specified)
OFF	Does not produce a restricted list (default if WHERE is not specified or has no value defined.)

Note: RLISTs can speed up access and display but they use memory. They are usually used in select windows.

Important! MLIST OFF must be specified if you specify RLIST OFF.

Example (STANDARD_LISTS Optional Statement)

This example provides both a master list and a restricted list. Both lists contain the values defined for the sym, code, and description attributes. The records in the list can be sorted according to the values in the sym and code attributes. The restricted list contains only records that were not deleted:

```
STANDARD_LISTS {
    SORT_BY "sym,code" ;
    FETCH "description" ;
    WHERE "delete_flag = 0" ;
};
```

The STANDARD_LISTS statement alone does not necessarily create entries that are listed in a dropdown field. To create the dropdown list in a web interface form, you need to customize the statement.

FACTORY Optional Statement

This article contains the following topics:

Defines access to the object, like its relation attribute, a common name, the security group that can access it, the type of lists produced, and how those lists can be sorted. If omitted, the object is treated according to default specifications.

Syntax (FACTORY Optional Statement)

```
FACTORY [fac_name]{
   [REL_ATTR name ;]
   [COMMON_NAME name ;]
   [FUNCTION_GROUP name ;]
   [DISPLAY_NAME name ;]
   [STANDARD_LISTS {
       [SORT_BY index_att ;]
       [FETCH fetch_att ;]
       [WHERE string ;]
       [MLIST ON|OFF;]
       [RLIST ON|OFF;] } ;]
};
```

Arguments (FACTORY Optional Statement)

- ***fac_name***
  The name of the factory that initiates the object. Specify this only if it is different from the name of the object. For example, the cnt object has four factories: cnt, cst, agt, grp.

Optional Statements (FACTORY Optional Statement)

At least one of these optional statements must be specified:

- **REL_ATTR *name***
  Identifies the attribute that will represent this object when it is referenced (used as an SREL) by another object. Here is an example:

  ```
  REL_ATTR id ;
  ```

- **REL_ATTR name, srel_name (attr1,attr2,...)**
  Identifies the attributes that will represent this object when it is referenced (used as an “named” SREL) by another object. where

  - **srel_name**
    matches the "named" SREL name

- **attr1**
  is mapped to by the first attribute in the "named" SREL attribute list.

- **attr2**
  is mapped to by the second attribute in the "named" SREL attribute list.

- DISPLAY_NAME name
  Defines an external name for the table.
  DISPLAY_NAME "Call Request" ;

- **COMMON_NAME *name***
  Defines the attribute to be displayed in drop-down lists or when the user double-clicks a field, as well as when the tag does not specify a complete attribute. In the first example, the value for sym appears on the window instead of the value for the REL_ATTR. The second example allows you to specify a tag as cr.customer instead of cr.customer.combo_name.

```
COMMON_NAME sym ;

COMMON_NAME combo_name ;
```

- **FUNCTION_GROUP *name***
  Indicates which security access group is permitted to access the object. For example:

```
FUNCTION_GROUP "admin" ;
```

- **STANDARD_LISTS { }**
  Creates lists of objects that are kept in a cache and can be displayed on list or select windows. The parameters determine whether the lists are master lists or restricted lists, whether the objects included in the list must meet specified conditions, how the lists can be sorted, and what additional attributes are stored. Refer STANDARD_LISTS Optional Statement (see page 3955) for the description of the syntax.

Example (FACTORY Optional Statement)

This example defines access to the object. A master list is produced. It can be sorted according to the values in the object's sym and code attributes. When first displayed, it is sorted according to the values in the sym attribute by default. When referenced by another object, this object is represented by the code attribute. When displayed in a window, the value for sym appears instead of the value for code. Only users in the admin security group can accessed it:

```
FACTORY {
    STANDARD_LISTS {SORT_BY "sym,code"} ;
    REL_ATTR code ;
    COMMON_NAME sym ;
    FUNCTION_GROUP "admin" ;
};
```

ATTRIBUTES Optional Statement

The optional statement on the OBJECT statement that defines the properties of the object.

Syntax

```
ATTRIBUTES [table_name]{
   att_name [field_name] value_type [access_type[status_type][DISPLAY_NAME string]]{
       [ON_NEW DEFAULT|SET value|NOW ;]
       [ON_CI DEFAULT|SET value|NOW ;]
    [ON_DB_INIT DEFAULT|SET value|NOW ;];]};]
```

Arguments

- ***table_name***
  The name of the table in the database that stores the values associated with the attributes in the object. If the table name is not specified, the *obj_name* in the OBJECT statement is used.

- ***att_name***
  The name of the attribute. Each attribute usually maps to a field (column) in the database table.

- ***field_name***
  The name of the field in the database table or LOCAL if the attribute does not map to a field or DERIVED (derived-expr) if the attribute is derived from other attributes. If neither LOCAL, DERIVED nor a field name is specified, the name of the field is assumed to be the same as the name of the attribute.
  A variable declared as DERIVED is constructed only when its value is retrieved. The operand of DERIVED contains a list of attribute names and string constants separated by spaces. All attributes in a derived value must be simple values (that is, they cannot be xRELs), and should be declared prior to the derived variable. The derived attribute's value is the concatenation of the values of its constituent values.
  String constants within a derived expression may contain references to environment variables in the one of the forms:
  ${var}
  ${var#pattern}
  ${var#pattern#replacement}
  Such specifications are replaced with the value of the environment variable at domsrvr startup time. The #pattern operand is optional. If provided, it is treated as a regular expression, and replaced wherever it appears in the environment variable's value. The #replacement operand defaults to null if not specified. Because # is a fixed delimeter, the pattern cannot contain a # symbol. There are no restrictions on the use of derived attributes in other messages. They behave in same way as standard attributes. A hotlink for a derived attribute fires whenever any of the attributes from which it is built changes.

- ***value_type***
  Identifies the data type of the attribute’s value as:

  - INTEGER
  - DOUBLE
  - STRING [*length*]
  - DURATION
  - UUID
  - DATE

- SREL *obj2_name*
- SREL { ob2_name_name srel_name (name, name2, ...) }

If STRING is specified, the size can be specified in an integer following STRING. If no size is specified, the value in the database is used.
UUID is 16 bytes of binary data that is used as a unique identifier for certain database records.
SREL refers the attribute to another object. If SREL is specified, *obj2_name* must be specified to identify the object that the attribute refers to.
srel_name specifies a "named" SREL. Like a "simple" SREL, a "named" is a type of MAJIC OBJECT attribute that represents a single relation, which uniquely identifies a row in another table (ob2_name). A "simple" SREL attribute normally maps to the "id" field in another table, however a "named" SREL maps two or more attributes (name, name2, …) to two or more attributes in the referenced table that uniquely identify a row in the referenced table.

- ***access_type***
  Defines access to the attribute. Valid values are:

Value	Description
CONST	Cannot be changed
PRIVATE	Read-only
PUBLIC	Read/write access (the default)
WRITE_NEW	Can be written only when the object is created, before the object is saved

- ***status_type***
  Indicates the status of the attribute as:
  - REQUIRED
  - NOT_REQUIRED (the default)
- **DISPLAY_NAME string**
  Specifies a string to be used in place of the attribute name in messages concerning this attribute, such as"required attribute missing"

ON Statements

Use one of these only when *value_type* is INTEGER, STRING, DATE, or SREL.

- **ON_NEW DEFAULT|SET *value*|NOW**
  Indicates to set the value of an attribute when the object is being created for the first time:

Value	Description
DEFAULT	Changes a null current value to *value* or NOW.
SET	Changes any current value to *value* or NOW.
value	Specifies a numeric value or a string value, depending on the data type of the attribute.
NOW	Specify this if the attribute is of type DATE; it sets the attribute to the current date and time.

In the following example, 90 is the value set as a default when the object is created:

```
ON_NEW DEFAULT 90 ;
```

- **ON_CI DEFAULT|SET *value*|NOW**
  Indicates to set the value of an attribute when the attribute is being checked into the database. See the description of each parameter for ON_NEW.

- **ON_DB_INIT DEFAULT|SET *value*|NOW**
  Indicates to set the value of an attribute when the attribute is being instantiated from the database. See the description of each parameter for ON_NEW.

Example

This example defines attributes with names like start_date whose values are stored in fields like nlh_start in the Notify_Log_Header table in the database. The field names are followed by each attribute's data type. Optional parameters define access to some of the attributes, indicate that the attribute is required, and tell when to set the value of some of the attributes to the current date and time.

For example, an attribute named last_mod is defined; its value is set to the current date and time when the attribute is checked into the database. An attribute named contact is also defined; its value is a single relation stored in database field nlh_c_addressee. The object referred to is cnt:

```
ATTRIBUTES Notify_Log_Header {
   start_date          nlh_start          DATE WRITE_NEW {ON_NEW DEFAULT NOW;} ;
   last_mod                               DATE {ON_CI SET NOW ;} ;
   msg_hdr             nlh_hdr            STRING 20 WRITE_NEW ;
   msg_text            nlh_msg            STRING WRITE_NEW ;
   msg_ack             nlh_user_ack       STRING ;
   contact             nlh_c_addressee    SREL cnt WRITE_NEW ;
   notify_method       nlh_cm_method      INTEGER WRITE_NEW ;
   activity_notify     nlh_transition     INTEGER WRITE_NEW ;
   pri_event           nlh_pri            INTEGER WRITE_NEW ;
   notify_type         nlh_type           INTEGER WRITE_NEW ;
   ack_time            nlh_ack_time       DURATION ;
   status              nlh_status         INTEGER REQUIRED ;
   end_date            nlh_end            DATE {ON_NEW DEFAULT NOW ;} ;

};
```

Where Clauses

This article contains the following topics:

Several Web Services methods, such as doSelect() and doQuery(), require *the Where clauses* for searching by CA SDM and Knowledge Management. A Where clause is the string appearing after the 'WHERE' keyword in an SQL statement. For example, a where clause to find contacts (the 'cnt' object) by last name:

```
last_name = 'Jones'
```

or

```
last_name LIKE 'Jone%'
```

The second example finds all contacts with names beginning with ‘Jone’, while the first just finds the Jones’.

CA SDM supports only a subset of the standard SQL parameters for where clauses, and are listed as follows:

- Logical operators AND, OR, and NOT
- LIKE and IS
- NULL
- IN
- Wildcard characters ‘%’ and ‘_’ for string matches
- All comparison operators: <, >, <=, >=, !=, <>

Note: Parenthesis is used for grouping. Explicit joins, EXISTS, and GROUP BY elements are not supported by CA SDM. String value must be enclosed in quotes, for example, ‘Jones’.

The column names denote the object attribute names. CA SDM data types,data and duration, are treated as integers. For example:

```
creation_date > 38473489389
```

Note: You must use the attribute names at the object Level. Do not use the actual DBMS column names.

Dot-notation is allowed in the Where clause to search through SREL (foreign key) types. For example, a query against the Request (‘cr’) object, returns all Requests assigned to contacts with a specific last name, as illustrated by the following example:

```
assignee.last_name like 'Martin%'
```

Dot-notation is very helpful in forming the where clauses, but you must ensure that the query is an efficient one. The query in the example *assignee.last_name like 'Martin%'* can be inefficient if the contact’s last_name attribute is not indexed in the DBMS. To ensure indexes are used to their best advantage when searching through SRELs, make use of the ID attributes of the CA SDM objects. All tables in CA SDM have an index on the ID attribute.

The ID attribute of an object can be easily obtained from the object's handle. An object's handle is a string of the form "<*objectName*>:<*id*>", where <*id*> is the value of the ID attribute found in every CA SDM object. Extract the ID portion and use "<attributeName>.id" in the Where clause.

An object's ID is either an integer or a UUID. If it is an integer, simply use it as such. For example, to search for Requests with the *rootcause* pointing to a Root Cause object with handle, "*rc:1234*", the Where clause is:

```
rootcause.id = 1234
```

If the ID attribute of an object is a UUID type, you must format it as:

```
U'<uuid>'
```

The string representation of a UUID is enclosed in single quotes and prefixed with capital 'U'. This string is the <id> part of an object handle. For example, if you know that the handle for a particular contact is cnt:913B485771E1B347968E530276916387, you can form the query as:

```
assignee.id = U'913B485771E1B347968E530276916387'
```

Do not form the Where clauses by querying the 'persistent_id' attribute, as in the following example:

```
rootcause.persistent_id = 'rc:1234'
```

For more information about handles, see Default Handles (see page 1855).

IN Clause

The IN clause requires some special explanation. The two syntactic forms are:

```
SREL_attr_name.subq_WHERE_attr[.attr] IN ( value1 [, value2 [,...]] )
SREL_attr_name.[subq_SELECT_attr]LIST_name.subq_WHERE_attr IN (value1, [,value2
[,...]] )
```

The left side of the clause must begin with an SREL-type attribute of the table being queried, which is represented by *SREL_attr_name*. *subq_WHERE_attr* is an attribute of the foreign object, which itself may be another SREL pointer.

For example, a query against the request ('cr') object may be coded as follows:

```
category.sym IN ('Soft%', 'Email')
```

This translates to the following pseudo-SQL:

```
SELECT ... FROM cr WHERE cr.category IN (SELECT persistent_id FROM pcat WHERE sym
LIKE 'Soft%' OR sym = 'Email')
```

In the previous sub query , 'pcat' is the object name pointed to by cr.category.

The second form of the IN clause can search through BREL lists. For example, to find all requests assigned to an analyst in a specific group, the clause is as follows:

```
assignee.[member]group_list.group IN (U'913B485771E1B347968E530276916387')
```

The first part of the clause, assignee, is an SREL (foreign key) of the cr object, pointing to the cnt object. Next, group_list, which is an attribute of the cnt object, is a list of cnt objects that represent groups to which a contact belongs. The last part, group, forms the first part of the where clause for the IN sub query. ‘U’913B485771E1B347968E530276916387is the foreign key value to match on group. The sub query return is specified by [member]. This translates to the following pseudo-SQL statement:

```
SELECT ... FROM cr WHERE cr.assignee IN (SELECT member from grpmem WHERE group =
U'913B485771E1B347968E530276916387')
```

You can specify multiple foreign keys for matching multiple objects by providing a comma-separated list:

```
assignee.[member]group_list.group IN (U'913B485771E1B347968E530276916387',
U'913B485771E1B347968E530276916300')
```

You cannot extend the dot notation for this use of the IN clause, for example, the following is not valid:

```
assignee.[member]group_list.group.last_name IN ('Account Center')
```

One use of IN is to avoid Cartesian products. For example, the following query results in a Cartesian product and is very inefficient:

```
assignee.last_name LIKE 'MIS%' OR group.last_name LIKE 'MIS%'
```

Using IN, the query can be coded as follows:

```
assignee.last_name IN 'MIS%' OR group.last_name IN 'MIS%'
```

This query does not create a Cartesian product; in fact, it creates no joins at all.

Note: The parentheses that normally enclose the list of values on the right side of IN can be omitted if there is only one value in the list. Similarly, you should avoid joins by converting queries.

```
assignee.last_name LIKE 'Smith'
```

to:

```
assignee = U'913B485771E1B347968E530276916387'
```

This avoids the join with some loss in clarity. Using IN, the same partition can be written as follows, with the clarity of the first version and almost the same efficiency as the second version:

```
assignee.last_name IN 'Smith'
```

The ‘NOT’ keyword cannot be in conjunction with IN, for example, “NOT IN”.

Lists

Some Web Services methods return *lists*, represented by a unique integer handle. A list is simply a collection of same-type objects. Lists are especially useful when dealing with a large collection of objects (for example, all the contacts in the system) because you can retrieve information about items in a range of the list. The disadvantage is that you must make more method calls to obtain a list handle, retrieve information, and finally, free the list handle. If the expected number of list rows is small, use methods that do not involve list handles, such as doSelect().

The following describes more details about lists:

- **Lists are homogenous**
  List may only contain objects of a single type, for example, lists of contacts, list of organizations, and so on.

- **Lists are Static**
  For example, if a list object is obtained for all contacts and another contact is added to the system, the update is not reflected in the list. Another list handle must be obtained to get the most current data.

- **List Handles**
  A request for a list returns an integer handle representing the list of same-type objects. No other information is sent to the client. The client may query the list for specific information about its rows. When a client is finished with a list, the handle must be released with freeListHandles(). The CA SDM server maintains the list, consuming system resources. Therefore, it is important to free lists. Unlike object handles, list handles are not persistent across sessions.

- **Integer Index**
  Several methods require an integer index into a list. Lists are zero-based so the first element is at index = 0.

As previously mentioned, using list handles is most useful for larger sets of data that may be queried multiple times. For some operations, however, lists are excessive. Several methods are provided, but the most notable is doSelect(), as it returns requested information about a set of data without the overhead of list handles.

The decision to use list handles versus methods, such as doSelect(), is one of performance and convenience. For example, suppose your application does processing on all 15,000 Contacts in your system. The doSelect() method can retrieve all the contact data in one call, but the reply will be delayed and will negatively impact overall system performance while it assembles and returns a very large data set. The doQuery() method, in this case, will return a list reference very quickly. Ranges of data can be queried from the list to improve response times from the server. A good practice to follow is to use list references if the data set exceeds 250 items.

Sometimes it does not make sense to use list handles. For example, an issue has a list of Activity Logs. Depending on the installation, the number of logs can range from a few to several dozen. It is probably faster to request the data all at once instead of requesting a list reference, querying it for data, and then releasing the list.

Examples of methods that return data sets instead of list references include the following:

- doSelect()

- getRelatedListValues()
- getLrelValues()
- getTaskListValues()
- getValidTaskTransitions()

As previously stated, queries that return a large number of rows can severely impact the performance of the server. To protect against this, CA SDM limits the number of rows returned to 250. This affects all CA SDM Web Services methods that return lists of objects, including the following:

- doSelect()
- doSelectKD()
- getGroupMemberListValues()
- getListValues()
- getPropertyInfoForCategory()
- getRelatedListValues()
- getTaskListValues()
- getValidTaskTransitions()

This limit applies even if you request one of these methods to retrieve more than 250 rows.

To retrieve large numbers of rows, you should obtain a handle to the list of results and use getListValues() to retrieve chunks of 250 or fewer rows each. This strategy helps keep the server from becoming slow while serving huge amounts of data.

Attribute Data Types

This article contains the following topics:

Each attribute of an object is of a specific type that has meaning to the CA SDM application, such as string, date, or integer. Knowing the attribute type is essential to correctly retrieving and updating attribute values.

The CA SDM uses an enumeration to identify each data type. These enumeration values are returned in various web methods, as illustrated by the following table:

Data Type	Value
Integer	**2001**
String	**2002**
Duration	2003
Date	2004
SREL	2005
UNKNOWN	2006
List (QREL/BREL)	2007
Lrel (many-to-many)	2008
UUID	2009

Integer

The Integer data type represents a 32-bit signed integer. Null an integer attribute by passing the empty string.

String

The String data type represents a character string, where the maximum length is defined by the database storage allocated for a particular string attribute.

If you attempt to set a string attribute to a value that exceeds its length, the value is truncated and an error message is written to the CA SDM log.

Duration

The Duration data type is an integer representing time duration in seconds. For example, “90” represents one minute and 30 seconds. To set a duration type, use an integer representing the number of seconds for the duration. Negative values are not permitted. To make a duration attribute null, pass the empty string.

Date

The Date data type represents a date value. This is stored as a UNIX-like UTC value in the database (the number of seconds since 1-1-1970). When retrieving date values, the integer UTC is returned. Similarly, use a UTC value to set a date. Negative values are not permitted. Null a date attribute by passing the empty string.

SREL

The SREL data type represents an SREL (Single RELation), which is a pointer to another object. It is a foreign key to another table in a database. For example, an Issue object has a pointer attribute to a Contact representing the Assignee.

Most CA SDM Web Services methods permit dot-notation to retrieve information about objects to which an SREL points. For example, to specify the name of a Contact's organization from the context of the Contact, use the following:

```
organization.name
```

You may expand to an arbitrary number of levels as shown in the following example:

```
organization.contact.first_name
```

Dot-notation can only be used to retrieve attribute values, such as using getObjectValues(), or in a Where clause. You cannot use dot-notation to set values.

To set an SREL attribute, such as with updateObject(), you can pass the persistent id of the object to which you want to point. In order to simplify this action, this release of CA SDM has been enhanced so that the REL_ATTR (foreign key) value may be used to set an SREL.

For example, as the REL_ATTR of the crt object (Request Type) is its code attribute, the values "R", "I" and "P" can be used to set the type attribute of a cr object to specify that the ticket is a Request, Incident or Problem. The cr's type attribute can be set to "R" instead of "crt:180", "I" instead of "crt: 182" and "P" instead of "crt:181".

To set an SREL attribute to null, pass the empty string ("").

List (QREL/BREL)

An object can have a list attribute that represents a one-to-many relationship. These are defined in majic files with the QREL or BREL keywords. A list exists at the object level -- it does not take any additional storage in the DBMS.

The CA SDM system handles list collections as abstract data types. The Web Services provides several methods to interact with lists -- for references and queries to lists defined in an object, use getRelatedList() and getRelatedListValues(). For more information about lists, see CA SDM Lists in this chapter.

LREL

The LREL data type represents a many-to-many relationship between two object types. An LREL has two names, one for each side of the relationship. The CA SDM Web Services provides special functions for interacting with LRELs.

UNKNOWN

The Unknown data type represents an unknown data type.

UUID

A UUID is a 128-bit integer (16 bytes) or a 32-byte character that can be used across all computers and networks wherever a unique identifier is required. Such an identifier has a very low probability of being duplicated (for example, a contact ID). UUIDs are used mostly with primary keys.

Web Services Methods

This article contains the following topics:

This section provides the details for using the Web Services methods. Each method explains the parameters, description, and returns.

Web Services Method Summary

The following table provides a summary of web services methods in the product:

Method Name (Input Parameters)	Return Type [XML Root Element]	Output Parameters (Type: StringHolder) [XML Root Element]	Description
addAssetLog (int sid, String assetHandle, String contactHandle, String logText)	void		Adds a new log entry to an asset.
addBookmark (int sid, String contactId, int docId)	String [UDSObject]		Adds a bookmark to a knowledge document.
addComment (int sid, String comment, int docId, String email, String username, String contactId)	String [UDSObject]		Adds a comment to a knowledge document.
addMemberToGroup (int sid, String contactHandle, String groupHandle)	void		Adds a contact to a group.
attachChangeToRequest (int sid, String creator, String requestHandle, String changeHandle, ArrayOfString changeAttrVals, String description)	String		Attaches a new or existing change order to a request.
attachURLLink (int sid, int docId, String url, String attmntName, String description)	int		Attaches a URL link to a knowledge document.
attmntFolderLinkCount (int sid, int folderId)	int		Returns the number of attachment links for a folder.
callServerMethod (int sid, String methodName, String factoryName, String formatList, ArrayOfString parameters)	String [ServerReturn]		Invokes any arbitrary server-side method.
changeStatus (int sid, String creator, String objectHandle, String description, String newStatusHandle)			

Method Name (Input Parameters)	Return Type [XML Root Element]	Output Parameters (Type: StringHolder) [XML Root Element]	Description
	String [UDSObject (Handle only)]		Performs an update status activity on a ticket.
clearNotification (int sid, String lrObject, String clearBy)	int		Clears a notification message.
closeTicket (int sid, String description, String ticketHandle)	String [UDSObject (Handle only)]		Sets the status of the ticket to Closed.
createActivityLog (int sid, String creator, String objectHandle, String description, String logType, int timeSpent, boolean internal)	String [UDSObject (Handle only)]		Creates an activity log entry for a ticket.
createAsset (int sid, ArrayOfString attrVals, ArrayOfString attributes, StringHolder createAssetResult, StringHolder newAssetHandle, StringHolder newExtensionHandle, StringHolder newExtensionName)	void	createAssetResult [UDSObject] newAssetHandle newExtensionHandle newExtensionName	Creates a configuration item (asset).
createAssetParentChildRelationship (int sid, String parentHandle, String childHandle)	String		Creates an asset parent-child relationship.
createAttachment (int sid, String repositoryHandle, String objectHandle, String description, String fileName)	String		Uploads a file to the back-end server and attaches it to a ticket.
createAttmnt (int sid, String repositoryHandle, int folderId, int objectHandle, String description, String fileName)	String		Uploads a file to the back-end server and attaches it to a knowledge document.
			Creates a Change Order ticket.

Method Name (Input Parameters)	Return Type [XML Root Element]	Output Parameters (Type: StringHolder) [XML Root Element]	Description
createChangeOrder (int sid, String creatorHandle, ArrayOfString attrVals, ArrayOfString propertyValues, String template, ArrayOfString attributes, StringHolder newChangeHandle, StringHolder newChangeNumber)	String [UDSObject]	newChangeHandle newChangeNumber	
createDocument (int sid, ArrayOfString kdAttributes)	String [UDSObjectList]		Creates a knowledge document.
createFolder (int sid, int parentFolderId, int repId, int folderType, String description, String folderName)	String [UDSObject]		Creates a folder in an attachment repository.
createIssue (int sid, String creatorHandle, ArrayOfString attrVals, ArrayOfString propertyValues, String template, ArrayOfString attributes, StringHolder newIssueHandle, StringHolder newIssueNumber)	String [UDSObject]	newIssueHandle newIssueNumber	Creates an Issue ticket.
createLrelRelationships (int sid, String contextObject, String lrelName, ArrayOfString addObjectHandles)	void		Adds one or more many-to-many relationships.
createObject (int sid, String objectType, ArrayOfString attrVals, ArrayOfString attributes, StringHolder createObjectResult, StringHolder newHandle)	void	createObjectResult [UDSObject] newHandle	Creates any CA SDM object.
createQuickTicket (int sid, String customerHandle, String description, StringHolder newTicketHandle, StringHolder newTicketNumber)	String [UDSObject]	newTicketHandle newTicketNumber	Creates a ticket based on the preferred document type of the given end user.
createRequest (int sid, String creatorHandle, ArrayOfString attrVals, ArrayOfString propertyValues, String template, ArrayOfString attributes, StringHolder newRequestHandle, StringHolder newRequestNumber)	String [UDSObject]	newRequestHandle newRequestNumber	Creates a Request ticket.
createTicket (int sid, String description, String problem_type, String userid, String asset, String duplication_id, StringHolder newTicketHandle, StringHolder newTicketNumber, StringHolder returnUserData, StringHolder returnApplicationData)	String [UDSObject (empty)]	newTicketHandle newTicketNumber returnUserData returnApplicationData	Creates a ticket based on the rules defined in the Service Aware Policy and the given Problem Type.
	void		

Method Name (Input Parameters)	Return Type [XML Root Element]	Output Parameters (Type: StringHolder) [XML Root Element]	Description
createWorkFlowTask (int sid, ArrayOfString attrVals, String objectHandle, String creatorHandle, String selectedWorkFlow, String taskType, ArrayOfString attributes, StringHolder createWorkFlowTaskResult, StringHolder newHandle)		createWorkFlowTaskResult [UDSObject] newHandle	Creates Workflow Task.
deleteBookmark (int sid, String contactId, int docId)	int		Deletes a bookmark from a knowledge document.
deleteComment (int sid, int commentId)	int		Deletes a comment for a knowledge document.
deleteDocument (int sid, int docId)	int		Flags a knowledge document for deletion.
deleteWorkFlowTask (int sid, String workFlowHandle, String objectHandle)	void		Removes a workflow task from its associated ticket.
detachChangeFromRequest (int sid, String creator, String requestHandle, String description)	String		Detaches a change order from a request.
doQuery (int sid, String objectType, String whereClause)	ListResult [listHandle, listLength]		Performs a SQL-like select on the specified object type.
doSelect (int sid, String objectType, String whereClause, int maxRows, ArrayOfString attributes)	String [UDSObjectList]		Performs a SQL-like select on the specified object type.
doSelectKD (int sid, String whereClause, String sortBy, boolean desc, int maxRows, ArrayOfString attributes, int skip)	String [UDSObjectList]		Performs a SQL-like select on the knowledge document object.
escalate (int sid, String creator, String objectHandle, String description, boolean setAssignee, String	String [UDSObject (Handle only)]		Performs an escalate activity on a ticket.

Method Name (Input Parameters)	Return Type [XML Root Element]	Output Parameters (Type: StringHolder) [XML Root Element]	Description
newAssigneeHandle, boolean setGroup, String newGroupHandle, boolean setOrganization, String newOrganizationHandle, boolean setPriority, String newPriorityHandle)			
faq (int sid, String categoryIds, int resultSize, String propertyList, String sortBy, boolean descending, String whereClause, int maxDocIDs)	String [UDSObjectList]		Performs a faq search on knowledge documents.
findContacts (int sid, String userName, String lastName, String firstName, String email, String accessType, int inactiveFlag)	String [UDSObjectList]		Retrieves a list of contacts.
freeListHandles (int sid, ArrayOfInt handles)	void		Frees the server-side resources for lists and invalidates the list handles.
getAccessTypeForContact (int sid, String contactHandle)	String		Returns a handle for the Access Type of a contact.
getArtifact (int sid, String contact, String password)	String		Returns an artifact for appending to URLs.
getAssetExtensionInformation (int sid, String assetHandle, ArrayOfString attributes, StringHolder getAssetExtInfoResult, StringHolder extensionHandle, StringHolder extensionName)	void	getAssetExtInfoResult [UDSObject] extensionHandle extensionName	Returns extension information for an asset.
getAttmntInfo (int sid, int attmntId)	String [UDSObjectList]		Returns the attributes for an attachment.
getAttmntList (int sid, int folderId, int repId)	String [UDSObjectList]		Returns a list of attachments under a given attachment folder.
getAttmntListPerKD (int sid, int docId)	String [UDSObjectList]		Returns a list of attachments for a given knowledge document.

Method Name (Input Parameters)	Return Type [XML Root Element]	Output Parameters (Type: StringHolder) [XML Root Element]	Description
getBookmarks (int sid, String contactId)	String [UDSObjectList]		Retrieves bookmarks for a given contact.
getBopsid (int sid, String contact)	String		Returns a token for appending to URLs.
getCategory (int sid, int catId, boolean getCategoryPaths)	String [UDSObjectList]		Retrieves information for a knowledge category.
getComments (int sid, String docIds)	String [UDSObjectList]		Retrieves all comments from the list of knowledge documents.
getConfigurationMode (int sid)	String		Returns confirmation if CA SDM is running in ITIL mode.
getContact (int sid, String contactId)	String [UDSObject]		Retrieves information for a given contact.
getDecisionTrees (int sid, String propertyList, String sortBy, boolean descending)	String [UDSObjectList]		Retrieves all Decision Tree knowledge documents.
getDependentAttrControls (int sid, String handle, ArrayOfString attrVals)	String [UDSObjectList]		Returns a list of locked and required attributes for the Status object.
getDocument (int sid, int docId, String propertyList, boolean relatedDoc, boolean getAttmnt, boolean getHistory, boolean getComment, boolean getNotiList)	String [UDSObject]		Retrieves information for a knowledge document.
getDocumentsByIDs (int sid, String docIds, String propertyList, String sortBy, boolean descending)	String [UDSObjectList]		Retrieves information for one or more knowledge documents.
getDocumentTypes (int sid)			

Method Name (Input Parameters)	Return Type [XML Root Element]	Output Parameters (Type: StringHolder) [XML Root Element]	Description
	String [UDSObjectList]		Returns a list of all knowledge document types.
getFolderInfo (int sid, int folderId)	String [UDSObject]		Retrieves information for a given attachment folder.
getFolderList (int sid, int parentFolderId, int repId)	String [UDSObjectList]		Returns a list of folders under a given parent folder.
getGroupMemberListValues (int sid, String whereClause, int numToFetch, ArrayOfString attributes)	String [UDSObjectList]		Queries the group of the system and member relationship.
getHandleForUserid (int sid, String userID)	String		Returns the persistent handle for a contact.
getKDListPerAttmnt (int sid, int attmntId)	String [UDSObjectList]		Returns a list of knowledge documents with reference to a given attachment.
getListValues (int sid, int listHandle, int startIndex, int endIndex, ArrayOfString attributeNames)	String [UDSObjectList]		Returns attribute values for a range of objects in a list.
getLrelLength (int sid, String contextObject, String lrelName)	int		Returns the number of objects on one side of a many-to-many relationship.
getLrelValues (int sid, String contextObject, String lrelName, int startIndex, int endIndex, ArrayOfString attributes)	String [UDSObjectList]		Returns attribute values for a range of objects in a many-to-many relationship.
getNotificationsForContact (int sid, String contactHandle, int queryStatus)	ListResult [listHandle, listLength]		Returns a list handle of notifications (lr objects) for a given contact.

Method Name (Input Parameters)	Return Type [XML Root Element]	Output Parameters (Type: StringHolder) [XML Root Element]	Description
getObjectTypeInformation (int sid, String factory)	String [UDSObject (special)]		Returns a list of all attribute names for a given object.
getObjectValues (int sid, String objectHandle, ArrayOfString attributes)	String [UDSObject]		Returns the attribute values for a given object handle.
getPendingChangeTaskListForContact (int sid, String contactHandle)	ListResult [listHandle, listLength]		Returns all the pending change order workflow tasks assigned to a given contact.
getPendingIssueTaskListForContact (int sid, String contactHandle)	ListResult [listHandle, listLength]		Returns all the pending issue workflow tasks assigned to a contact.
getPermissionGroups (int sid, int groupId)	String [UDSObjectList]		Retrieves info for a permission group.
getPolicyInfo (int sid)	String [SAPolicy]		Returns information about the access policy for the current session.
getPriorities (int sid)	String [UDSObjectList]		Retrieves all the knowledge priorities.
getPropertyInfoForCategory (int sid, String categoryHandle, ArrayOfString attributes)	String [UDSObjectList]		Retrieves property information for a given category.
getQuestionsAsked (int sid, int resultSize, boolean descending)	String [UDSObjectList]		Retrieves historical knowledge document search text.
getRelatedList (int sid, String objectHandle, String listName)			Returns a list handle for a list (QREL or BREL) of an object.

Method Name (Input Parameters)	Return Type [XML Root Element]	Output Parameters (Type: StringHolder) [XML Root Element]	Description
	ListResult [listHandle, listLength]		
getRelatedListValues (int sid, String objectHandle, String listName, int numToFetch, ArrayOfString attributes, StringHolder getRelatedListValuesResult, IntHolder numRowsFound)	void	getRelatedListValuesResult [UDSObjectList] numRowsFound (IntHolder)	Returns values for lists of an object.
getRepositoryInfo (int sid, int repositoryId)	String [UDSObject]		Returns information of a repository.
getStatuses (int sid)	String [UDSObjectList]		Retrieves all the knowledge statuses.
getTaskListValues (int sid, String objectHandle, ArrayOfString attributes)	String [UDSObjectList]		Returns values for tasks associated with a given issue or change order.
getTemplateList (int sid)	String [UDSObjectList]		Retrieves all the document templates.
getValidTaskTransitions (int sid, String taskHandle, ArrayOfString attributes)	String [UDSObjectList]		Returns all possible status transitions for a particular task.
Returns all possible status transitions for a particular task.	String [UDSObjectList]		Returns all possible status transitions for a particular ticket.
getWorkflowTemplateList (int sid)	String [UDSObjectList]		Retrieves all the knowledge workflow templates.
getWorkFlowTemplates (int sid, String objectHandle, ArrayOfString attributes)	String [UDSObjectList]		Returns all the workflow templates

Method Name (Input Parameters)	Return Type [XML Root Element]	Output Parameters (Type: StringHolder) [XML Root Element]	Description
			associated with the category of a change order or issue.
impersonate (int sid, String userid)	int		Invalidates the old session and returns a new session ID for the new user.
isAttmntLinkedKD (int sid, int attmntId)	int		Returns the number of attachment links to all knowledge documents.
logComment (int sid, String ticketHandle, String comment, int internalFlag)	void		Performs a log comment activity on a ticket.
login (String username, String password)	int		Authenticates a user and returns a unique session ID.
loginService (String username, String password, String policy)	int		Authenticates a user and returns a unique session ID.
loginServiceManaged (String policy, String encrypted_policy)	String		Performs user authentication for PKI configurations and returns a session ID.
loginWithArtifact (String userid, String artifact)	int		Authenticates a user with artifact and returns a unique session ID.
logout (int sid)	void		Invalidates and frees a session ID.
modifyDocument (int sid, int docId, ArrayOfString kdAttributes)	String [UDSObject]		Updates a knowledge document.
notifyContacts (int sid, String creator, String contextObject, String messageTitle, String messageBody, int notifyLevel, ArrayOfString notifyees, boolean internal)	String [UDSObject (Handle only)]		Sends a notification to one or more contacts.

Method Name (Input Parameters)	Return Type [XML Root Element]	Output Parameters (Type: StringHolder) [XML Root Element]	Description
rateDocument (int sid, int docId, int rating, int multiplier, String ticketPerId, boolean onTicketAccept, boolean solveUserProblem, boolean isDefault)	String [UDSObjectList]		Rates a particular knowledge document.
removeAttachment (int sid, String attHandle)	int		Removes an attachment from a ticket.
removeLrelRelationships (int sid, String contextObject, String lrelName, ArrayOfString removeObjectHandles)	void		Removes one or more many-to-many relationships.
removeMemberFromGroup (int sid, String contactHandle, String groupHandle)	void		Removes a contact from a group.
search (int sid, String problem, int resultSize, String properties, String sortBy, boolean descending, boolean relatedCategories, int searchType, int matchType, int searchField, String categoryPath, String whereClause, int maxDocIDs)	String [UDSObjectList (nested)]		Searches for knowledge document solutions.
serverStatus (int sid)	int		Returns the status (up or down) of the CA SDM server.
transfer (int sid, String creator, String objectHandle, String description, boolean setAssignee, String newAssigneeHandle, boolean setGroup, String newGroupHandle, boolean setOrganization, String newOrganizationHandle)	String [UDSObject (Handle only)]		Performs a transfer activity on a ticket.
updateObject (int sid, String objectHandle, ArrayOfString attrVals, ArrayOfString attributes)	String [UDSObject]		Updates one or more attributes for a given object.
updateRating (int sid, int buId, int rate)	String [UDSObject]		Updates an existing rating of a knowledge document.
loginWithArtifact (String userid, String artifact)	int		Authenticates a user with artifact and returns a unique session ID.
	String		

Method Name (Input Parameters)	Return Type [XML Root Element]	Output Parameters (Type: StringHolder) [XML Root Element]	Description
getArtifact (int sid, String contact, String password)			Returns an artifact for appending to URLs.

XML Object Returns

Many of the Web Services methods return an XML representation of CA SDM objects. The Web Services uses a standard XML structure beginning with the following root element:

```
<UDSObject>
```

The format of the XML representation is described in the following table:

XML Element	Type	Description
<UDSObject>	N/A	Identifies the root node.
<Handle>	String	Identifies the object's handle.
<Attributes>	Sequence	Identifies the attribute values. This holds zero or more elements for the object's attribute values.
<*attrName0* DataType = *"typeEnum"*>	String	Identifies the *AttrName0,* which is an object attribute name as defined in the CA SDM majic (.maj) or mod (.mod) file. This name may use dot-notation depending on the web method used. The element's value is the attribute's value. An empty element indicates a null/empty value for this object's attribute. The DataType attribute is an integer indicating the attribute's data type in the CA SDM environment.

For example, a call to getObjectValues() can return information illustrated by the following:

```
<UDSObject>
    <Handle>cnt:555A043EDDB36D4F97524F2496B35E75</Handle>
    <Attributes>
        <Attribute DataType="2003">
            <AttrName>first_name</AttrName>
            <AttrValue>first name</AttrValue>
            <DisplayValue>Yaakov</DisplayValue>
        </Attribute>
        <Attribute DataType="2005">
            <AttrName>organization</AttrName>
                <AttrValue>342</AttrValue>
        <DisplayValue>Accounting Crew</DisplayValue>
    </Attribute>
</Attributes>
```

```
    <Lists>        <List name="mylist1">
            <UDSObject>...</UDSObject>
            <UDSObject>...</UDSObject>
        </List>
    </Lists>
</UDSObject>
```

Some methods, such as doSelect(), return a sequence of <UDSObject> elements contained inside a <UDSObjectList> element.

The <Lists> section holds zero or more <List> nodes. A <List> node holds zero or more <UDSObject> nodes. <List> elements are generally returned only when a specific request for list values is made.

When you want to return a list of values related to a specific object, you should use the *getRelatedListValues* method.

If a request is made just for a list with no attribute name, such as actlog, then the entire <UDSObject> is returned in the <List> section.

Specialized methods, like getDocument(), can of course be different. When a request is made for an attribute, the database value is returned. For SREL attributes, this may not be so useful. Requesting the assignee attribute of a Request returns an integer because the Contact REL_ATTR (foreign key) is its ID. For CA Service Desk Manager r11.0, the return data for attributes includes elements for the DBMS and common name value of SREL references.

REST HTTP Methods

This article contains the following topics:

The REST API supports the following HTTP methods to manipulate resources:

- POST (CREATE) creates a resource.
- GET (READ) returns a representation of a resource.
- PUT (UPDATE) updates an existing resource.
- DELETE deletes the resource.

Refer to this basic set of methods as CRUD. Each method works in the same manner on all CA SDM resources. You require an HTTP client library, available with most programming languages. Use the HTML client library to complete the following tasks:

- Access and modify associated (or related) resources using a multilevel URI path.
- Send an HTTP request to the server for the resource that you want to manipulate.
- Control the object attributes to be returned by using HTTP headers.

After you update Majic object definitions and recycle CA SDM, the product automatically regenerates and redeploys the corresponding Plain Old Java Objects (POJOs) into the REST Tomcat *webapps* directory.

Note: The pdm_rest_util command line utility lets you *manually* generate, compile, and deploy Java code that REST web services require.

Important! Requests for attributes that do *not* respond indicate a null attribute value. Modify your client code accordingly because REST does *not* display null attribute values in responses.

REST Web Services provide a scalable configuration and better flexibility to our users by letting you connect to a dedicated domsrvr on the local server. By default, CA SDM Release 12.9 provides the NX_REST_WEBSERVICE_DOMSRVR variable to domsrvr. You can edit NX.env to change this setting.

CA SDM disables the REST sample mobile user interface and exposes all Majic factories through REST Web Services by default.

Important! The REST API does not support Majic attributes of type DOUBLE.

The following table shows how the REST API uses HTTP methods on resources.

Resource	CREATE	READ	UPDATE	DELETE
Collection URL For example: http://myweb site.com /resources/	Creates an entry in the collection. Assigns a new entry URL automatically and returns it by the operation.	Lists the URLs and other details of the collection members.	N/A	N/A
Element URL For example: http://myweb site.com /resources /item1	N/A	Retrieves a representation of the addressed member of the collection.	Updates the addressed member of the collection, and when the member does not exist, creates it.	Deletes the addressed member of the collection.

Sample URI Paths for CRUD Operations

The following table shows sample URI paths for CRUD operations:

CRUD Operation	HTTP Method	Noun	Sample URI Path
CREATE	Post	URI	/caisd-rest/chg
READ (Multiple)	GET	Collection URI	/caisd-rest/chg
Read (Multiple with Filter)	GET	Collection URI	/caisd-rest/chg?WC=status%3D6001
Read (Single ID)	GET	Entry URI	/caisd-rest/chg/400001
Read (Single COMMON_NAME)	GET	Entry URI	/caisd-rest/chg/COMMON_NAME-21
Read (Single REL_ATTR)	GET	Entry URI	/caisd-rest/chgstat/REL_ATTR-OP
Update	PUT	Entry URI	/caisd-rest/chg/40001
Delete	DELETE	Entry URI	/caisd-rest/grpmem/400001

Important! COMMON_NAME and REL_ATTR are case-sensitive. If you do not use upper case, REST returns the HTTP-404 error code.

REST Considerations

Consider the following information about REST methods:

- POST operations create a resource from the provided representation, but CA SDM can add or modify attribute values internally. These values are based on business object logic that attribute triggers, SPEL code, methods, or both set. The result causes the POST operation to return the actual representation that it created to the client. This behavior lets clients reconcile the representation that they sent to the server with the actual representation that they created.
- For GET operations, enter **%20** instead of a space in the WHERE clause.

REST Limitations

The REST API does *not* support dotted attribute name references in its resource queries or attributes. REST does *not* expose any BREL, QREL or LREL attribute that contains a dotted attribute in its relationship query. For example, the chg object in base.maj contains the following QREL attributes:

```
workload_chg QREL chg DYNAMIC {
WHERE "assignee = ? and active = 1" ;
PARAM_NAMES { id } ;
DOMSET chg_list;
} ;
change_tasks QREL wf DYNAMIC {
WHERE "assignee = ? AND status.allow_task_update = 1 " ;
PARAM_NAMES { id } ;
DOMSET wf_list ;
} ;
```

In this example, workload_chg QREL attributes are available. The change_tasks QREL is unavailable because it contains a dotted attribute (status.allow_task_update) in its WHERE clause.

REST and Object Access

Many CA SDM components consist of objects. A metalanguage named Majic defines these objects. Majic statements let you create objects and modify existing objects, so you can customize these objects to meet your business requirements. You can customize the exposure of the CA SDM objects through REST to determine the following:

- Objects accessible through REST
- Permitted operations for each object

After you install CA SDM, all objects are accessible through REST. The REST_OPERATIONS keyword specifies the operations that you can perform on an object. By default, all objects allow the CREATE, READ, and UPDATE operations. Some default objects also permit the DELETE operation, as indicated in the REST_OPERATIONS list in their object definition. You do *not* need to use the REST_OPERATIONS keyword for the default setup. You can refine object access to perform the following tasks:

- Override the REST_OPERATIONS list by using a Majic MODIFY statement to remove or add operations, except for the DELETE operation.
  Note: You cannot add the DELETE operation to any default object.
- Remove an object from REST entirely by specifying NONE in the REST_OPERATIONS list.

rest_access resource

The rest_access resource contains REST API access information for the authenticated users. It is an administrative table and contains the list of users allowed through the REST API.

The following list shows the deviations from the default behavior:

- **POST**
  Creates a REST access object and returns access key, secret key and expiration date as part of default values.
- **GET**
  Retrieves REST access information (except for secret key).
- **DELETE**
  Deletes the REST access object.
- **PUT**
  Does not allow updates to secret_key, access_key, and contact due to the Majic WRITE_NEW property.

REST_OPERATIONS Keyword

The Majic keyword, REST_OPERATIONS, uses a parenthesized list of tokens. These tokens let you specify the REST operations that are permitted for an object. You use an object definition and a MODIFY clause to customize the keyword.

The REST_OPERATIONS keyword has the following syntax:

```
REST_OPERATIONS "[<OP>],[<OP>] | NONE";
```

- **OP**
  Specifies the CREATE, READ, UPDATE, and DELETE operations.

This keyword produces the following statements:

```
REST_OPERATIONS "CREATE, READ, UPDATE DELETE";
REST_OPERATIONS "NONE";
```

At run time, CA SDM allows overrides by using the following Majic MODIFY statement:

```
MODIFY FACTORY cr {
             REST_OPERATIONS "READ, UPDATE";
       };
```

REST_OPERATIONS Syntax Examples

The following example modifies the cr object to limit the operations to READ and UPDATE. Any attempt to create or delete the object returns an error of *HTTP error code 405 Method Not Allowed*.

Important! CA SDM sets the default value for a REST_OPERATIONS property as “CREATE READ UPDATE” for most Objects. For example, cr, iss, and chg. For some object, CA SDM sets the default REST_OPERATIONS value to “CREATE READ UPDATE DELETE.” For example, rest_access and KCAT.

```
MODIFY FACTORY cr {
REST_OPERATIONS "READ UPDATE";
};
```

The following example removes announcements from REST completely:

```
MODIFY FACTORY cnote {
REST_OPERATIONS "NONE";
};
```

Note: You cannot use DELETE in a MODIFY statement. The NONE operation is standalone and not allowed with the CREATE READ UPDATE combination in the MODIFY statement.

Working with BLRELs

The BLREL keyword refers to Majic attributes that point to an LREL table. These attributes are part of a three-factory relationship. BLREL attributes were known as LREL attributes in previous releases of CA SDM, but they have changed to BREL attributes. This name helps distinguish BLRELs from the classic BREL attributes which are only a two-factory relationship.

An example of this three-factory relationship is the group and members relationship. This relationship consists of a grp object, a cnt object, and the LREL table object that the grpmem object represents. In this three-factory relationship, two BLREL attributes always point to a common LREL table. In the group/member relationship, both BLREL attributes are frequently part of the same object, but not always.

The following example shows how CA SDM defines BLREL attributes in Majic files.

```
OBJECT cnt {
    ...
    member_list         BREL  grpmem group DYNAMIC { LREL member; } ;
    group_list          BREL  grpmem member DYNAMIC { LREL group; } ;
}
```

You can always view the attributes of an object by executing the bop_sinfo command on an active system:

```
bop_sinfo -d grpmem
```

The LREL table record creates an association between records of two other tables. For the group /member relationship, the grpmem record is the LREL table that creates this association. It is a many-to-many relationship, where groups can have many members, and members can be part of many groups.

WHERE Clause Resource Search

REST Web Services let you use a *WC* (WHERE clause) query for the GET request. REST only supports the SQL query notation, not the Majic query notation. For example, you cannot use a dotted attribute notation. If you do not add a WC parameter to the URL, all records return up to the page size and maximum size limits.

Consider the following information:

- Use percent-encoding for all requests before you send them to the server. For example, enter **%3D** instead of =, the equals sign.
- The WC parameter is part of the URI instead of a message header to allow bookmarking.
- The WC query parameter only applies to Collection GET requests.

Example: Search for Contact Records with a Last Name that Equals ServiceDesk

```
http://<host>:<REST port>/caisd-rest/cnt?WC=last_name%3D'ServiceDesk'
```

Example: Search for Priority 2 Incidents

```
/in?WC=priority%3D4
```

The 4 value in the example specifies the REL_ATTR value for the Priority 2 record.

Important! Use REL_ATTR values in the WC parameter when you reference SREL attributes such as priority.

Example: Search for Incidents that Contain test% in the Summary Field

```
/in?WC=summary%20LIKE%20'test%25'
```

Valid URI Path Patterns

Not all resource paths and subresource paths expose all four HTTP methods, depending on the URI path level and the resource. The following list shows the exposed methods:

- **/caisd-rest/<factory>**

Example: /caisd-rest/cr

GET searches for objects and returns a collection of objects.

POST creates an object and returns the object that you created.

- **/caisd-rest/<factory>/<object id>**

Example: /caisd-rest/cr/400001

GET returns details for one object.

PUT updates the object.

DELETE removes the object. If allowed.

- **/caisd-rest/<factory>/<object id>/<attribute name (SREL)>**

Example: /caisd-rest/chg/400001/status

GET returns Details for the SREL attribute object, same as going directly to the SREL object if you know the ID. For example, /caisd-rest/crs/5200

- **/caisd-rest/<object>/<object id>/<attribute name (BREL)>**

Example: /caisd-rest/chg/400001/act_log

GET returns a collection of objects of the type the BREL points to.

- **/caisd-rest/<factory>/<object id>/<attribute name (BLREL)>**

Example: /caisd-rest/chg/400001/attachments

GET returns a collection of objects of the type the BLREL points to (the LREL record).

- **/caisd-rest/<factory>/<object id>/<attribute name (QREL)>**

Example: /caisd-rest/chg/400001/workflow

GET returns a collection of objects of the type the QREL points to.

Search Result Sorting

CA SDM Web Services let you sort search results by using the SORT query parameter, included as part of the URI. You can specify a list of attributes as the sort order. You can also specify ASC for ascending order, or specify DESC for descending order.

For default behavior, the SORT parameter provides that same support that the DBMS provides for the ORDER BY clause. For example, if you omit ASC or DESC, the DBMS may use ASC automatically. If you do not provide a SORT parameter in the URI, the DBMS uses *id ASC* by default.

This behavior only applies to collection GET requests, such as the example:

```
GET http://<host>:<REST-port>/caisd-rest/<fac name>
GET http://myserver:8080/caisd-rest/cr?SORT=priority DESC, severity ASC
```

Consider the following information:

- You *must* encode all requests before sending them to the server. For example, enter **%20** instead of spaces.
- All object attributes specified in the SORT parameter add to the X-Obj-Attrs list of object attributes automatically. This behavior helps ensure that the attributes selected for sorting are part of the response.
- The SORT parameter is part of the URI instead of a message header to allow for bookmarking.

Note: If you do not provide the X-Obj-Attrs header, id, REL_ATTR, and COMMON_Name list by default, as they always appear as part of the response.

Search Result Navigation

Provide ATOM links to improve navigating search and list results. These links take the user to the previous or next step when more records become available. By default, the Collection GET result contains up to 25 records. Use the rest_webservice_list_page_length and rest_webservice_list_max_length options to configure the page length and maximum number of records to display.

The ATOM links appear only for available records for that purpose. REST does not provide the *previous* link if the current page contains the first record in the list. Similarly, REST only provides the *next* and *all* links when you have more available records.

Users can also provide their own list return size with the *size* parameter. If the user does not provide *size*, REST defaults to the value of rest_webservice_list_page_length. If you do not provide start, REST defaults to 1.

Example Request Returns a Specific Number of Records

In this example, you request a return of 10 records:

```
http://myserver:8050/caisd-rest/cnt?start=11&size=10
```

If this result set contained 50 records, the following links appear:

```
<link href="http://myserver:8050/caisd-rest/cnt?start=1&size=10" rel="previous"/>
<link href="http://myserver:8050/caisd-rest/cnt?start=21&size=10" rel="next"/>
<link href="http://myserver:8050/caisd-rest/chg?start=1&size=50" rel="all"/>
```

Note: When the result set contains more than the maximum number allowed, the all link does not appear.

HTTP Status and Error Codes

Every HTTP response contains an HTTP status code. Successful HTTP response code numbers range from 200 to 399. Standard HTTP error response code numbers range from 400 to 599.

The following list shows the successful and error code numbers that the REST API returns for each of the HTTP methods.

- **GET (single)**
  200, 400, 401, 404, 409
- **GET (collection)**
  200, 400, 401
- **PUT**
  200, 400, 401, 404, 409
- **DELETE**
  204, 400, 401, 409
- **POST**
  201, 400, 401, 409

Note: For the PUT and DELETE operations, the API does *not* try to determine the validity of the ID initially. Instead, the API tries to run the update and delete queries directly. If an error occurs, the API returns the *409 Conflict* code. If the API returns a *404 Not Found* code in this situation, performance degrades.

In addition, the following error messages return under the following cases:

- If the HTTP request contains an invalid or inaccessible URI address, the server responds with a *404 Not Found* response code.
- If the HTTP request contains an unsupported HTTP method for a valid URI, the server responds with a *405 Method Not Allowed* response code.
- If the HTTP request requests an unsupported media type (Accept header), the server responds with a *406 Not Acceptable* response code.
- If the HTTP request sends an unsupported media type (Content-Type header), the server responds with a *415 Unsupported Media Type* response code.
- Various syntax or internal Web Server errors can return a 500 internal error.

Code Matching Limitations

Because of a limited number of available HTTP codes, not all CA SDM errors match to an HTTP error code. Matching errors return the corresponding HTTP error codes whenever possible, but most backend process errors return a generic *400 Bad Request* code. A message summarizes the error.

The following error messages match the corresponding HTTP error code. All others use error code 400.

- A request for a resource that does not exist in CA SDM returns a *404 Not Found* error code.
- A request for a resource that returns multiple matches, such as when using a nonunique COMMON_NAME value returns a *409 Conflict* error code.
- A request for an unaccessible resource due to Authentication Failure or Function Access security return a *401 Unauthorized* error code.

Known Status Codes

The following list describes the known status codes that the API returns. Other codes may exist from the web server or the CXF framework, but it depends on the type of error.

- **200**
  OK
  Indicates a successful return.
- **201**
  Created
  Indicates a new record.
- **204**
  No Content
  Indicates an empty response body.
- **304**
  Not Modified
  Indicates that the record did not update.
- **400**
  Bad Request
  Indicates that an error occurred due to a user or backend server issue.
- **401**
  Unauthorized
  Indicates a function Access error or any authentication failure.
- **404**
  Not Found
  Indicates that a record is not found.
- **405**
  Method Not Allowed
  Indicates an unsupported HTTP method.
- **406**
  Not Acceptable
  Indicates an unsupported requested format.

- **409**
  Conflict
  Indicates that multiple records were found for the given identifier.

- **415**
  Unsupported Media Type
  Indicates that the provided format is not supported.

- **500**
  Internal Server Error
  Indicates an error on the server or CXF framework.

Atom Feeds

CA SDM supports Atom feeds through the collection GET URI path because Atom feeds represent a list of records. This implementation supports all query parameters that REST Web Services support, such as the WC, start, and size query parameters. This implementation supports two additional query parameters, EntryTitle and EntrySummary, which let you specify a mapping between the Atom entry Title and Summary elements to Majic attributes.

```
EntryTitle=<Majic attribute name>
EntrySummary=<Majic attribute name>
```

Note: If you do *not* specify these parameters, REST uses the COMMON_NAME as the default title and summary values.

The following sample displays these query parameters:

```
GET /caisd-rest/cnt?size=2&EntryTitle=userid&EntrySummary=notes HTTP/1.1
Accept: application/atom+xml
```

The following sample displays the Atom response:

```
<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom">
  <author>
    <name>CA Service Desk Manager</name>
  </author>
  <title type="text">REST API Atom feed</title>
  <id>http://myserver:8050/caisd-rest/cnt</id>
  <updated>2012-01-17T17:56:04.301Z</updated>
  <link href="http://myserver:8050/caisd-rest/cnt?start=3&amp;size=2"
  rel="next"/>
  <link href="http://myserver:8050/caisd-rest/cnt?start=1&amp;size=12"
  rel="all"/>
  <link href="http://myserver:8050/caisd-rest/cnt"
  rel="self"/>
  <entry>
    <author>
      <name>CA Service Desk Manager</name>
    </author>
    <title type="text">System_AM_User</title>
```

```
    <id>http://myserver:8050/caisd-rest/cnt/U'16226C765005B94E957E0F477DEF1B1C'</id>
    <updated>1970-01-01T00:00:00.000Z</updated>
    <summary type="text"> User for Asset Management Integration</summary>
    <content type="application/xml">
      <cnt id="U'16226C765005B94E957E0F477DEF1B1C'" REL_ATTR="
U'16226C765005B94E957E0F477DEF1B1C'"
      COMMON_NAME="System_AM_User" xmlns="">
        <link href="http://myserver:8050/caisd-rest/cnt
/U'16226C765005B94E957E0F477DEF1B1C'"
        rel="self"/>
      </cnt>
    </content>
  </entry>
  <entry>
    <author>
      <name>CA Service Desk Manager</name>
    </author>
    <title type="text">cavizuser</title>
    <id>http://myserver:8050/caisd-rest/cnt/U'17DEA1027C7C3746B6F25DB6604EEE23'</id>
    <updated>1970-01-01T00:00:00.000Z</updated>
    <summary type="text">Username used by Visualizer for
            accessing CA Service Desk Manager using Web Services</summary>
    <content type="application/xml">
      <cnt id="U'17DEA1027C7C3746B6F25DB6604EEE23'" REL_ATTR="
U'17DEA1027C7C3746B6F25DB6604EEE23'"
      COMMON_NAME="System_CMDB_Visualizer_User" xmlns="">
        <link href="http://myserver:8050/caisd-rest/cnt
/U'17DEA1027C7C3746B6F25DB6604EEE23'"
        rel="self"/>
      </cnt>
    </content>
  </entry>
</feed>
```

Additional REST Support when Requesting Data Formats

REST Web Services also supports other ways of specifying the representation format using the URI. The Web Services work similarly specifying the representation format in the Accept HTTP header.

Example 1:

GET /caisd-rest/chg/400001.xml HTTP/1.1

GET /caisd-rest/chg/400001.json HTTP/1.1

GET /caisd-rest/chg.feed HTTP/1.1

Example 2:

GET /caisd-rest/chg/400001?_type=xml HTTP/1.1

GET /caisd-rest/chg/400001?_type=json HTTP/1.1

GET /caisd-rest/chg?_type=atom HTTP/1.1

Consider the following information:

- If the representation format is specified on the URI and through the “Accept” header, the one in the URI takes precedence over the Accept header.
- If a representation format is not specified in any way, the representation returns in the XML format by default.
- The *_type=* query parameter supersedes all parameters.

CA SDM Role Authorization

As with SOAP Web Services, part of the REST Web Services Access Key creation (login operation) includes verifying the user has authorization to access REST Web Services. In SOAP, the Web Service and API Role lookup field controls this verification in the Access Type detail form. In REST, a new lookup field named REST Web Service API Role controls the verification for REST. You can only associate one role to this field, and this field is the default role for the user. If this lookup field is empty, the users belonging to this Access Type do not have access to CA SDM through the REST Web Services interface.

In addition, REST Web Services supports the same list of Attached Roles that are part of the Web Client interface. A REST user can select a different role from the list of Attached Roles (including the roles in its Contact record) by passing in an additional message header as part of the request.

Example: Use the Administrator role for the request

```
POST /caisd-rest/cnt HTTP/1.1
Host: hostname
Date: Mon, 21 Apr 2011 19:37:58 +0000
X-Role: 10002
```

REST Java Sample Code

CA SDM provides REST Java sample code in the NX_ROOT\samples\sdk\rest\java directory. These sample files let you build custom Java client code in your environment, similar to SOAP web service samples. This directory contains instructions for compiling and executing the sample programs in the README.txt file. Each Java file documents additional instructions and sample input parameters. The following directories in \rest\java provide the following samples:

- **test1_basic**
- SampleBasicAuth.java
  Demonstrates how to get an Access Key using a username/password through the Basic Authentication scheme.
- SampleCRUDOperations.java
  Demonstrates how to perform simple CRUD operations (Create, Read, Update and Delete) on Incident tickets. The same can be used for any other object in CA SDM.
- **test2_auths**

- SampleBOPSIDAuth.java
  Demonstrates how to get an Access Key using a BOPSID token. This CA SDM token can be obtained from other CA SDM Interfaces such as SOAP Web Services.

- SampleEEMAuth.java
  Demonstrates how to get an Access Key using an CA EEM artifact/token. This token can be obtained from other applications that use CA EEM as their authentication server.

- SampleSDMAuth.java
  Demonstrates how to get an Access Key and a Secret Key using a username/password through the CA SDM custom authentication scheme.

- SampleUsingSecretKey.java
  Demonstrates how to make a REST API request (get a list of Contacts) using the Secret Key. It uses the Secret Key obtained from the CA SDM custom authentication operation to encrypt a configurable amount of data. All requests using this scheme are verified against the Secret Key.

- **test3_attachments**

- SampleNewResourceWithAttachment.java
  Demonstrates how to create a new Change Order ticket with an attachment document all in one step.

- SampleAttachFileToResource.java
  Demonstrates how to attach a document to an existing Change Order ticket.

- **test4_xrels**

- SampleGetQRELDetails.java
  Demonstrates how to retrieve details on a QREL attribute. In this sample, details for chg.children are retrieved. The same approach works for BREL and BLREL attributes.

- SampleCreateBRELResource.java
  Demonstrates how to create a new record for a BREL attribute. In this sample, a new Log Comment activity is added to an existing Change Order. The same approach works for creating a new record for BLREL attributes.

Build and Execute the Sample Programs

You can build and execute the sample Java programs to test them in your environment.

Follow these steps:

1. Copy rest_java_test.bat.txt (Windows) or rest_java_test.sh.txt (UNIX) to the subdirectory where the sample program exists.

2. Rename the copied file by removing the .txt extension.

3. Edit the copied file and verify that the first three SET variables are correct for your CA SDM installation.

4. In addition, edit the Java file that you want to run and verify that the configurable variables are set for your CA SDM installation. Also, read the comments at the top of the page.

CA SDM Authentication Scheme

CA SDM provides sample code in the NX_ROOT/samples/sdk/rest/java directory. This directory also contains instructions about how to compile and execute the sample programs. REST Web Services support the following security authentication schemes:

- REST Secret Key Authentication (see page 3996) that uses SSL and HMAC for login
- REST BOPSID Authentication (see page 3997) that validates CA SDM BOPSIDs
- REST Basic Authentication (see page 3997) that uses clear text encoded username and password
- External (CA EEM) Artifact Authentication (see page 3998) that uses a CA EEM artifact token

REST Secret Key Authentication

REST Secret Key authentication uses a custom, secure HMAC mechanism. This authentication lets CA SDM verify the identity of a user and also verifies that the request came from a registered, verified user. To complete this authentication successfully, each request must provide information about the identity of the request sender.

HMAC_ALGORITHM supports the HmacSHA1, HmacSHA256, HmacSHA384, HmacSHA512, and HmacMD5 valid HMAC algorithms. By default, REQUEST_METHOD, REQUEST_URI, and QUERY_STRING (if present) are used to compute the signature. You can also use other header fields to compute the signature, such as date, x-obj-attrs, and content-type. To add these fields set the following NX variable in NX.env file:

```
@NX_STRING_TO_SIGN_FIELDS=date,x-obj-attrs,content-type
```

Note: When you compute the signature on the Client side, use the same fields exactly in the same order as specified the fields for the STRING_TO_SIGN_FIELDS option.

- **Access Key**
  The Access Key is an assigned value to CA SDM clients after a successful login authentication. Requests use the Access Key to identify the client responsible for the request. However, because an Access Key is sent as a request parameter, the Access Key is not secret. A possibility exists that anyone could use the Access Key by sending a request to CA SDM. As a result, this authentication requires a Secret Key. REST uses the CA SDM session ID as the Access Key.

- **Secret Key**
  After you log in to CA SDM successfully, the product assigns a Secret Key and Access Key to the client. To protect users from impersonation, the client must provide additional information that CA SDM can use to verify the identity. CA SDM generates the 40-character Secret Key during the REST Access Key creation automatically.

The following steps describe the authentication process:

1. The client obtains the Access Key and Secret Key through the REST URI (POST /caisd-rest /rest_access) by providing user credentials using the basic authentication style over SSL.

2. For every subsequent HTTP request, the client uses the Secret Key, NX_STRING_TO_SIGN_FIELDS provides the header fields, and the NX_HMAC_ALGORITHM variable provides the hash function. This function calculates the request signature, a Keyed-Hash based Message Authentication Code (HMAC).

3. The client sends the request data, the signature, and the Access Key to CA SDM.
4. CA SDM uses the Access Key to look up the Secret Key from the persistence store.
5. CA SDM uses the request data and the Secret Key to generate the signature using the same hash algorithm that the client used.
6. If the signature that CA SDM generates matches the signature that the Client sent, CA SDM considers the request as authentic. Otherwise, CA SDM discards the request and returns an error response.

REST BOPSID Authentication

After a user logs in to CA SDM through one interface, they can access CA SDM from a different interface by using a BOPSID token. The BOPSID token provides a way for the invoked application to authenticate the user without requiring a login, such as Single Sign-On. After CA SDM authenticates a user, the application can request a BOPSID from boplgin. This single-use token identifies the user and session. Boplgin returns the userid and session when it receives the BOPSID. Boplgin also cancels the BOPSID if it does not receive a verification request within 5 minutes of token creation.

The following example shows the HTTP message header for passing the BOPSID token:

```
POST /caisd-rest/rest_access HTTP/1.1
Host: hostname
Date: Mon, 21 Apr 2012 19:37:58 +0000

X-BOPSID: <BOPSID token>
```

Note: To obtain a BOPSID token through REST Web Services, you send a POST request (see page 4002) to /caisd-rest/bopsid.

REST Basic Authentication

The basic authentication scheme assumes that the credentials of a client contain a username and password, where the password is a secret known only to the client and server.

If the incoming request does not contain the client credentials, the server sends back a 401 response that contains an authentication challenge. This challenge consists of the "Basic" token and a name-value pair that specifies the name of the protected realm, such as the following example:

```
WWW-Authenticate: Basic realm="<USDK> 12.9"
```

After receiving the 401 response from the server, the client (such as a browser) prompts for the username and password associated with that realm. The Authentication header of the client follow-up request should contain the "Basic" token and the base64-encoded group of the username, password, and a colon.

```
POST /caisd-rest/rest_access HTTP/1.1
Host: hostname
Date: Mon, 21 Apr 2012 19:37:58 +0000

Authorization: Basic QWRtaW46Zm9vYmFy
```

REST decodes credentials using base64 and compares them against the username/password and validates the credentials through boplgin. If this validation succeeds, the server provides access to the requested resource.

If the user sends the BOPSID instead of the username and password, CA SDM uses the the boplgin method validate_bopsid(). If you are concerned about using basic authentication scheme, you can disable it by setting the Options Manager option NX_REST_WEBSERVICE_DISABLE_BASIC_AUTH to Yes.

Important! Basic authentication is not as secure as the Secret Key method. However, you can use Basic authentication over an SSL connection for increased security.

External CA EEM Artifact Authentication

You can use CA EEM Artifact Authentication for REST requests. Clients send the CA EEM Artifact with the username using predefined customer headers (X-ExtAuthArtifact, X-UserName). When this header entry appears in an incoming request, the security interceptor performs the login validation by sending a VALIDATE_ARTIFACT message to boplgin.

The following example shows how to use the CA EEM Artifact:

```
POST /caisd-rest/rest_access HTTP/1.1
Host: hostname
Date: Mon, 21 Apr 2012 19:37:58 +0000

X-ExtAuthArtifact: <EEM Artifact token>
X-UserName: <username>
```

CRUD Operations on Tickets

The REST API provides sample Java code (see page 3994) for the user to work with tickets through the REST API. These files contain the following operations:

- Create a Change Order with hard-coded sample data.
- Update a recent Change Order with a status update.
- Create an Incident and display the Incident number on the console.
- Get a list of Incident numbers using a where clause and display on the console.

BREL, QREL, and BLREL Processing

The REST API provides the sample Java code (see page 3994) for the user to work with tickets through the REST API with BREL and QREL attributes. The BREL, QREL, and BLREL attributes only support the Get operation. The files contain the following operations:

- Create BREL using the documented, multistep process. For example, add activity logs to a Change Order. For QREL, create multiple Change Orders as children to a Change Order. For BLREL, add multiple CIs to a Change Order.
- Get a list of attributes that returns the URI for a BREL, QREL, or BLREL attribute, and display them on the console.

- Get the collection of the BREL, QREL, or BLREL attribute with the URI and display it on the console. For example, /caisd-rest/chg/40001/act_log.

Managing Attachments for Tickets

The REST API provides the sample Java code (see page 3994) for the user to work with tickets through the REST API. The files contain the following operations:

- Create an Incident.
- Create an attachment.
- Add the attachment to the Incident (2 step).
- Create an Incident with the attachment (1 step).
- Delete the attachment from the Incident.

CA SDM Resource Examples

Examples demonstrate how REST API uses basic Create, Read, Update, and Delete (CRUD) HTTP operations on CA SDM objects. Use the examples to understand how each REST operation works in the same manner on all CA SDM objects.

Note: For readability, the examples do not show all HTTP message headers -- only the relevant information.

Example Create a Change Order With an Attachment

This REST API example provides a complex use case: create a change order ticket and an attachment.

Note: MIME types application/xml and text/xml are often used interchangeably. We recommend that you use application/xml. All text/*-MIME types have an us-ascii character set unless otherwise explicitly specified in the HTTP headers. In effect, any encoding defined in the XML prolog (for example, <?xml version=”1.0” encoding=”UTF-8”?>) is ignored.

The following example shows the request:

```
POST /caisd-rest/chg/?
repositoryId=1002&AttachmentId=att1&serverName=HOSTNAME&mimeType=doc&description=Desc
HTTP/1.1
Content-Type: multipart/form-data
X-AccessKey: 51461077
User-Agent: Jakarta Commons-HttpClient/3.0.1
Host: hostname:8050
```

```
Content-Length: 1045

--Vschb1Sy2JD93ODUnWVAkRxp3IoXIMgXd
Content-Disposition: form-data; name="chg"
Content-Type: application/xml; charset=US-ASCII
Content-Transfer-Encoding: 8bit

<chg><description>Attachments Testing</description><status COMMON_NAME="RFC"
REL_ATTR="RFC" id="40020"><link rel="self" href="http://hostname:8050/caisd-rest
/chgstat/40020"/></status><summary>Attachment test</summary><requestor COMMON_NAME="
ServiceDesk" REL_ATTR="U'279B25DD051D0A47B54880D86700397F'" id="
U'279B25DD051D0A47B54880D86700397F'"><link rel="self" href="http://hostname:8050
/caisd-rest/cnt/U'279B25DD051D0A47B54880D86700397F'"/></requestor></chg>
--Vschb1Sy2JD93ODUnWVAkRxp3IoXIMgXd
Content-Disposition: form-data; name="Test.txt"; filename="Test.txt"
Content-Type: application/octet-stream; charset=ISO-8859-1
Content-Transfer-Encoding: binary
```

The following example shows the response:

```
HTTP/1.1 201 Created
Content-Type: application/xml;charset=UTF-8
Location: http://hostname:8050/caisd-rest/chg/400202

<chg id="400202" REL_ATTR="400202" COMMON_NAME="1047">
    <link href="http://hostname:8050/caisd-rest/chg/400202" rel="self"/>
</chg>
```

Example Create a Resource

This REST API example demonstrates how to create a resource. In this example, the REST API creates a change order ticket.

The following example shows the request:

```
POST /caisd-rest/chg HTTP/1.1
Host: hostname
Accept: application/xml
Content-Type: application/xml;charset=UTF-8
X-Obj-Attrs: chg_ref_num
<chg>
  <summary>Created via REST API</summary>
  <requestor REL_ATTR="U'793ED69B4E87A545BD8E911834D829FC'"/>
</chg>
```

The following example shows the response:

```
HTTP/1.1 201 Created
Content-Type: application/xml;charset=UTF-8
Location: http://hostname:8050/caisd-rest/chg/400001

<?xml version="1.0" encoding="UTF-8"?>
<chg id="400003" REL_ATTR="400003" COMMON_NAME="23">
```

```
  <link href="http://hostname:8050/caisd-rest/chg/400003"
        rel="self"/>
  <chg_ref_num>23</chg_ref_num>
</chg>
```

Example Delete a Resource

This REST API example demonstrates how to delete a resource.

Note: Not all objects are available for deletion. Most objects only support updating the delete_flag to true or false, or status equal to active or inactive. You perform these actions using an UPDATE request rather than a DELETE request.

The following example shows the request:

```
DELETE /caisd-rest/grpmem/400001 HTTP/1.1
Host: hostname
```

The following example shows the response:

```
HTTP/1.1 204 No Content
Content-Type: application/xml;charset=UTF-8
Content-Length: 0
```

Example Delete an Access Key

This REST API example demonstrates how to delete a CA SDM access key.

The following example shows the request:

```
DELETE /caisd-rest/rest_access/1201703106 HTTP/1.1
Host: hostname
```

The following example shows the response:

```
HTTP/1.1 204 No Content
Content-Type: application/xml;charset=UTF-8
Content-Length: 0
```

Example Mark a Resource Inactive

This REST API example demonstrates how to mark a resource as inactive.

Note: Most CA SDM objects only support marking them inactive and not actually deleting them.

The following example shows the request:

```
PUT /caisd-rest/loc/U'0502D608F9122B48B7C9DAB9E0457F94' HTTP/1.1
Host: hostname
Content-Type: application/xml;charset=UTF-8
X-Obj-Attrs: delete_flag

<loc id="U'0502D608F9122B48B7C9DAB9E0457F94'">
  <delete_flag COMMON_NAME="Inactive"/>
</loc>
```

The following example shows the response:

```
HTTP/1.1 200 OK
Content-Type: application/xml;charset=UTF-8

<?xml version="1.0" encoding="UTF-8"?>
<loc id="U'0502D608F9122B48B7C9DAB9E0457F94'"
     REL_ATTR="U'0502D608F9122B48B7C9DAB9E0457F94'"
     COMMON_NAME="Stadium 1">
  <link href="http://hostname:8050/caisd-rest/loc/U'0502D608F9122B48B7C9DAB9E0457F94'"
        rel="self"/>
  <delete_flag id="4552" REL_ATTR="1"
               COMMON_NAME="Inactive">
    <link href="http://hostname:8050/caisd-rest/actbool/4552"
          rel="self"/>
  </delete_flag>
</loc>
```

Example Obtain a BOPSID Token

A BOPSID token is single use authentication token that provides a single sign-on capability. This REST API example demonstrates how to obtain a BOPSID token to use for logging in to the web client.

The following example shows the request:

```
POST /caisd-rest/bopsid HTTP/1.1
Host: hostname.ca.com
Accept: application/xml
<bopsid/>
```

The following example shows the response:

```
HTTP/1.1 201 OK
Content-Type: application/xml;charset=UTF-8

<bopsid>
  <bopsid_val>987982618</bopsid_val>
</bopsid>
```

Example Obtain an Access Key

This REST API example demonstrates how to obtain an access key (login) for userid ServiceDesk. Perform this operation using SSL to avoid risking an unauthorized user stealing your secret key. Keep the force_unique_userid Options Manager option enabled at all times. When you disable this option, and multiple contact records with the same login ID exist, problems with data partitions, multi-tenancy, security, and other functions can occur.

The following example shows the request:

```
POST /caisd-rest/rest_access HTTP/1.1
Host: hostname
Content-Type: application/xml;charset=UTF-8
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
<rest_access/>
```

The following example shows the response:

```
HTTP/1.1 201 Created
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<rest_access id="400001" REL_ATTR="400001" COMMON_NAME="770921656">
    <link href="http://hostname:8050/caisd-rest/rest_access/400001"
    rel="self"/>
    <access_key>770921656</access_key>
    <expiration_date>1335276895</expiration_date>
</rest_access>
```

Example Retrieve a Collection of Resources

This REST API example demonstrates how to retrieve a collection of resources. In this example, the REST API retrieves a collection of all change order ticket objects.

Note: The root node (for example, collection_chg) also has other link elements such as previous, next, and all for navigating lists.

The following example shows the request:

```
GET /caisd-rest/chg HTTP/1.1
Host: hostname
Accept: application/xml
```

The following example shows the response:

```
HTTP/1.1 200 OK
Content-Type: application/xml;charset=UTF-8

<?xml version="1.0" encoding="UTF-8"?>
```

```
<collection_chg>
  <chg id="400001" REL_ATTR="400001" COMMON_NAME="21">
    <link href="http://hostname:8050/caisd-rest/chg/400001"
          rel="self"/>
  </chg>
  <chg id="400002" REL_ATTR="400002" COMMON_NAME="22">
    <link href="http://hostname:8050/caisd-rest/chg/400002"
          rel="self"/>
  </chg>
</collection_chg>
```

Example Retrieve a Collection of Resources Using a Where Clause

This REST API example demonstrates how to retrieve a collection of resources using a where clause. In this example, the REST API retrieves a collection of all request (cr) ticket objects with the Closed status.

Note: BREL queries are supported.

The following examples show the request:

```
GET /caisd-rest/cr?WC=status%3D'cl'
GET /caisd-rest/cr?WC=status%3D'op'%20and%20active%3D0
Host: hostname
Accept: application/xml
X-Obj-Attrs: ref_num, priority
```

The following example shows the response:

```
HTTP/1.1 200 OK
Content-Type: application/xml;charset=UTF-8

<?xml version="1.0" encoding="UTF-8"?>
<collection_cr COUNT="3" TOTAL_COUNT="3">
  <cr id="2903" REL_ATTR="cr:2903" COMMON_NAME="AM:12">
    <link href="http://hostname:8050/caisd-rest/cr/2903"
          rel="self"/>
    <priority id="502" REL_ATTR="3" COMMON_NAME="3">
      <link href="http://hostname:8050/caisd-rest/pri/502"
            rel="self"/>
    </priority>
    <ref_num>AM:12</ref_num>
  </cr>
  <cr id="2907" REL_ATTR="cr:2907" COMMON_NAME="AM:14">
    <link href="http://hostname:8050/caisd-rest/cr/2907"
          rel="self"/>
    <priority id="502" REL_ATTR="3" COMMON_NAME="3">
      <link href="http://hostname:8050/caisd-rest/pri/502"
            rel="self"/>
    </priority>
```

```
    <ref_num>AM:14</ref_num>
  </cr>
  <cr id="3105" REL_ATTR="cr:3105" COMMON_NAME="UAPM:13">
    <link href="http://hostname:8050/caisd-rest/cr/3105"
          rel="self"/>
    <priority id="502" REL_ATTR="3" COMMON_NAME="3">
      <link href="http://hostname:8050/caisd-rest/pri/502"
            rel="self"/>
    </priority>
    <ref_num>UAPM:13</ref_num>
  </cr>
</collection_cr>
```

Example Retrieve a Specific Resource

This REST API example demonstrates how to retrieve a specific resource using ID, COMMON_NAME, or REL_ATTR. In this example, the REST API retrieves details about the unique change order ticket object ID 400001.

The following example shows the request when you use ID:

```
GET /caisd-rest/chg/400001 HTTP/1.1
Host: hostname.ca.com
Accept: application/xml
X-Obj-Attrs: chg_ref_num, summary, requestor, status
```

The following example shows the request when you use COMMON_NAME:

```
GET /caisd-rest/chg/COMMON_NAME-32 HTTP/1.1
```

The following example shows the request when you use REL_ATTR:

```
GET /caisd-rest/chg/REL_ATTR-chg:400001 HTTP/1.1
```

The following example shows the response:

```
HTTP/1.1 200 OK
Content-Type: application/xml;charset=UTF-8

<?xml version="1.0" encoding="UTF-8"?>
<chg id="400001" REL_ATTR="400001" COMMON_NAME="21">
  <link href="http://hostname:8050/caisd-rest/chg/400001"
        rel="self"/>
  <chg_ref_num>21</chg_ref_num>
  <requestor id="U'793ED69B4E87A545BD8E911834D829FC'"
             REL_ATTR="U'793ED69B4E87A545BD8E911834D829FC'"
             COMMON_NAME="System_AHD_generated">
    <link href="http://hostname:8050/caisd-rest/cnt
/U'793ED69B4E87A545BD8E911834D829FC'"
          rel="self"/>
  </requestor>
  <status id="40020" REL_ATTR="RFC" COMMON_NAME="RFC">
    <link href="http://hostname:8050/caisd-rest/chgstat/40020"
```

```
        rel="self"/>
  </status>
  <summary>Testing</summary>
```

Example Retrieve a Subresource

This REST API example demonstrates how to retrieve a subresource.

The following example shows the request:

```
GET /caisd-rest/chg/400001/status HTTP/1.1
Host: hostname
Accept: application/xml
X-Obj-Attrs: code, sym, description
HTTP/1.1 200 OK
Content-Type: application/xml;charset=UTF-8

<?xml version="1.0" encoding="UTF-8"?>
<chgstat id="40020" REL_ATTR="RFC" COMMON_NAME="RFC">
  <link href="http://hostname:8050/caisd-rest/chgstat/40020"
        rel="self"/>
  <code>RFC</code>
  <description>Request for Change is in draft form</description>
  <sym>RFC</sym>
</chgstat>
```

Example Update a Resource

This REST API example demonstrates how to update a resource. In this example, the REST API updates the summary field for the change order ticket ID 400003.

The following example shows the request:

```
PUT /caisd-rest/chg/400003 HTTP/1.1
Host: hostname
Content-Type: application/xml;charset=UTF-8
X-Obj-Attrs: chg_ref_num, summary
<chg id="400003">
  <summary>Summary updated via REST API</summary>
</chg>
```

The following example shows the response:

```
HTTP/1.1 200 OK
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<chg id="400003" REL_ATTR="400003" COMMON_NAME="23">
  <link href="http://hostname:8050/caisd-rest/chg/400003"
        rel="self"/>
  <chg_ref_num>23</chg_ref_num>
  <summary>Summary updated via REST API</summary>
</chg>
```

Example Get a BLREL Record

This example shows how to retrieve a BLREL record:

The following example shows the request:

```
GET /caisd-rest/grpmem HTTP/1.1
Host: localhost
Accept: application/xml
X-Obj-Attrs: *
```

The following example shows the response:

```
HTTP/1.1 200 OK
Content-Type: application/xml;charset=UTF-8
<?xml version="1.0" encoding="UTF-8"?>
<collection_grpmem COUNT="3" START="1" TOTAL_COUNT="3">
    <grpmem id="400001" REL_ATTR="grpmem:400001" COMMON_NAME="400001">
        <link href="http://localhost:8050/caisd-rest/grpmem/400001"
        rel="self"/>
        <group id="U'CFCC2DC94B3A66448C085B07E7286CAA'" REL_ATTR="
U'CFCC2DC94B3A66448C085B07E7286CAA'"
        COMMON_NAME="Unicef">
            <link href="http://localhost:8050/caisd-rest/grp
/U'CFCC2DC94B3A66448C085B07E7286CAA'"
            rel="self"/>
        </group>
        <manager_flag>0</manager_flag>
        <member id="U'3F05B7450203AD449BFB8088D991A03E'" REL_ATTR="
U'3F05B7450203AD449BFB8088D991A03E'"
        COMMON_NAME="System_SD_User">
            <link href="http://localhost:8050/caisd-rest/cnt
/U'3F05B7450203AD449BFB8088D991A03E'"
            rel="self"/>
        </member>
        <notify_flag>1</notify_flag>
        <persistent_id>grpmem:400001</persistent_id>
        <producer_id>grpmem</producer_id>
    </grpmem>
    <grpmem id="400002" REL_ATTR="grpmem:400002" COMMON_NAME="400002">
        <link href="http://localhost:8050/caisd-rest/grpmem/400002"
        rel="self"/>
        <group id="U'55E3CCE805756B4F8084D63E05E6C216'" REL_ATTR="
U'55E3CCE805756B4F8084D63E05E6C216'"
        COMMON_NAME="Apache">
            <link href="http://localhost:8050/caisd-rest/grp
/U'55E3CCE805756B4F8084D63E05E6C216'"
            rel="self"/>
        </group>
        <manager_flag>0</manager_flag>
        <member id="U'FCF9A8AC6381AA4386C9B10EE382E10B'" REL_ATTR="
U'FCF9A8AC6381AA4386C9B10EE382E10B'"
        COMMON_NAME="System_MA_User">
```

```
            <link href="http://localhost:8050/caisd-rest/cnt
/U'FCF9A8AC6381AA4386C9B10EE382E10B'"
            rel="self"/>
        </member>
        <notify_flag>1</notify_flag>
        <persistent_id>grpmem:400002</persistent_id>
        <producer_id>grpmem</producer_id>
    </grpmem>
    <grpmem id="400003" REL_ATTR="grpmem:400003" COMMON_NAME="400003">
        <link href="http://localhost:8050/caisd-rest/grpmem/400003"
        rel="self"/>
        <group id="U'55E3CCE805756B4F8084D63E05E6C216'" REL_ATTR="
U'55E3CCE805756B4F8084D63E05E6C216'"
        COMMON_NAME="Apache">
            <link href="http://localhost:8050/caisd-rest/grp
/U'55E3CCE805756B4F8084D63E05E6C216'"
            rel="self"/>
        </group>
        <manager_flag>0</manager_flag>
        <member id="U'16226C765005B94E957E0F477DEF1B1C'" REL_ATTR="
U'16226C765005B94E957E0F477DEF1B1C'"
        COMMON_NAME="System_AM_User">
            <link href="http://localhost:8050/caisd-rest/cnt
/U'16226C765005B94E957E0F477DEF1B1C'"
            rel="self"/>
        </member>
        <notify_flag>1</notify_flag>
        <persistent_id>grpmem:400003</persistent_id>
        <producer_id>grpmem</producer_id>
    </grpmem>
</collection_grpmem>
```

This sample returns three grpmem records that represent the following associations:

- Group Unicef <-> Member System_SD_User
- Group Apache <-> Member System_MA_User
- Group Apache <-> Member System_AM_User

Example Retrieve a List of LREL Records Associated with a Group

The following example returns two grpmem records associated with the Group Apache whose REL_ATTR value is U'55E3CCE805756B4F8084D63E05E6C216'. Note that

- Group Apache <-> Member System_MA_User
- Group Apache <-> Member System_AM_User

The WHERE clause (WC) query parameter does not support dotted notation.

The following example shows the request:

```
GET /caisd-rest/grpmem?WC=group%3DU%2755E3CCE805756B4F8084D63E05E6C216%27 HTTP/1.1
Host: hostname
Accept: application/xml
X-Obj-Attrs: *
```

The following example shows the response:

```
HTTP/1.1 200 OK
Content-Type: application/xml;charset=UTF-8
<?xml version="1.0" encoding="UTF-8"?>
<collection_grpmem COUNT="2" START="1" TOTAL_COUNT="2">
    <grpmem id="400002" REL_ATTR="grpmem:400002" COMMON_NAME="400002">
        <link href="http://hostname:8050/caisd-rest/grpmem/400002"
        rel="self"/>
        <group id="U'55E3CCE805756B4F8084D63E05E6C216'" REL_ATTR="
U'55E3CCE805756B4F8084D63E05E6C216'"
        COMMON_NAME="Apache">
            <link href="http://hostname:8050/caisd-rest/grp
/U'55E3CCE805756B4F8084D63E05E6C216'"
            rel="self"/>
        </group>
        <manager_flag>0</manager_flag>
        <member id="U'FCF9A8AC6381AA4386C9B10EE382E10B'" REL_ATTR="
U'FCF9A8AC6381AA4386C9B10EE382E10B'"
        COMMON_NAME="System_MA_User">
            <link href="http://hostname:8050/caisd-rest/cnt
/U'FCF9A8AC6381AA4386C9B10EE382E10B'"
            rel="self"/>
        </member>
        <notify_flag>1</notify_flag>
        <persistent_id>grpmem:400002</persistent_id>
        <producer_id>grpmem</producer_id>
    </grpmem>
    <grpmem id="400003" REL_ATTR="grpmem:400003" COMMON_NAME="400003">
        <link href="http://hostname:8050/caisd-rest/grpmem/400003"
        rel="self"/>
        <group id="U'55E3CCE805756B4F8084D63E05E6C216'" REL_ATTR="
U'55E3CCE805756B4F8084D63E05E6C216'"
        COMMON_NAME="Apache">
            <link href="http://hostname:8050/caisd-rest/grp
/U'55E3CCE805756B4F8084D63E05E6C216'"
            rel="self"/>
        </group>
        <manager_flag>0</manager_flag>
        <member id="U'16226C765005B94E957E0F477DEF1B1C'" REL_ATTR="
U'16226C765005B94E957E0F477DEF1B1C'"
        COMMON_NAME="System_AM_User">
            <link href="http://hostname:8050/caisd-rest/cnt
/U'16226C765005B94E957E0F477DEF1B1C'"
            rel="self"/>
        </member>
        <notify_flag>1</notify_flag>
        <persistent_id>grpmem:400003</persistent_id>
```

```
        <producer_id>grpmem</producer_id>
    </grpmem>
</collection_grpmem>
```

Example Create a BLREL Record

The following example adds an existing contact System_SA_User as a member of group Apache. It uses the COMMON_NAME value of each of those records.

Group Apache <-> Member System_SA_User

The following example shows the request:

```
POST /caisd-rest/grpmem HTTP/1.1
Host: hostname
Accept: application/xml
Content-Type: application/xml;charset=UTF-8
X-Obj-Attrs: *
<grpmem>
    <group id="U'55E3CCE805756B4F8084D63E05E6C216'"/>
    <manager_flag>0</manager_flag>
    <member id="U'E70DFE4817614C06BE9E5991A96A6015'"/>
    <notify_flag>1</notify_flag>
</grpmem>
```

The following example shows the response:

```
HTTP/1.1 201 Created
Content-Type: application/xml;charset=UTF-8
<?xml version="1.0" encoding="UTF-8"?>
<grpmem id="400005" REL_ATTR="grpmem:400005" COMMON_NAME="400005">
    <link href="http://hostname:8050/caisd-rest3/grpmem/400005"
    rel="self"/>
    <group id="U'55E3CCE805756B4F8084D63E05E6C216'" REL_ATTR="
U'55E3CCE805756B4F8084D63E05E6C216'"
    COMMON_NAME="Apache">
        <link href="http://hostname:8050/caisd-rest3/grp
/U'55E3CCE805756B4F8084D63E05E6C216'"
        rel="self"/>
    </group>
    <manager_flag>0</manager_flag>
    <member id="U'E70DFE4817614C06BE9E5991A96A6015'" REL_ATTR="
U'E70DFE4817614C06BE9E5991A96A6015'"
    COMMON_NAME="System_SA_User">
        <link href="http://hostname:8050/caisd-rest3/cnt
/U'E70DFE4817614C06BE9E5991A96A6015'"
        rel="self"/>
    </member>
    <notify_flag>1</notify_flag>
    <persistent_id>grpmem:400005</persistent_id>
    <producer_id>grpmem</producer_id>
</grpmem>
```

Example Update a BLREL Record

The following example updates the relationship of the added record and sets member System_SA_User as a Manager.

The following example shows the request:

```
PUT /caisd-rest/grpmem/400005 HTTP/1.1
Host: hostname
Accept: application/xml
Content-Type: application/xml;charset=UTF-8
X-Obj-Attrs: *
<grpmem>
    <manager_flag>1</manager_flag>
</grpmem>
```

The following example shows the response:

```
HTTP/1.1 200 OK
Content-Type: application/xml;charset=UTF-8
<?xml version="1.0" encoding="UTF-8"?>
<grpmem id="400005" REL_ATTR="grpmem:400005" COMMON_NAME="400005">
    <link href="http://hostname:8050/caisd-rest3/grpmem/400005"
    rel="self"/>
    <group id="U'55E3CCE805756B4F8084D63E05E6C216'" REL_ATTR="
U'55E3CCE805756B4F8084D63E05E6C216'"
    COMMON_NAME="Apache">
        <link href="http://hostname:8050/caisd-rest3/grp
/U'55E3CCE805756B4F8084D63E05E6C216'"
        rel="self"/>
    </group>
    <manager_flag>1</manager_flag>
    <member id="U'E70DFE4817614C06BE9E5991A96A6015'" REL_ATTR="
U'E70DFE4817614C06BE9E5991A96A6015'"
    COMMON_NAME="System_SA_User">
        <link href="http://hostname:8050/caisd-rest3/cnt
/U'E70DFE4817614C06BE9E5991A96A6015'"
        rel="self"/>
    </member>
    <notify_flag>1</notify_flag>
    <persistent_id>grpmem:400005</persistent_id>
    <producer_id>grpmem</producer_id>
</grpmem>
```

Example Delete a BLREL Record

The following example removes member System_MA_User from group Apache. This example does not delete the member record or the group record. It only removes the association between them. It does physically remove the grpmem record.

The following example shows the request:

```
DELETE /caisd-rest/grpmem/400002 HTTP/1.1
```

```
Host: hostname
```

The following example shows the response:

```
HTTP/1.1 204 No Content
Content-Type: application/xml;charset=UTF-8
Content-Length: 0
```

Web Services Attachment-Related Methods

This article contains the following topics:

This section describes the Web Services attachment-related methods. Only file attachments are handled by these methods; link type attachments are handled by generic methods, such as CreateObject(). In addition, file uploads through Web Services employ the Direct Internet Message Encapsulation (DIME) protocol. Your SOAP implementation must support DIME in order to use these methods.

createAttachment

The following parameters apply to the createAttachment method:

Parameter	Data Type	Description
SID	INTEGER	Identifies the session retrieved from logging in.
repositoryHandle	STRING	Identifies the object handle of a document repository.
objectHandle	STRING	Identifies the object handle of a call request, change order, or issue, to which this attachment is attached. This parameter can be NULL, however, you must manage the attachment ID that is returned because the attachment is not associated to a ticket when NULL is passed in.
description	STRING	Identifies the description for the attachment object.
fileName	STRING	Identifies the full path of the file to be uploaded.

Description

Uploads a file to the back-end server. An uploaded file is stored in a document repository specified by the repositoryHandle. An attachment object is then created and attached to a ticket object specified by the objectHandle. The attachment object has all the information for accessing the newly uploaded file in the repository.

Returns

createAttachment has the following returns:

Parameter	Type	Description
<Handle>	STRING	Identifies the object handle of the newly created attachment object.

Could not perform the operation, policy limit exceeded

- **Symptom:**

When using the createAttachment() web service method to attach a document to an existing request or incident, you receive this error, even when the web services policy setting for attachments is set to -1(unlimited), which is the out-of-the-box default setting. You may receive this error when calling the web service method when there are no attached files in the received SOAP message. You must attach at least one file to the SOAP message before calling the createAttachment() web service method.

- **Solution:**

Set your SOAP implementation to support Direct Internet Message Encapsulation (DIME), and attach the file to be uploaded manually using DIME support before calling the createAttachment() method.

You can refer to the examples on how to support DIME from the $NX_ROOT\samples\sdk\websvc\java\test3_attachments directory.

Example: Visual Basic .NET

This code example illustrates sample Visual Basic .NET code to attach a file using DIME support before calling the createAttachment() web service method.

```
Dim reqContext As SoapContext = objCA SDM_WS.RequestSoapContext
Dim dimeAttach As New DimeAttachment("image/gif",
TypeFormat.MediaType, "c:\test.txt")
reqContext.Attachments.Add(dimeAttach)

strResult = objCA SDM_WS.createAttachment(sid, "doc_rep:1002",
"cr:400001", "my desc", "c:\test.txt")
```

Note: For information about the DIME attachment methods used in the previous sample code, see the Microsoft website. For programs written in other languages, see your documentation for the SOAP implementation that supports DIME.

Example: Java

This code example illustrates sample Java code to attach a file using DIME support before calling the createAttachment() web service method.

```
FileDataSource fds = new FileDataSource(filename);
DataHandler dhandler = new DataHandler(fds);
CA SDM._setProperty(Call.ATTACHMENT_ENCAPSULATION_FORMAT,
Call.ATTACHMENT_ENCAPSULATION_FORMAT_DIME);
```

```
CA SDM.addAttachment(dhandler);

String handle = CA SDM.createAttachment(sid, repHandle, objHandle,
description, filename);
```

removeAttachment

The following parameters apply to the removeAttachment method:

Parameter	Type	Description
SID	Integer	Identifies the SID of the current login session.
attHandle	String	Identifies the object handle of an attachment to be removed.

Description

Removes an attachment from a ticket object. The attached file is then removed from the repository.

Returns

Nothing.

attachURLLinkToTicket

The following parameters apply to the attachURLLinkToTicket method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
docId	Integer	Identifies the unique ID of the ticket.
URL	String	Indicates the URL to attach to the ticket.
attmntName	String	Identifies the name of the attachment.
Description	String	Indicates the description of the attachment.

Description

Attaches a URL link to a ticket.

Example:

```
CA SDM.attachURLLinkToTicket(sid, "cr:400001", "http://www.ca.com", "ca.com", "CA
Technologies Website");
```

Web Services Knowledge Attachment Methods

This article contains the following topics:

This section describes the Web Services Knowledge attachment methods.

createAttmnt

The following parameters apply to the createAttmnt method:

Parameter	Data Type	Description
SID	Integer	Identifies the session retrieved from logging in.
repositoryHandle	String	Identifies the object handle of a document repository.
folderId	Integer	Identifies the folder handle ID.
objectHandle	Int	Identifies the object handle of a Knowledge document to which this attachment is attached.
description	String	Identifies the description for the attachment object.
fileName	String	Identifies the name of the full path of the file to be uploaded.

Description

Uploads a file to the back-end server. An uploaded file is stored in a document repository specified by the repositoryHandle. An attachment object is then created and attached to a document object specified by the objectHandle. The attachment object has all the information for accessing the newly uploaded file in the repository.

Returns

The following:

Parameter	Type	Description
<Handle>	String	Identifies the object handle of the newly created attachment object.

attmntFolderLinkCount

The following parameters apply to the attmntFolderLinkCount method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
folderId	Integer	Identifies the unique ID of the folder

Description

Describes the number of attachment links under a specific folder to be attached.

Returns

Returns the number of attachments found under the specific folder.

attachURLLink

The following parameters apply to the attachURLLink method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
docId	Integer	Identifies the unique ID of the Knowledge document.
URL	String	Indicates the URL to attach to the Knowledge document.
attmntName	String	Identifies the name of the attachment.
Description	String	Indicates the description of the attachment.

Description

Attaches a URL link to a Knowledge document.

Returns

Returns error codes only for *individual* errors. For additional information, see Error Codes.

getKDListPerAttmnt

The following parameters apply to the getKDListPerAttmnt method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
attmntId	Integer	Identifies the unique ID of the attachment.

Description

Returns a list of Knowledge documents with reference to a given attachment.

Returns

A <UDSObject> node with zero or more <UDSObject> nodes describing the Knowledge document with the following <Attributes> child nodes:

XML Element Value	Type	Description
id	Integer	Identifies the unique ID of the Knowledge document.

getAttmntListPerKD

The following parameters apply to the getAttmntListPerKD method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
docId	Integer	Identifies the unique ID of the Knowledge document.

Description

A list of attachments with reference to a given Knowledge document.

Returns

A <UDSObject> node with zero or more <UDSObject> nodes describing the attachment with the following <Attributes> child nodes:

XML Element Value	Type	Description
id	Integer	Identifies the unique ID of the attachment

isAttmntLinkedKD

The following parameters apply to the AttmntLinkedKD method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
attmntId	Integer	Identifies the unique ID of the attachment.

Description

Checks if an attachment is linked to any Knowledge document, and returns the number of links found.

Returns

Any number of links found.

createFolder

The following parameters apply to createFolder method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
parentFolderId	Integer	Identifies the unique ID of the parent folder (zero if no parent).
repId	Integer	Identifies the unique ID of the repository.
folderType	Integer	Identifies the type of folder to be created.
description	String	Identifies the description of the folder.

Parameter	Type	Description
folderName	String	Identifies the name of the folder.

Description

Creates a new folder in the Service Desk repository that is accessed through the Attachments Library.

Note: Folder types other then 0 are hidden folders and can be viewed only by navigating to Attachments Library on the Administration tab. These folders are automatically created by the system during upload and should not be created by the user or Web Services, because their files are private and cannot be shared with other Knowledge Documents, QA or Knowledge Files.

Returns

A <UDSObject> describing the folder created, with some of the following child <Attributes> nodes:

XML Element Value	Type	Description
repository	SREL	Identifies the repository name.
parent_id	SREL	Identifies the unique ID of the parent folder.
folder_type	Integer	Identifies the type of folder created.
folder_name	String	Identifies the name of the folder.
description	String	Identifies the description of the folder.

getFolderList

The following parameters apply to getFolderList method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
parentFolderId	Integer	Identifies the unique ID of the parent folder (0 if no parent).
repId	Integer	Identifies the unique ID of the repository.

Description

Returns a list of folders under a given parent folder

Returns

A <UDSObjectList> with zero or more <UDSObject> describing the attachment folder, with some of the following child <Attributes> nodes:

XML Element Value	Type	Description
repository	SREL	Identifies the repository name.
parent_id	SREL	Identifies the unique ID of the parent folder.
folder_type	Integer	Identifies the type of folder created.
folder_name	String	Identifies the name of the folder.

XML Element Value	Type	Description
description	String	Identifies the description of the folder.

getFolderInfo

The following parameters apply to the getFolderInfo method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
folderId	Integer	Identifies the unique ID of the attachment folder.

Description

Returns the attributes of a folder.

Returns

A <UDSObject> describing the attachment folder, with some of the following child <Attributes> nodes:

XML Element Value	Type	Description
repository	SREL	Identifies the repository name.
parent_id	SREL	Identifies the unique ID of the parent attachment folder.
folder_type	Integer	Identifies the type of attachment folder.
folder_name	String	Identifies the name of the attachment folder.
description	String	Identifies the description of the attachment folder.

getAttmntList

The following parameters apply to the getAttmntList method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
folderId	Integer	Identifies the unique ID of the attachment folder.
repId	Integer	Identifies the unique ID of the repository. This parameter is required only when the folder ID is zero, which indicates the root folder.

Description

Returns a list of attachments under a given attachment folder.

Returns

A <UDSObjectList> with zero or more <UDSObject> describing the attachment, with some of the following child <Attributes> nodes:

XML Element Value	Type	Description
repository	SREL	Identifies the repository name.
parent_id	SREL	Identifies the unique ID of the parent folder.
folder_type	Integer	Identifies the type of folder created.
folder_name	String	Identifies the name of the folder.
description	String	Identifies the description of the folder.

getAttmntInfo

The following parameters apply to the getAttmntInfo method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
attmntId	Integer	Identifies the unique ID of the attachment folder.

Description

Returns the attributes of an attachment.

Returns

A <UDSObject> describing the attachment, with some of the following child <Attributes> nodes:

XML Element Value	Type	Description
id	Integer	Identifies the unique ID of the attachment.
description	String	Identifies the description of the attachment.
attmnt_name	String	Identifies the name of the attachment.
file_name	String	Identifies the name of the file.
folder_id	Integer	Identifies the unique ID of the attachment folder.
repository	SREL	Identifies the unique ID of the repository.

getRepositoryInfo

The following parameters apply to the getRepositoryInfo method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
repositoryId	Integer	Identifies the unique ID of the repository.

Description

Returns the attributes of a repository.

Returns

A <UDSObject> describing the repository, with some of the following child <Attributes> nodes:

XML Element Value	Type	Description
repository	SREL	Identifies the repository name.
parent_id	SREL	Identifies the unique ID of the parent attachment folder.
folder_type	Integer	Identifies the type of attachment folder.
folder_name	String	Identifies the name of the attachment folder.
description	String	Identifies the description of the attachment folder.

Web Services Miscellaneous Methods

This article contains the following topics:

This section describes the Web Services Miscellaneous methods.

callServerMethod

The following parameters apply to the callServerMethod method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
methodName	String	Identifies the name of the method to call.
factoryName	String	Identifies the factory name of the object type containing the method.
formatList	String	Identifies the format list, a series of characters describing the intended data types for the incoming parameters. It is related to the Parameter() description in this table).
parameters	String[]	Indicates zero or more parameter values for the method.

Description

Use this method to invoke an arbitrary server-side method. These are methods defined in the proprietary “spell” scripting language.

Only factory methods can be called and the caller must be logged in with full administrative rights.

The format list is a series of zero or more characters that indicate (in order) the data types of the parameters to follow. The character codes are as follows:

- 0 S -- string
- 0 I -- integer (covers dates and duration)
- 0 N -- null

For example, suppose a spell method is defined as follows:

```
cr::DoStuff(int in_one, string in_two, string in_three);
```

Invoke it with the following:

```
callServerMethod("DoStuff", "cr", "ISS", [3, "a string", "another one"]);
```

This method is intended for CA Development and services for customizations only; it is not recommended for most sites.

Returns

Each return message component in its own XML element. The elements are all string representations of the value. The elements are ordered in the return order from the server using the following format:

```
<ServerReturn>
   <Paramx>
```

This call does not support object reference returns. If an object reference is returned by the spell method, the return data is the string, “OBJECT”. This is not an error and any other parameters are also returned.

XML Element	Type	Description
<ServerReturn>	N/A	Indicates the outer element, which contains zero or more <ParamX> elements for return values.
<Paramx>	String	Indicates zero or more for the return values, where *x* is an integer starting at zero and increments for each return element.

You can validate BOPSIDs using check_bopsid. This is invoked with callServerMethod as follows:

```
String bopsid; // somehow gets populated with the BOPSID value
String [] stuff  = new String [] { bopsid };

String ret = usd.callServerMethod
(sid, "check_bopsid", "api", "I", stuff);
```

If the BOPSID validation fails, a SOAP Fault is returned. If validation succeeds, the return value is a small XML structure of the following form:

```
<ServerReturn>
<Param0>CONTACT_PERSID</Param0>
<Param1>SESSION_TYPE</Param1>
<Param2>SESSION_ID</Param2>
```

```
</ServerReturn>
```

- **CONTACT_PERSID**
  Defines the unique persistent id of the validated/trusted contact. It is of the form, "cnt:<uuid>".

- **SESSION_TYPE**
  Defines a small integer id indicating the type of session that generated the BOPSID. This is typically not used by integrators

- **SESSION_ID**
  Defines an optional session id. This is the id of the session that generated the BOPSID. It may or may not be set. This is useful to maintain a user's logical session within CA SDM, especially if the user is "passed" back to CA SDM by another BOPSID.

Note: If the BOPSID validation returns a success, log into CA Support Automation bypassing the login screen, else the CA Support Automation Login screen will be displayed.

createObject

The following parameters apply to the createObject method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
ObjectType	String	Identifies the type of object to create (the majic factory name).
attrVals	String[]	Identifies a sequence of name-value pairs used to set the initial attribute values for the new issue. **Note:** Dotted names are not permitted.
attributes	String[]	Identifies a sequence of attribute names from the new object for which to return values. Dot-notation is permitted. If this field is empty, all attribute values are returned.
createObjectResult	StringHolder	Identifies the String Holder object for capturing returned data. See the XML Element Return list below for details.
newHandle	StringHolder	Identifies the String Holder object for capturing returned data. See the XML Element Return list below for details.

Description

Creates a CA SDM object. The caller is responsible for setting any required fields in the *attrVals* parameter. Dotted-names are not permitted.

- **ObjectType**
  Identifies the name for an object type (factory).

- **attrVals**
  Describes the array of name-value pairs used to initialize the new object. For example, the following pseudo-code shows how to create a contact and return a <UDSObject> element with values for all its attributes:

```
String [4] attrVals;

attrVals[0] = "first_name";    // attribute name

attrVals[1] = "Edgar";

attrVals[2] = "last_name";

attrVals[3] = "Martin";

string [0] emptyArray;

CreateObject(sid, "cnt", attrVals, emptyArray, createObjectReturn, newHandle);
```

Note: Do not use this method for new assets, issues, requests, or change orders. Use the specialized createXXX() methods for those object types. This comment also applies if you are using the ITIL methodology -- use the appropriate methods to create Configuration Items, Incidents, and Problems.

Returns

A <UDSObject> element containing the new objects handle, along with attribute values specified in the *attributes* parameter. If the *attributes* parameter is empty, *all* attribute values are returned. List and LREL types are also returned, but as empty elements.

XML Element	Type	Description
<createObjectResult>	N/A	Identifies the standard UDSObject element containing the handle and requested attribute values.
<newHandle>	String	Identifies the new objects handle.

serverStatus

The following parameter applies to the serverStatus method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.

Description

Returns the status of the CA SDM server, that is, whether it is up and ready or shut down.

Note: This method executes rapidly on the server. Calling this method periodically is a good way to keep a SID active.

Returns

The following values apply:

- **1** -- Indicates the Service Desk server is not available
  Note: Any non-zero return code indicates that the server is unavailable, such as 1010.
- **0** -- Indicates the Service Desk server it is running

XML Element	Type	Description
<ServerStatus>	Integer	Identifies the value associated with the server status, zero or 1.

updateObject

The following parameters apply to the updateObject method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
objectHandle	String	Identifies the handle of a CA SDM object to update.
attrVals	String[]	Identifies the name-value pairs for the update.
attributes	String[]	Identifies the sequence of attribute names from the object for which to return values. Dot-notation is permitted. If this field is empty, all attribute values are returned.

Description

Updates one or more attributes for the specified object.

To set values for the object, the caller passes a single-dimensional array of attribute name-value pairs. The first half of the pair is an attribute name; the second is the actual value. Dotted-names are not permitted.

To update an attribute that is a Pointer type (for example, the customer field on a request) a handle must be used for the value. For Integer, Date, and Duration types, pass the string representation of an integer.

For example, to update a request with a new assignee, description and priority, the array would appear as follows:

```
[0]  -  "assignee"
[1]  -  "cnt:555A043EDDB36D4F97524F2496B35E75"  (a contact Handle)
[2]  -  "description"
[3]  -  "My new description"
[4]  -  "priority"
```

```
[5]  -  "pri:38903"  (a priority Handle)
```

If the update fails for any reason, the entire operation aborts and no changes occur.

Note: When updating a task, set the status value last in the attribute array.

Returns

A <UDSObject> element containing the updated object's handle, along with attribute values specified in the *attributes* parameter. If the *attributes* parameter is empty, *all* of the attribute values are returned. List and LREL types are also returned (see page 3980), but as empty elements.

Web Services Knowledge Management

This article contains the following topics:

To use the Web Services Knowledge Management, it is helpful if you are familiar with the database structure.

Table Types

Some of the more important tables are described as follows:

Table Type	Description
skeleton	Stores all information pertaining to documents with each row representing one document. Field names from this table can be used when passing the PropertyList and SortBy parameters to methods such as FAQ() and Search(). The field names are case-sensitive so make sure you pass them just as they are in the database.
o_indexes	Stores all information pertaining to categories with each row representing one category.

Knowledge Management General Methods

This section describes Knowledge Management general methods. Valid Knowledge document sorting properties (when available) are as follows:

- RELEVANCE
- AUTHOR_ID
- BU_RESULT
- CREATION_DATE
- DOC_TYPE_ID
- EXPIRATION_DATE
- HITS
- id
- MODIFY_DATE
- OWNER_ID
- PRIORITY_ID
- ACCEPTED_HITS
- ASSET_ID
- SD_ASSET_ID
- ASSIGNEE_ID
- PRODUCT_ID

- START_DATE
- STATUS_ID
- SUBJECT_EXPERT_ID

faq

The following parameters apply to the faq method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
categoryIds	String	Identifies the category ID used to perform the faq. Use 1 for the 'Root' category. **Note:** Multiple ids are supported, for example, "1, 2, 3".
resultSize	Integer	Identifies the number of documents for which you want to retrieve detailed information. For the rest of the documents, only their IDs return. Detailed information for these documents can be accessed later using the getDocumentsByIDs() method. The default is 10.
propertyList	String	Identifies the comma-separated list of database fields from which you want to retrieve information. The following fields are always returned, regardless of the propertyList parameter: id DOC_TYPE_ID BU_RESULT
sortBy	String	Identifies the database field that you want to use for sorting the results. Multiple sort fields are not supported. The default is BU_RESULT, meaning that the faq rating sorts it. When id is used as a secondary sort, it always sorts the results.
descending	Boolean	Identifies an indicator available for sorting the results in descending order.
whereClause	String	Use this to add your own 'SQL where clause' for filtering the results of the search.
maxDocIds	Integer	Identifies the maximum amount of document IDs to be returned (the default is 100). For example, if you specify a resultSize of 10 and a maxDocIds of 50, if there are 100 matching documents in the database, then 10 have their detailed information retrieved and 40 have just their IDs returned. The remaining 50 are not returned at all.

Description

Use to perform a faq search. Documents are retrieved based on the category ID that is passed. Any documents residing in that category or in any sub-category are returned. To improve performance, these methods only retrieve detailed information on a user-defined set of documents, which is controlled through the resultSize parameter. The rest of the documents return their IDs only. Using this method, you can for example, set up a paging mechanism where the user can click on 'Top', 'Previous', 'Next', and 'Bottom' links. When you need to retrieve the next set of information, you can use the getDocumentsByIDs() method. The maximum number of 100 IDs is returned.

Returns

A <UDSObjectList> node with the following sections:

<UDSObject> node from the <UDSObject> Node Description section of this chapter. There is a <UDSObject> node with all the given properties for the first *n* documents that the method finds where *n* equals the resultSize parameter.

For example, if the resultSize parameter is 10, the maxDocIDs parameter is 50, and the method finds 100 documents, then there are 10 <UDSObject> with <Attributes> nodes in the first<UDSObject> section with detail attribute information from propertyList parameter and 40 <UDSObject> nodes with only ID <Attributes> in the following section. If you want to retrieve detailed ID <AttrName> information for documents numbering 11-20, you have to make a call to the getDocumentsByIDs() method and pass it those IDs from <AttrValue>.

search

The following parameters apply to the search method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
problem	String	Identifies the problem description to which you want to find solutions.
resultSize	Integer	Identifies the number of documents for which you want to retrieve detailed information. The remaining documents have their IDs returned only. Detailed information for these documents can be accessed later using the getDocumentsByIDs() method. The default is 10.
propertyList	String	Identifies the comma-separated list of database fields from which you want to retrieve information. The following fields are always returned, regardless of the propertyList parameter: id DOC_TYPE_ID
sortBy	String	Identifies the database field that you want to use for sorting the results. Multiple sort fields are not supported. The default is RELEVANCE. When id is a secondary sort, it always sorts the results. For a valid sort property, see the faq method.
descending	Boolean	Identifies an indicator you can use for sorting the results in descending order.
relatedCategories	Boolean	Returns a list of all related categories for the documents found.
searchType	Integer	Type of search to perform: 1 = Natural Language Search (NLS) 2 = Knowledge Management search
matchType	Integer	Represents the type of match: 0 = OR type match 1 = AND type match 2 = Exact match **Note:** If NLS is selected for the searchType parameter, then only the OR and AND matchTypes are valid.
searchField	Integer	

Parameter	Type	Description
		Represents the binary combination of fields in which to search: Title = 1 Summary = 2 Problem = 4 Resolution = 8 For example, to search all fields, specify 15 (1+2+4+8). To search in Summary and Problem only, specify 6 (2+4). **Note:** The default is to search Problem. If you set the searchType parameter to NLS, the searchFields parameter is ignored because NLS searches can only search the Problem field.
categoryPath	String	Limits the results of the search to a specific category or categories. You need to specify the full ID path to the category and separate multiple categories with commas. For example, 1-3-5, 1-4-8 to limit the search to categories 5 and 8 (and their sub-categories).
whereClause	String	Use this to add your own 'SQL where clause' for filtering the results of the search.
maxDocIds	Integer	Represents the maximum amount of document IDs allowed to be returned. For example, if you specify a resultSize of 10 and a maxDocIds of 50, if there are 100 matching documents in the database, then 10 have their detailed information retrieved, and 40 have just their IDs returned. The remaining 50 are not returned at all. The default is 100.

Description

Searches for solutions to a problem. Documents are retrieved based on the problem that is passed. Any documents matching the description of the problem or a similar description, are returned. To improve performance, these methods only retrieve detailed information on a user-defined set of documents, which is controlled through the resultSize parameter. The rest of the documents return their ids only. Using this method, you can for example, set up a paging mechanism, where the user can click on 'Top', 'Previous', 'Next', and 'Bottom' links. When you need to retrieve the next set of information, you can use the getDocumentsByIDs() method.

Returns

A <UDSObjectList> node with the following sections:

<UDSObject> node from the <UDSObject> Node Description section of this chapter. There will be a <UDSObject> node with all the given properties for the first *n* documents that the method finds, where *n* equals the resultSize parameter. For example, if the resultSize parameter is 10, the maxDocIds parameter is 50, and the method finds 100 documents, then there are 10 <UDSObject> nodes with all the properties requested in the <Attributes> section and 40 <UDSObject> with only the ID property in the <Attributes> section. If you want to retrieve detailed <UDSObject> information for documents 11-20, you need to make a call to the getDocumentsByIDs() method and pass it those IDs.

If the getRelatedCategories parameter is set to True, the <UDSObjectList> node is included in the <Attributes> section for related categories. Each <INDEX_DOC_LINKS> node contains the relational ID of the category, as shown by the following example:

```
1-70
```

doSelectKD

The following parameters apply to the doSelectKD method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
whereClause	String	(Optional) Identifies the where clause for the query.
sortBy	String	Identifies the database field that you want to use for sorting the results. Multiple sort fields are not supported. The default is BU_RESULT, meaning that the faq rating sorts it. When id is used as the secondary sort, it always sorts the results.
desc	Boolean	Identifies the indicator available for sorting the results in descending order. Use True for descending and False for ascending the document order.
maxRows	Integer	Indicates the maximum number of rows to return. Specify -1 to return all rows. **Note:** Regardless of the integer specified, CA SDM will return a maximum of 250 rows per call.
attributes	String[]	Identifies the attribute list from which to fetch values. Dotted-attributes are permitted. If this field is blank, all value-based attributes are returned. These attributes cannot be defined as LOCAL in the majic definition file. LOCAL attributes are temporal; they have no database storage.
skip	Integer	Identifies the number of knowledge documents to skip from the beginning. Enter zero (0) to return all documents.

Description

Performs an SQL-like select on a Knowledge Document table. Supply one or more attributes you want fetched from the objects that match the supplied where clause.

Returns

A sequence of <UDSObject> elements. The following format applies:

```
<UDSObjectList>
<UDSObject>
 <Handle>
 <Attributes>
<AttributeName0>
<AttributeName1>
```

XML Element	Type	Description
<UDSObject>	Sequence	Contains a <Handle> element and an <Attributes> sequence.
<UDSObjectList>		Signifies the outer element, which contains a sequence of <UDSObject (see page 3980)> elements.

createDocument

The following parameters apply to the createDocument method:

Parameter	Type	Description
SID	String	Identifies the session retrieved from logging in.
kdAttributes	String[]	Identifies an array of name-value pairs used to set the initial attribute values for the new Knowledge document, as illustrated by the following: `"SUMMARY","Summary text",` "TITLE","Title text"

As part of the createDocument method, the following table reflects examples of valid, commonly used attribute values for a document. Data in the Type column reflect the actual type, which must be parsed to the method in string format in the attrVals string array.

Attribute Value	Type	Description
PRIMARY_INDEX	Integer	Identifies the category ID in which to create the document. Use 1 for the *Root* category.
USER_DEF_ID	String	Identifies any ID that you would like to use to represent the document.
TITLE	String	Identifies the title of the document.
SUMMARY	String	Identifies the summary of the document.
PROBLEM	String	Identifies the problem of the document.
RESOLUTION	String	Identifies the resolution of the document. This can contain html.
STATUS_ID	Integer	Identifies the status ID for the document. The default is 10 (Draft).
PRIORITY_ID	Integer	Identifies the priority ID for the document. The default is 20 (Normal).
CREATION_DATE	Date (String)	Identifies the date and time the document was created. Leave blank to assign current date.
MODIFY_DATE	Date (String)	Identifies the date and time the document was last modified. Leave blank to assign the current date.
START_DATE	Date (String)	Identifies the date the document becomes active and is used in conjunction with Expiration_Date. Leave blank to specify no start date and the document will be active as long as the expiration date has not been reached.

Attribute Value	Type	Description
EXPIRATION_DATE	Date (String)	Identifies the date the document expires, and it is used in conjunction with Start_Date. Leave blank to specify no expiration date.
PUBLISHED_DATE	Date (String)	Identifies the date and time the document was published. Leave blank to assign current date if the status is Published. If the status is not Published, this parameter is ignored.
SD_PRODUCT_ID	Integer	Identifies the product ID from CA SDM with which to associate this document.
ASSIGNEE_ID	UUID	Identifies the unique assignee ID from CA SDM to which this document is assigned.
SD_ASSET_ID	UUID	Identifies the asset ID from CA SDM with which to associate this document.
SD_ROOTCAUSE_ID	Integer	Identifies the root cause ID from CA SDM with which to associate this document.
SD_PRIORITY_ID	Integer	Identifies the priority ID from CA SDM with which to associate this document.
SD_SEVERITY_ID	Integer	Identifies the severity ID from CA SDM with which to associate this document.
SD_IMPACT_ID	Integer	Identifies the impact ID from CA SDM with which to associate this document.
SD_URGENCY_ID	Integer	Identifies the urgency ID from CA SDM with which to associate this document.
AUTHOR_ID	UUID	Identifies the unique ID of the contact who authored this document. If the author is not an internal contact, you can set this field to zero and use the Author parameter instead.
OWNER_ID	UUID	Identifies the unique ID of the contact who owns this document.
SUBJECT_EXPERT_ID	UUID	Identifies the unique ID of the contact who is the subject expert for this document.
NOTES	String	Identifies the notes for the document.
READ_GROUP_LIST	String	Identifies the dash-separated list of group IDs that have read permission for this document (for example: 1-3-4). Use *A* to assign permission to everyone.
WRITE_GROUP_LIST	String	Identifies the dash-separated list of group IDs that have write permission for this document (for example: 1-3-4). Use *A* to assign permission to everyone.
INHERITPERMISSIONS	Boolean	Indicates the status of the flag to inherit permissions from the category in which the document is being created. Set to True if you want to inherit permissions, and then ReadPermissions and the WritePermissions parameters will be ignored.

Attribute Value	Type	Description
DOC_TYPE_ID	Integer	Identifies the ID for the type of document that this document will be; a regular document or a tree document. The default is a regular document.
HITS	Integer	Identifies the number of times that the document has been viewed.
DOC_TEMPLATE_ID	Integer	Identifies the ID for the template you want to assign to this document.
WF_TEMPLATE	Integer	Identifies the ID for the workflow template you want to assign to this document.
CUSTOM1	String	Specifies a custom field.
CUSTOM2	String	Specifies a custom field.
CUSTOM3	String	Specifies a custom field.
CUSTOM4	String	Specifies a custom field.
CUSTOM5	String	Specifies a custom field.
CUSTOM_NUM1	Double	Specifies a numeric custom field.
CUSTOM_NUM2	Double	Specifies a numeric custom field.

Description

Creates a new document.

Returns

A <UDSObject> node describing the Knowledge Document created.

modifyDocument

The following parameters apply to the modifyDocument method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
docId	Integer	Identifies the unique ID of the document you want to modify.
kdAttributes	String[]	Specifies the name-value pairs for the update, for example, “SUMMARY”, ”Summary text”, “TITLE”, and “Title text”.

As part of the modifyDocument method, the following table reflects examples of valid, commonly used attribute values for a document. Data in the Type column reflect the actual type, which must be parsed to the method in string format in the attrVals string array.

Parameter	Type	Description
MODIFY_DATE	(String)	Indicates a special field used for "record locking" purposes to make sure that someone else is not updating the document at the same time that you are. You must pass in the existing MODIFY_DATE of the document. If you leave the modify date blank, you receive an error that another user has updated the document.
USER_DEF_ID	String	Specifies any ID that you want to use to represent the document.
TITLE	String	Indicates the title of the document.
SUMMARY	String	Indicates the summary of the document.
PROBLEM	String	Indicates the problem of the document.
RESOLUTION	String	Indicates the resolution of the document. This can contain html.
STATUS_ID	Integer	Indicates the status ID for the document. The default is 10 (Draft).
PRIORTY_ID	Integer	Indicates the priority ID for the document. The default is 20 (Normal).
START_DATE	Date (String)	Indicates the date that the document becomes active, which is also used in conjunction with ExpirationDate. Leave blank to specify no start date and the document becomes active as long as the expiration date is not exceeded.
EXPIRATION_DATE	Date (String)	Indicates the date that the document expires, which is used in conjunction with StartDate. Leave blank to specify no expiration date.
SD_PRODUCT_ID	Integer	Indicates the product ID from CA SDM with which to associate this document.
ASSIGNEE_ID	UUID	Indicates the unique ID from CA SDM to which this document is assigned.
SD_ASSET_ID	UUID	Indicates the asset ID from CA SDM with which to associate this document.
SD_ROOT CAUSE_ID	Integer	Indicates the root cause ID from CA SDM with which to associate this document.
SD_PRIORITY_ID	Integer	Indicates the priority ID from CA SDM with which to associate this document.
SD_SEVERITY_ID	Integer	Indicates the severity ID from CA SDM with which to associate this document.
SD_IMPACT_ID	Integer	Indicates the impact ID from CA SDM with which to associate this document.
SD_URGENCY_ID	Integer	Specifies the urgency ID from CA SDM with which to associate this document.

Parameter	Type	Description
AUTHOR_ID	UUID	Identifies the unique ID of the contact who authored this document. If the author is not an internal contact, you can set this filed to zero (0) and use the Author parameter instead.
OWNER_ID	UUID	Identifies the unique ID of the contact who owns this document.
SUBJECT_EXPERT_ID	UUID	Indicates the unique ID of the contact who is the subject expert for this document.
NOTES	String	Indicates notes for the document.
READ_GROUP_LIST	String	Indicates the dash-separated list of group ids that have read permission for this document (for example: 1-3-4). Use *A* to assign permission to everyone.
WRITE_GROUP_LIST	String	Indicates the dash-separated list of group IDs that have write permission for this document (for example: 1-3-4). Use *A* to assign permission to everyone.
INHERIT_PERMISSION	Boolean	Indicates the status of the inherit permissions flag. Set to True if you want to inherit permissions from the category in which the document is being created. If set to True, the ReadPermissions and WritePermissions parameters are ignored.
DOC_TYPE_ID	Integer	Identifies the ID for the type of document that this document is to become; a regular document or a tree document. The default is a regular document.
HITS	Integer	Indicates the number of times that the document has been viewed.
DOC_TEMPLATE_ID	Integer	Identifies the ID for the template you want to assign to this document.
WF_TEMPLATE	Integer	Identifies the ID for the workflow template you want to assign to this document.
WF_ACTION	String	Identifies the action for the workflow you want to assign to this document. For example, wf_unpublish lets the document become unpublished.
WF_COMMENT	String	Identifies the comment for the workflow you want to assign to this document. For example, unpublish.
WF_CONTACT_ID	UUID	Identifies the user id for the workflow you want to assign to this document.
WF_REJECT_TO_ID	Integer	Identifies the task id for the workflow you want to assign to this document, matching its approval process. Task ids are stored in the CI_ACTIONS table.
CUSTOM1	String	Indicates a custom field.
CUSTOM2	String	Indicates a custom field.
CUSTOM3	String	Indicates a custom field.
CUSTOM4	String	Indicates a custom field.
CUSTOM5	String	Indicates a custom field.

Parameter	Type	Description
CUSTOMNUM1	Double	Indicates a numeric custom field.
CUSTOMNUM2	Double	Indicates a numeric custom field.

Description

Modifies a document.

Returns

A <UDSObject> node describing the Knowledge Document modified.

deleteDocument

The following parameters apply to the deleteDocument method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
docId	Integer	Identifies the unique ID of the document you want to delete.

Description

Flags a document for deletion. The Knowledge Management Windows Service permanently deletes the document.

Returns

Returns error codes only when there are *individual* errors. For additional information, see Error Codes.

Use the Knowledge Management Web Services

The login process and any error codes that may display for the Knowledge Management Web Services are the same as those found for the CA SDM Web Services. For additional information, see Login and Error Codes.

Access the Knowledge Management Web Services

The Knowledge Management Web Services uses Apache Axis implementation of standards set forth by the W3C. Ideally, a client on any type of platform should be able to access the services, but vendor implementations vary. For example, Java and .NET both provide tools for generating proxy classes from a WSDL service description. If you experience any issues using the Web Services with a different technology, consult your platform vendor or Microsoft's knowledge base.

addComment

The following parameters apply to the addComment method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
comment	String	Identifies the comment to add.
docId	Integer	Identifies the document ID for the comment you want to add.
email	String	Indicates the email address of the person who submitted the comment. Leave blank if you want the email address retrieved from the database based on the user ID parameter.
username	String	Indicates the user name of the person who submitted the comment. Leave blank if you want the user name retrieved from the database based on the user id parameter.
contactId	String	Indicates the ID of the person submitting the comment. If this contact ID exists in the database, the associated email and user name are retrieved and placed in the email and user name fields. If this ID does not exist, the email and user name parameters are used instead, if supplied. Use zero (0) if you are not using this parameter. Contact ID is UUID in string format.

Description

Adds a comment to a particular document.

Returns

A <UDSObject> node with the following<Attributes> child nodes describing the comment most recently added:

XML Element Value	Data Type	Description
id	Integer	Identifies the unique identifier for the comment most recently added.
DOC_ID	Integer	Identifies the document ID for the comment most recently added.
USER_ID	Integer	Identifies the ID of the person who submitted the comment.
USER_NAME	String	Identifies the user name of the person who submitted the comment.
EMAIL_ADDRESS	String	Identifies the email address of the person who submitted the comment.
COMMENT_TEXT	String	Identifies the text for the comment recently added.
COMMENT_TIMESTAMP	Date	Identifies the date and time the comment was added.

deleteComment

The following parameters apply to the deleteComment method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
commentId	Integer	Identifies the unique ID for the comment you want to delete.

Description

Deletes a comment.

Returns

Returns error codes only for *individual* errors. For additional information, see Error Codes.

rateDocument

The following parameters apply to the rateDocument method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
docId	Integer	Identifies the document ID to rate.
rating	Integer	Identifies the rating to give the document (a scale of 0-4, where 0 is the worst and 4 is the best).
multiplier	Integer	Identifies the multiplier parameter. This parameter can be used to simulate many ratings at once. Use the default of 1 for a single rating and any other number for multiples. For example, if you submit 3, it acts as if you called the method 3 times. Three ratings with the value you supplied in the rating parameter is added to the database.
ticketPerId	String	Identifies the persistent ID of a ticket related to this Knowledge document.
onTicketAccept	Boolean	Identifies whether the document was accepted as a solution for the ticket.
solveUserProblem	Boolean	Identifies whether this document solved the user's problem. It signifies how the user responded to the question "Did this document solve your problem?" on the Solution Survey.
isDefault	Boolean	Indicates a default rating status. If you are setting the rating just because the user viewed the document and not because he actually rated it, set this to True. This is used for reporting reasons.

Description

Rates a particular document.

Returns

A <UDSObject> node with the following <Attributes> children nodes describing the rating BU_TRANS :

XML Element Value	Data Type	Description
id	Integer	Identifies the unique identifier for the rating most recently added. Use this with the updateRating() method if you want to modify the rating at a later time.
DOC_ID	Integer	Identifies the document ID.
INDEX_ID	Integer	Identifies the category ID.
BU_RATING	String	Identifies the rating given to the document.
HIT_NO_VOTE	Integer	Identifies the rating set because a user viewed the document and not actually rated it, or vice versa.

updateRating

The following parameters apply to the updateRating method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
buID	Integer	Identifies the unique ID of the rating you want to modify. This ID is returned by the rateDocument() method.
rate	Integer	Identifies the new rating to apply to the document (a scale of 0 -- 4, where 0 is the worst and 4 is the best).

Description

Updates one of the ratings of a particular document.

Returns

A <UDSObject> node describing BU_TRANS with the updated rating attribute.

getQuestionsAsked

The following parameters apply to the getQuestionsAsked method:

Parameter	Type	Description
SID	String	Identifies the session retrieved from logging in.
resultSize	Integer	Identifies the number of searched text for which you want to retrieve detailed information.
Descending	Boolean	Indicates an option available for sorting the results in descending order of the ASKED_DATE.

Description

Retrieves historical Knowledge document search text.

Returns

A <UDSObjectList> node with zero or more <UDSObject> nodes describing EBR_LOG with the following <Attributes> child nodes:

XML Element Value	Data Type	Description
id	Integer	Indicates the unique identifier of the question asked.
SEARCH_TEXT	Integer	Indicates the search text of the question asked.

getBookmarks

The following parameters apply to the getBookmarks method:

Parameter	Type	Description
SID	String	Identifies the session retrieved from logging in.
contactId	String	Identifies the unique ID of the contact for which you want to retrieve bookmarks. Contact ID is UUID in string format.

Description

Retrieves bookmarks for a particular contact.

Returns

A <UDSObjectList> node with zero or more <UDSObject> nodes describing CI_BOOKMARKS with the following <Attributes> child nodes:

XML Element Name	Type	Description
DOCUMENT_ID	Integer	Identifies the unique ID of the document.
id	Integer	Identifies the bookmark ID
USER_ID	String	Identifies the user ID for the owner of this bookmark.
BOOKMARK_TITLE	String	Identifies the bookmark title from the document.

addBookmark

The following parameters apply to the addBookmark method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
contactId	String	Identifies the unique ID of the contact for which you want to retrieve bookmarks. Contact ID is UUID in string format.
docId		Identifies the document ID you want to bookmark.

Parameter	Type	Description
	Integer	

Description

Adds a bookmark for a particular contact.

Returns

A <UDSObject> node describing the newly created bookmark.

deleteBookmark

The following parameters apply to the deleteBookmark method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
contactId	String	Identifies the unique ID of the contact for which you want to delete a bookmark. Contact ID is UUID in string format
docId	Integer	Identifies the document ID of the bookmark you want to remove.

Description

Deletes a bookmark for a particular contact.

Returns

Returns error codes only for *individual* errors. For additional information, see Error Codes.

getStatuses

The following parameter applies to the getStatuses method:

Parameter	Type	Description
SID	String	Identifies the session retrieved from logging in.

Description

Retrieves the list of statuses.

Returns

A <UDSObjectList> node with zero or more <UDSObject> nodes describing CI_STATUSES with the following <Attributes> child nodes:

XML Element Values	Data Type	Description
id	Integer	Identifies the unique ID of the status.
STATUS	String	Identifies the name for the status.
STATUS_DESCRIPTION	String	Identifies the description for the status.
PREDEFINED	Integer	Indicates whether the status is predefined by the Knowledge Management system, meaning that it cannot be deleted.
STATUS_ORDER	Integer	Describes the order by which the status should appear in the Workflow task list. Workflows can only be created when they follow this order.

getPriorities

The following parameter applies to the getPriorities method:

Parameter	Type	Description
SID	String	Identifies the session retrieved from logging in.

Description

Retrieves the list of priorities.

Returns

A <UDSObjectList> node with zero or more <UDSObject> nodes describing CI_PRIORITIES with the following <Attributes> child nodes:

XML Element Values	Data Type	Description
id	Integer	Identifies the unique ID of the priority.
PRIORITY	String	Identifies the name for the priority.

getDocumentTypes

The following parameter applies to the getDocumentTypes method:

Parameter	Type	Description
SID	String	Identifies the session retrieved from logging in.

Description

Retrieves the list of document types.

Returns

A <UDSObjectList> node with zero or more <UDSObject> nodes describing CI_DOC_TYPES with the following <Attributes> child nodes:

XML Element Values	Data Type	Description
id	Integer	Identifies the unique ID of the document type.
DOC_TYPE_TXT	String	Identifies the name for the document type.

getTemplateList

The following parameter applies to the getTemplateList method:

Parameter	Type	Description
SID	String	Identifies the session retrieved from logging in.

Description

Retrieves the list of document templates

Returns

A <UDSObjectList> node with zero or more <UDSObject> nodes describing CI_DOC_TEMPLATES with the following <Attributes> child nodes:

XML Element Value	Type	Description
id	Integer	Identifies the unique ID of the document type.
TEMPLATE_NAME	String	Identifies the name for the document template.
IS_PREDEFINED	Integer	Indicates whether the template is predefined by the Knowledge Management system and cannot be deleted.
IS_DEFAULT	Integer	Indicates whether the template is the default that will be assigned to new documents.

getWorkflowTemplateList

The following parameter applies to the getWorkflowTemplateList method:

Parameter	Type	Description
SID	String	Identifies the session retrieved from logging in.

Description

Retrieves the list of workflow templates.

Returns

A <UDSObjectList> node with zero or more <UDSObject> nodes describing WF_TEMPLATE with the following <Attributes> child nodes:

XML Element Value	Type	Description
id	Integer	Identifies the unique ID of the workflow template.
WF_NAME	String	Identifies the name for the workflow template.
WF_DESCRIPTION	String	Identifies the description for the workflow template.
IS_DEFAULT	Integer	Indicates that the default template is to be assigned to new documents.

getCategory Method

This article contains the following topics:

The following parameters apply to the getCategory method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
categoryId	Integer	Identifies the category ID in which to create the document.
getCategoryPaths	Boolean	Indicates the path for which to get category information. It returns category information and the full text category path for each category.

Description

Retrieves information for a category, including a listing of all of its child categories.

Returns

A <UDSObjectList> node with an <UDSObject> node describing the category requested.

getPermissionGroups

The following parameters apply to the getPermissionGroups method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
groupID	Integer	Returns only the group with this ID. Pass zero (0) when you do not want to use this parameter. **Note:** This groupID relates to a knowledge category, and differs from the groupID for contacts.

Description

Retrieves the list of Permission Groups.

Returns

A <UDSObject> node with zero or more <UDSObject> nodes describing Permission Group with the following <Attributes> child nodes:

XML Element Value	Type	Description
id	Integer	Identifies the unique ID of the group.
GRP_LIST_KEY	String	Shows a list of the IDs of CA SDM groups, separated by commas.
GRP_LIST	String	Displays a field containing the entire group list.

getComments

The following parameters apply to the getComments method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
docIds	String	Identifies the document IDs for all the comments you want to retrieve. **Note:** Use commas to separate, for example, "400001,400002".

Description

Gets all the comments from documents.

Returns

A <UDSObjectList> node with zero or more <UDSObject> nodes describing O_COMMENTS with the following <Attributes> child nodes:

XML Element Value	Data Type	Description
id	Integer	Identifies the unique identifier for the comment most recently added.
DOC_ID	Integer	Identifies the document IDs for the comment recently added.

XML Element Value	Data Type	Description
USER_ID	Integer	Identifies the ID of the person who submitted the comment.
USER_NAME	String	Identifies the user name of the person who submitted the comment.
EMAIL_ADDRESS	String	Identifies the email address of the person who submitted the comment.
COMMENT_TEXT	String	Identifies the text for the comment recently added.
COMMENT_TIMESTAMP	Date	Identifies the date and time the comment was added.

getDecisionTrees

The following parameters apply to the getDecisionTrees method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
propertyList	String	Identifies the comma-separated list of database fields for which you want to retrieve information. The following fields are always returned, regardless of the propertyList parameter: id DOC_TYPE_ID BU_RESULT
sortBy	String	Identifies the database field that you want to use for sorting the results. The default is id. Multiple sort fields are not supported. If you specify another field, id as a secondary sort always sorts the results.
descending	Boolean	Identifies an indicator available for sorting the results in descending order.

Description

Retrieves all Decision Trees. Decision trees are Knowledge Documents that provide users with resolutions after answering specific questions on the document.

Returns

A <UDSObjectList> node with the following sections:

```
<UDSObject> nodes with requested <Attributes> nodes
```

getDocument

The following parameters apply to the getDocument method:

Parameter	Type	Description
SID		Identifies the session retrieved from logging in.

Parameter	Type	Description
	Integer	
docId	Integer	Identifies the document ID to retrieve.
propertyList	String	Identifies the comma-separated list of database fields from which you want to retrieve information. Leave blank to retrieve all fields.
relatedDoc	Boolean	Indicates whether to retrieve a list of documents that are related to this document.
getAttmnt	Boolean	Indicates whether to retrieve the list of attachments and URL links for the document.
getHistory	Boolean	Indicates whether you want to retrieve the complete history for the document.
getComment	Boolean	Indicates whether you want to retrieve all comments for the document.
getNotiList	Boolean	Indicates whether you want to retrieve the email notification list for the document.

Description

Retrieves information for a document.

Returns

A <UDSObject> node, as described in the <UDSObject> Node Description, with requested <Attributes> provided by the propertList parameter.

getDocumentsByIDs

The following parameters apply to the getDocumentsByIDs method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
docIds	String	Identifies the comma-separated list of document IDs to retrieve.
propertyList	String	Identifies the comma-separated list of database fields for which you want to retrieve information. The following fields are always returned, regardless of the propertyList parameter: id DOC_TYPE_ID BU_RESULT
sort By	String	Identifies the database field that you want to use for sorting the results. The default is id, but multiple sort fields are not supported. If you specify another field, id as a secondary sort always sorts the results.
descending	Boolean	Identifies an indicator available for sorting the results in descending order.

Description

Retrieves information on one or more documents by passing the document IDs for which you want to retrieve information. This is usually used after calling the faq() or search() methods. In order to improve performance, these methods only retrieve detailed information on a user-defined set of documents. The rest of the documents return their IDs only. For example, you can set up a paging mechanism, where the user can click on Top, Previous, Next, and Bottom links. When you need to retrieve the next set of information, you can use the getDocumentsByIDs() method.

Returns

A <UDSObjectList> node with the following section:

```
<UDSObject> nodes with requested <Attributes> nodes describing Knowledge Document
```

You should pass the IDs into the getDocumentsByIDs() docIds parameter in this same format.

getBopsid

The following parameters apply to the getBopsid method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
contact	String	Identifies the name of the user associated with the returned BOPSID. **Note:** This is the system login name, not the CA SDM contact name.

Description

Facilitate the building of Web Interface URLs, which may be used to launch the Web Interface in the context of a given user without a login challenge. The URL may look similar to the following:

```
http://host/CAisd/pdmweb.exe?BOPSID=nnnnn+OP=xxxx...
```

To launch the Web Interface in the context of a given user (for example, an analyst), a calling application must first construct a Web Interface URL, which includes a BOPSID token (a web-interface security token). Failure to provide a BOPSID token may result in an interactive login challenge when attempting to launch the Web Interface in the chosen context (such as, a detail view of a given ticket). The getBopsid method allows the BOPSID to be generated in the context of the user provided by the Name parameter. If the Name parameter is not provided, it uses the user associated with the current Web Interface BOPSID.

Note: To prevent unauthorized elevation of privileges, the BOPSID of the current login must have equal or greater access rights than the name of the user entered.

Returns

A BOPSID based on the name of the user entered. You must use the BOPSID to launch the Web Interface within 30 seconds of it being generated.

Note: The BOPSID of the current login must have equal or greater access rights than the name of the user entered.

getConfigurationMode

The following parameters apply to the getConfigurationMode method:

Parameter	Type	Description
SID	Integer	Identifies the SID of the current login session.

Description

This method returns a string indicating if the CA SDM installation is in the ITIL mode.

Returns

A string "itil" if the installation is in ITIL mode. Otherwise, an empty string is returned.

getObjectValues

The following parameters apply to the getObjectValues method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
objectHandle	String	Identifies the handle of a CA SDM object to query.
attributes	String[]	Identifies the names of attributes to fetch. If this field is empty, all the attributes for the object are returned. **Note:** Dot-names for attributes are only supported for SREL type attributes, and not for LREL/BREL/QREL type attributes.

Description

This method returns the attribute values of an object. The caller passes one or more attribute names to fetch the object and dotted-names are permitted.

All values are returned as a string. Empty/null attributes are returned as empty strings.

Returns

A <UDSObject (see page 3980)> element.

XML Element	Type	Description
<UDSObject>	N/A	Contains a <Handle> element and zero or more <AttributeNameX> elements.

getObjectTypeInformation

The following parameters apply to the getObjectTypeInformation method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
factory	String	Identifies the object type (known as 'factory') to query. This is the majic name of the object, for example: "cr" = Request

Description

A list of all attribute names for a given object type, along with type information for each attribute. Information returned for the attribute's type includes the Integer, String, Date, Pointer, List, and so on, if the attribute is required for back-storing its storage space requirements (if appropriate).

Callers should cache the type information requested per object type to avoid multiple, redundant (and expensive) calls. The attribute information can change only after modifications are performed on the CA SDM server and the service is recycled.

Returns

The following:

XML Element	Type	Description
<UDSObject>	N/A	Indicates the root node.
<Attributes>	Sequence	Indicates zero or more elements for each attribute.
<attrName DataType="dataType" Size="storageSize" Required="Boolean" Factory="factoryName">	EmptyElement	Indicates an element with a name matching an object attribute name. The element has several attributes: **DataType**Signifies the integer representation of the data type. **Size**Represents the maximum size needed to store this attribute in a string. **Required**Represents the flag status of True if this attribute must be set for the object to back store. **Factory**Represents the Type name of the object if the attribute is a List, Lrel or Pointer type. It is not written unless it is a Llist, Lrel, or Pointer type data type.

getArtifact

The following parameters apply to the getArtifact method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.

Parameter	Type	Description
contact	String	Identifies the name of the user associated with the returned ARTIFACT. **Note:** This is the system login name, not the contact name for CA Service Desk Manager.
password	String	Identifies the password.

Description

Facilitates the building of Web Interface URLs, which may be used to launch the Web Interface in the context of a given user without a login challenge. The URL may look similar to the following:

```
http://host/CAisd/pdmweb.exe?USERNAME=xxxxx+ARTIFACT=nnnnn+OP=xxxx....
```

To launch the Web Interface in the context of a given user (for example, an analyst), a calling application must first construct a Web Interface URL, which includes an CA EEM ARTIFACT token (a web-interface security token). Failure to provide a CA EEM ARTIFACT token may result in an interactive login challenge when attempting to launch the Web Interface in the chosen context (such as, a detail view of a given ticket). The getArtifact method allows the CA EEM ARTIFACT to be generated in the context of the user provided by the contact parameter.

Note: Service Desk needs to be integrated with CA EEM to perform this operation.

Returns

An CA EEM ARTIFACT based on the name of the user entered. You can use the ARTIFACT to launch the Web Interface only once.

LREL Methods

This article contains the following topics:

LREL methods supply information about object relationships. Objects with relationships have a left-hand side (lhs) and right-hand side (rhs) definition to describe many-to-many relationships. Some examples of many-to-many relationships include the following:

- Issues and configuration items
- Contacts and configuration items
- Task types and status codes

When working with LREL methods, the BREL or LREL attribute describe many-to-many relationships. The BREL attribute replaces the LREL attribute to define many-to-many relationships. However, the LREL attribute remains backward compatible with previous releases. You declare each relationship in a .maj file and then your code uses the LREL methods, such as *CreateLrelRelationship()*, with the existing web service client code.

Note: When working with group object management, you can use the special web methods to define a member that belongs to a group.

You declare the relationship using the BREL attribute to define relationships in majic files. For example, the following statement declares a many-to-many relationship for the Change Order (chg) object in change.maj:

```
asset BREL lrel_asset_chgnr chg {LREL nr;};
```

The *BREL* attribute for the change order named, "asset" is a list of all associated configuration items. The optional, LREL flag is an attribute that describes a set of owned resources. The corresponding majic definition of the Configuration Item (nr) includes the following:

```
chgnr BREL lrel_asset_chgnr nr {LREL chg;};
```

The *chgnr* attribute is a list of all change orders for a configuration item.

In your code, you can discover how many configuration items are associated with a change order, call *getLrelLength()* with the following parameters:

```
getLrelLength(sid, ChangeHandle, "asset")
```

You use the *sid* parameter for the Service ID from a login method. The *ChangeHandle* parameter is a string handle to a particular change order. Similarly, the following statement describes how to get the names of all configuration items that are related to a change order:

```
String attrs[] = {"name"};
getLrelValues(sid, ChangeHandle, "asset", 0, -1, attrs);
```

The *getLrelValues()* method provides the relationships in the *attrs* array.

Note: For more information about LREL tables and objects, see the Data Element Dictionary and Objects and Attributes.

getLrelLength

The following parameters apply to the getLrelLength method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
contextObject	String	Identifies the object on one side of the LREL.
LrelName	String	Identifies the LrelName. Use the name.

Description

Returns the number of objects on one side of a many-to-many relationship:

- **contextObject**
  Specifies it as a handle to an object on one side of the LREL relationship.
- **LrelName**
  Specifies it as the name of the side of the relationship identified by *ObjHandle*.

Returns

The following:

XML Element	Type	Description
<Length>	Integer	Specifies the number of objects.

getLrelValues

The following parameters apply to the getLrelValues method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
contextObject	String	Identifies the object on one side of the LREL.
LrelName	String	Identifies the Lrel Name. Use the name.
startIndex	Integer	Identifies the position in the “list” from which to begin fetching.
endIndex	Integer	Identifies the Last “list” position from which to fetch. Specify -1 to fetch all rows from startIndex.
attributes	String[]	Identifies an array of one or more attribute names for which to fetch values.

Description

Returns attribute values for a range of objects in an LREL relationship. Remember that items involved in an LREL relationship have no specific ordering. In fact, it is not really a “list”, as defined in this document.

The start and end index parameters are there to help throttle a large number of items. The format is as follows:

```
< UDSObjectList >
   <UDSObject>
   <Handle>
   <AttributeName0>
   <AttributeName1>
```

Returns

This method has the following returns:

XML Element	Type	Description
<UDSObjectList>	Array	Specifies the outer element, which contains a sequence of <UDSObject> elements.
<UDSObject (see page 3980)>	Sequence	Contains a <Handle> element and zero or more *<AttributeNameX>* elements.

createLrelRelationships

The following parameters apply to the createLrelRelationships method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
contextObject	String	Identifies the object on one side of the LREL.
LrelName	String	Identifies the Lrel Name as seen by *contextObject*.
addObectHandles	String []	Identifies the handles of objects for the other side of the LREL relationships.

Description

Adds one or more many-to-many relationships. *contextObject* is one side of the LREL relation. The caller passes one or more object handles for the other side.

If a relationship already exists between the two objects, no change is made and the system continues to process the *addObjectHandles* array. If an invalid object handle is passed, the entire operation is canceled.

The following example shows how to add several assets to a contact's environment:

```
createLrelRelationships(sid, ContactHandle, "cenv",
 ["nr:655A043EDDB36D4F97524F2496B35E75", "nr:755A043EDDB36D4F97524F2496B35E75"])

ContactHandle is a string handle to a contact, and
"nr:655A043EDDB36D4F97524F2496B35E75" and
 "nr:755A043EDDB36D4F97524F2496B35E75" are Asset handles.
```

Returns

Nothing.

removeLrelRelationships

The following parameters apply to the removeLrelRelationships method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
contextObject	String	Identifies the object on one side of the LREL.
LrelName	String	Identifies the Lrel Name (as seen by *contextObject).*
removeObjectHandles	String[]	Identifies the handles of objects to remove from the other side of the LREL relationships.

Description

Removes one or more many-to-many relationships. *contextObject* is one side of the LREL relationship. The caller passes one or more object handles for the other side.

It is not an error if no relationship existed between the two objects. If an invalid object handle is passed, the entire operation is canceled.

For a usage example, see createLrelRelationships() in this chapter.

Returns

Nothing.

dbmonitor_nxd--Database Monitoring Daemon

The Database Monitoring daemon (dbmonitor_nxd) provides a mechanism to allow CA SDM cache of specific database tables to be refreshed when changes are made externally from CA SDM.

The main function of dbmonitor_nxd is to generate CHANGE notifications for changes in specified tables that did not occur through CA SDM. In order to perform this function, the monitor periodically queries the database, determines what was changed externally and then sends CHANGE notifications to the bpvirtdb_nxd server. The bpvirtdb_nxd server notifies all domsrvr servers of the change, which causes each domsrvr to update its cache of specific database objects and then notify all other processes that subscribe for changes in the specified tables.

This mechanism works well for the occasional external change in tables that are monitored. However, in cases where mass updates are made externally a storm of CHANGE notifications are broadcast which leads to many database queries from various CA SDM processes which significantly impacts CA SDM's performance.

In order to eliminate this impact on CA SDM performance, dbmonitor_nxd has been updated for this release of the product. The Monitor supports a command line interface that allows the user to start and stop the monitoring of specified tables.

Syntax

This command has the following format:

```
dbmonitor_nxd  -c <command> -t <tables>
```

- **<command>**
  Enter start or stop.

- **<tables>**
  Specifies a table name or a comma delimited list of table names that must match one or more of the tables specified in the NX_DBMONITOR_TABLES environment variable.

Each request is sent to the dbmonitor_nxd daemon. The daemon takes the appropriate action and returns a message to the user indicating the action taken.

- If a start request is invoked for a table that is already started, no action is taken.
- If a stop request is made for a table that is already stopped, no action is taken.
- If monitoring is successfully stopped or started for a table, a log message is also written to stdlog.

Note: When the Monitor is paused for a table, all CA SDM processes that cache data from these tables may become out of date and no provision is made to update this cache.

For example, BOPLGIN caches Contact records (from the ca_contact and usp_contact tables) and this cache would not be updated if the Monitor was paused for the ca_contact table during the time external updates were loaded into the database. In the BOPLGIN case this will have little consequence because the essential Contact attributes cached in BOPLGIN are taken from the usp_contact table and not the ca_contact table.

Note: When the Monitor is paused for a table, Web Users will not be able to see changes in the table while viewing a detail form that were made externally while the Monitor was paused.

List/Query Methods

This article contains the following topics:

- getPendingIssueTaskListForContact (see page 4064)
- getNotificationsForContact (see page 4064)

Two paradigms are available for working with lists. One paradigm uses a list handle for referring to and making queries on a server-side list and the other simply performs a SQL-like select.

If you need to maintain reference to a static list, use the methods that return list handles. These methods are especially useful when working with very large lists. For example, your application may need to perform operations using the entire table of 10,000 Contacts. Downloading values for all 10,000 at once could result in an unacceptable performance lag (this condition is actually prevented by the system -- see Where Clauses). With a list handle, however, you can select a range of rows upon which to query.

The primary drawback to using a list handle is the extra method calls it requires. At least two or three calls are necessary, as indicated by the following:

- One to get the handle
- A second (or third) to retrieve values
- A final call to free the list

You need to balance the amount of remote method calls versus the expected amount of data returned.

Note: CA SDM restricts the amount of data that can be returned from any one list. For more information, see Where Clauses.

doSelect

The following parameters apply to the doSelect method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
objectType	String	Identifies the object type (factory) to query.
whereClause	String	(Optional) Identifies the where clause for the query.
maxRows	Integer	Indicates the maximum number of rows to return. Specify -1 to return all rows. **Note:** Regardless of the integer specified, CA SDM will return a maximum of 250 rows per call.
attributes	String[]	Identifies the attribute list for which to fetch values. Dotted-attributes are permitted. If this field is blank, all value-based attributes are returned. These attributes cannot be defined as LOCAL in the majic definition file. LOCAL attributes are temporal; they have no database storage.

Description

Performs an SQL-like select on a specified object table. Supply one or more attributes you want fetched from the objects that match the supplied where clause.

Returns

A sequence of <UDSObject> elements. The following format applies:

```
<UDSObjectList>
   <UDSObject>
    <Handle>
    <Attributes>
   <AttributeNameA>
   <AttributeValueA0>
   <AttributeValueA1>
   <AttributeNameB>
   <AttributeValueB0>
   ...
```

XML Element	Type	Description
<UDSObject (see page 3980)>	N/A	Specifies the standard UDSObject element containing the handle and requested attribute values.
<UDSObjectList>	Sequence	Contains a <Handle> element and an <Attributes> sequence.

For example, if the method used is the following:

```
String[] myArray = ["last_name", "first_name"]
doSelect(mySID, "cnt", "last_name LIKE 'J%'", 2, myArray)
```

The return could be the following:

```
<UDSObjectList>
   <UDSObject>
   <Handle>cnt:555A043EDDB36D4F97524F2496B35E75</Handle>
   <Attributes>
   <AttributeName>last_name</AttributeName>
   <AttributeValue>Johnson</AttributeValue>
   <AttributeName>first_name</AttributeName>
   <AttributeValue>Carol</AttributeValue>
   </Attributes>
</UDSObject>
<UDSObject>
   <Handle>cnt:555A043EDDB36D4F97524F2496B35E76</Handle>
   <Attributes>
   <AttributeName>last_name</AttributeName>
   <AttributeValue>Jones</AttributeValue>
   <AttributeName>first_name</AttributeName>
   <AttributeValue>Ron</AttributeValue>
   </Attributes>
</UDSObject>
```

```
</UDSObjectList>
```

doQuery

The following parameters apply to the doQuery method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
ObjectType	String	Identifies the object type (factory) to query.
WhereClause	String	(Optional) Identifies the where clause for the query.

Description

Performs an SQL-like select for the specified object type. It also returns a *list handle* that points to a list of the rows returned from the query, where each row represents a CA SDM object that matched the supplied where clause. The caller can fetch values for the list rows using getListValues ().

Note: For more information about where clauses, see Where Clauses.

Important! The object list is stored on the CA SDM server and consumes system resources. The caller is responsible for freeing the list with freeListHandles(). Leaving a list in memory may increase memory for the process beyond the 2GB limit, resulting in memory leaks and can cause system failure.

Lists created with this function are homogenous, meaning the objects are all the same type, and they are static, meaning the list never changes even if a data change to an object excludes it from the initial where clause.

Returns

A list handle that must be freed with freeListHandle().

XML Element	Type	Description
<listHandle>	Integer	Identifies the list handle.
<listLength>	Integer	Identifies the length of the list generated.

getListValues

The following parameters apply to the getListValues method:

Parameter	Type	Description
SID		Identifies the session retrieved from logging in.

Parameter	Type	Description
	Integer	
ListHandle	Integer	Identifies the list handle obtained with a previous call.
StartIndex	Integer	Identifies the position in the list from which to begin fetching.
EndIndex	Integer	Identifies the last list position from which to fetch. Specify -1 to fetch all rows from StartIndex. **Note:** Regardless of the integer specified, Web Services will return a maximum of 250 rows per call.
AttributeNames	String[]	Identifies an array of one or more attribute names for which you want to fetch values.

Description

Returns attribute values for a range of objects in a list. For example:

```
< UDSObjectList >
   <UDSObject>
   <Handle>
   <Attributes>
       <AttributeName0>
       <AttributeName1>
```

Returns

This method has the following returns:

XML Element	Type	Description
<UDSObjectList>	Sequence	Identifies the outer Element, which contains a sequence of <UDSObject> elements.
<UDSObject (see page 3980)>	N/A	Contains a <Handle> element and <Attributes> sequence.

freeListHandles

The following parameters apply to the freeListHandles method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
Handles	Integer[]	Identifies an array of list handles to free.

Description

Frees the server-side resources for a list and invalidates the list handles. This method should be called whenever a list reference is no longer needed.

Returns

Nothing.

getRelatedList

The following parameters apply to the getRelatedList method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
ObjectHandle	String	Identifies the object handle.
ListName	String	Identifies a list-type attribute name of the object.

Description

Returns a list handle for list (QREL or BREL) attribute of an object. For example, the request object has a related list named “children”, which is a list of its child requests. The Request’s Activity Log (“act_log” or “act_log_all”) is another example.

To retrieve information about an object’s list attributes, refer to the object schema (majic) documentation or use getObjectTypeInformation().

Returns

The following:

XML Element	Type	Description
<listHandle>	Integer	Identifies the list handle.
<listLength>	Integer	Identifies the length of the list generated.

getRelatedListValues

The following parameters apply to the getRelatedListValues method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
objectHandle	String	Identifies the object handle.
listName	String	Identifies a list-type attribute name for the object.
numToFetch	Integer	Signifies the maximum number of rows to return. Cannot be zero Specify -1 to return all rows **Note:** Regardless of the integer specified, Web Services can return a maximum of 250 rows per call.
attributes	String[]	Identifies an array of one or more attribute names for which to fetch values. Dotted names are permitted.
		Identifies the String Holder object for capturing returned data.

Parameter	Type	Description
getRelatedListValuesResult	String Holder	
numRowsFound	Integer Holder	Identifies the Integer Holder object for capturing returned data.

Description

Returns values for lists related to a specific object. The lists must be defined as a QREL or BREL. Use the LREL methods to query LREL types.

For example, the request object has a related list named “children”, that is a list of its child requests. This method is a list handle-free alternative to getRelatedList(). The return format is similar to getListValues(), as indicated by the following:

```
<numRowsFound>
< UDSObjectList >
   <UDSObject>
   <Handle>
   <AttributeName0>
   <AttributeName1>
```

You can retrieve information for object list attributes using object schema (majic). An alternative method is to use getObjectTypeInformation().

Returns

This method has the following returns:

XML Element	Type	Description
<getRelatedListValuesResult>	N/A	Identifies the outer element, <UDSObjectList>, that contains a sequence of <UDSObject> elements. Each <UDSObject (see page 3980)> element contains a <Handle> element and zero or more <AttributeNameX> elements.
<numRowsFound>	Integer	Indicates the total number of rows in the queried list. **Note:** The total number of rows is not necessarily the number of rows returned.

getPendingChangeTaskListForContact

The following parameters apply to the getPendingChangeTaskListForContact method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
contactHandle	String	Identifies the contact handle.

Description

Returns a list handle representing all the “pending” change order workflow tasks assigned to a contact. A “pending” task is an active workflow task with a status that permits task updates.

Returns

The following:

XML Element	Type	Description
<listHandle>	Integer	Identifies the list handle.
<listLength>	Integer	Identifies the length of the list generated.

getPendingIssueTaskListForContact

The following parameters apply to the getPendingIssueTaskListForContact method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
contactHandle	String	Identifies the contact handle.

Description

Returns a list handle representing all the “pending” Issue tasks assigned to a contact. A “pending” task is an active task with a status that permits task updates.

Returns

The following:

XML Element	Type	Description
<listHandle>	Integer	Identifies the list handle.
<listLength>	Integer	Identifies the length of list generated.

getNotificationsForContact

The following parameters apply to the getNotificationsForContact method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
contactHandle	String	Identifies the contact handle.
queryStatus	Integer	(Optional) Identifies the target of the notifications.

Description

Returns a list of notifications (‘lr’ objects) for a contact.

You can query on a specific status for the notifications with the *queryStatus* field, which is useful for returning, for example, only non-cleared messages. The possible *queryStatus* values are as follows:

- **-1** -- Fetch all notifications
- **0** -- Fetch non-cleared notifications (those with a status value of less than 7)
- **1** -- Fetch cleared notifications (those with a status value of 7, 8 or 9)

Returns

The following:

XML Element	Type	Description
<listHandle>	Integer	Identifies the list handle.
<listLength>	Integer	Identifies the length of the list generated.

Asset Management Methods

This article contains the following topics:

It is possible for a client site to enhance the asset object using *extensions*. Asset extensions are separate tables that hold extra attribute information for an asset. The extension table is linked to a particular asset by using the asset ID as a foreign key. CA SDM Web Services ships two predefined extensions, Computer and Software. For more information, read the text executed by the following command:

```
/bopcfg/majic/assetx.maj
```

The asset's family attribute determines if the asset has an extension. Setting the Class attribute generally sets the family at asset creation time. To determine if an asset has an extension, query the 'extension_name' attribute of the asset's family (for example, "family.extension_name").

To retrieve values from an extension object, query it like any other object by using the following method:

```
getObjectValues()
```

To get the handle for a particular extension object, use the following method:

```
getAssetExtensionInformation()
```

Update an extension object like you would any other object by using the following method:

```
updateObject()
```

We do not recommend that you create your own extension objects. One is created for you, if needed, when createAsset() is called. Because of this automatic creation, we recommend that you only use createAsset() to create asset objects.

Note: If you are using the ITIL methodology, remember that Asset and Configuration Item are interchangeable in this context.

createAsset

The following parameters apply to the createAsset method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
attrVals	String	Identifies the array of name-value pairs used to set the initial attribute values for the new asset.
attributes	String Holder	Identifies the String Holder object for caputring returned data.
createAssetResult	String	Identifies the name for the new asset's extension. If no extension was created, this field is empty.
newAssetHandle	String Holder	Identifies the String Holder object for capturing returned data.
newExtensionHandle	String Holder	Identifies the String Holder object for capturing returned data.
newExtensionName	String Holder	Identifies the String Holder object for capturing returned data.

Description

Describes the recommend method for creating an asset. If you intend to create an asset with an extension, be sure to set the Asset Class attribute in the *attrVals* section.

Note: If you are using the ITIL methodology, use this method to create a Configuration Item.

Returns

A <UDSObject> element containing the handle for the new object, with attribute values specified in the *attributes* parameter. If the *attributes* parameter is empty, *all* attribute values are returned (see page 3980). List and LREL types are also returned, but as empty elements.

XML Element	Type	Description
<createAssetResult>	N/A	Identifies the standard <UDSObject> element containing the handle and requested attribute values.
<newAssetHandle>	String	Identifies the new request's handle.
<newExtensionHandle>	String	Identifies the handle for the new Asset's extension. If no extension was created, this field is empty.
<newExtensionName>	String	Identifies the name for the new asset's extension. If no extension was created, this field is empty.

getAssetExtensionInformation

The following parameters apply to the getAssetExtensionInformation method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
assetHandle	String	Identifies the asset to query.
attributes	String[]	Identifies the standard array of attributes from the asset extension object from which to request values. If this value is empty, all attributes are returned.
getAssetExtInfoResult	String Holder	Identifies the String Holder object for capturing returned data.
extensionHandle	String Holder	Identifies the String Holder object for capturing returned data.
extensionName	String Holder	Identifies the String Holder object for capturing returned data.

Description

Returns extension information for an asset. If the asset does not have an extension, nothing is returned.

An asset has an extension if a value exists for its "family.extension_name" property. This property is empty if the asset does not have an extension.

Returns

The following elements return (see page 3980)with empty values when the asset does not have an extension:

XML Element	Type	Description
<getAssetExtInfoResult>	String	Identifies all the attribute values for the extension.
<extensionHandle>	String	Identifies the extensions handle.
<extensionName>	String	Identifies the name for the assets extension.

addAssetLog

The following parameters apply to the addAssetLog method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
assetHandle	String	Identifies the asset handle.
contactHandle	String	(Required) Identifies the handle of the contact used for the log's author.
logText	String	Identifies the text for the new asset log.

Description

Adds a new log entry for an asset. The log's author is the user associated with the SID.

Returns

Nothing.

createAssetParentChildRelationship

The following parameters apply to the createAssetParentChildRelationship method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
parentHandle	String	Identifies the asset handle for the parent.
childHandle	String	Identifies the asset handle for the child.

Description

Makes *assetParent* a parent of *assetHandle*. Web Services creates a separate object (the *hier* object, which is the *Assignment* table) for parent-child relationships between assets. These are stored in related lists, *child_hier* and *parent_hier,* in the Asset (nr) object.

Returns

Handle of the new hier (Assignment) object.

Web Services Business Methods

This article contains the following topics:

This section describes the Web Services Business methods.

createIssue

The following parameters apply to the createIssue method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
creatorHandle	String	Identifies the handle of the contact responsible for the creation of the issue (the log agent). Pass an empty string to specify the default CA SDM user.
attrVals	String[]	Identifies the array of name-value pairs that is used to set the initial attribute values for the new issue. **Note:** Dotted names are not permitted.
propertyValues	String[]	(Optional) Identifies the array of values for any properties that are attached to the new issue.
template	String	(Optional) Identifies the handle of an issue template (iss_tpl object) from which to create the issue.
attributes	String[]	Identifies the sequence of attribute names from the new object for which to return values. Dot-notation is permitted. If this field is empty, all attribute values are returned.
newIssueHandle	String Holder	Identifies the String Holder object for capturing returned data. See the XML Element Return list below for details.
newIssueNumber	String Holder	Identifies the String Holder object for capturing returned data. See the XML Element Return list below for details.

Description

Creates a CA SDM Issue (iss) object. For more information about creating an Issue object with properties, see createRequest().

Note: You *must* use this function to create a Issue; do not use createObject().

Returns

Returns the new object handle, along with *all* of its attribute values. List and LREL types are also returned, but as empty elements.

XML Element	Type	Description
<UDSObject>	N/A	Identifies the standard UDSObject element containing the handle and requested attribute values.
<newIssueHandle>	String	Identifies the new issue's handle.
<newIssueNumber>	String	Identifies the new issue's number (its "ref_num" attribute).

createRequest

The following parameters apply to the createRequest method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
creatorHandle	String	Identifies the handle of the contact responsible for the creation of the request (the log agent). Pass an empty string to specify the default CA SDM user.
attrVals	String[]	Identifies an array of name-value pairs that is used to set the initial attribute values for the new request. **Note:** Dotted names are not permitted.
propertyValues	String[]	Identifies the array of values for any properties that are attached to the new request.
template	String	(Optional) Identifies the handle of the request template (cr_tpl) from which to create the request.
attributes	String[]	Specifies the sequence of attribute names from the new object for which to return values. Dot-notation is permitted. If this field is empty, all value-based attribute values are returned.
newRequestHandle	String Holder	Specifies the String Holder object for capturing returned data. See the XML Element Return list below for details.
newRequestNumber	String Holder	Specifies the String Holder object for capturing returned data. See the XML Element Return list below for details.

Description

Creates a CA SDM Request (cr) object. You *must* use this function to create a Request; do not use createObject().

propertyValues is a list of values for each Property object that will be attached to the new Request. The Properties that are attached are determined by the new Request's 'category' attribute value. All properties created from the CA SDM Web Services interface will have a default value (for more information, see Categories and Properties), which is important because a Request will not save until all of its Properties marked "required" have a value.

You may override the default by supplying values for any properties that will be attached when the Request is created. You must supply this information before the Request is created, since createRequest() attempts to back-store the object you most recently create. Use getPropertyInfoForCategory() to get a list of properties for a specific Category. This function returns the properties in order of their 'sequence' attribute, which is the expected order of the *propertyValues* array. For example, if the sequences and symbols of the properties are as follows:

```
100  -  Hard Drive Size
200  -  CPU
300  -  Memory
```

The *propertyValues* array, depending on the programming language, may appear as follows:

```
["40 GB", "Pentium 4 1.7 Ghz", "256"]
```

getPropertyInfoForCategory() indicates which Properties are marked *required*.

If you do not set the Request category or do not want to set any Property values, pass an empty string for *propertyValues.*

If you do not want to rely on the default property values, the following is the suggested order for creating a new Request (or Issue or Change Order):

1. Retrieve a list of Categories/Areas. The object name for Request Area is 'pcat'.
2. Call getPropertyInfoForCategory() and examine the list of properties for the category of the new Request/Issue/Change.
3. Create a value array for each of the properties returned. This is identified by the *propertyValues* parameter for the create operation.
4. Assemble the *attrVals* array and call the create method.

As an alternative to the previous procedure, you can retrieve the list of properties using getRelatedListValues() after createRequest() returns. Properties are stored in the 'properties' list for a Request.

Depending upon the application, it may be faster to at least cache the list of Categories, since this data does not change often at many client sites.

Note: By default, this method creates a Request. If you are using the ITIL methodology, you need to set the 'type' attribute in the attrVals array to define whether you are creating an Incident or a Problem ticket. For more information about ITIL procedures, see ITIL Methodology (see page 1873).

Returns

Returns the new objects handle with *all* of its attribute values. List and LREL types are also returned, but as empty elements.

XML Element	Type	Description
<UDSObject (see page 3980)>	N/A	Identifies the standard UDSObject element containing the handle and requested attribute values.
<newRequestHandle>	String	Identifies the new request handle.
<newRequestNumber>	String	Identifies the new request's number (its "ref_num" attribute).

createChangeOrder

The following parameters apply to the createChangeOrder method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
creatorHandle	String	Identifies the handle of the contact responsible for the creation of the change order (the log agent). Pass an empty string to specify the default CA SDM user.
attrVals	String[]	Identifies an array of name-value pairs that is used to set the initial attribute values for the change order. **Note:** Dotted names are not permitted.
propertyValues	String[]	(Optional) Identifies the array of values for any properties that are attached to the new change order.
template	String	(Optional) Identifies the handle of the change template (chg_tpl object) from which to create the change order.
attributes	String[]	Specifies the sequence of attribute names from the new object for which to return values. Dot-notation is permitted. If this field is empty, all value-based attribute values are returned.
newChangeHandle	StringHolder	Specifies the String Holder object for capturing returned data.
newChangeNumber	StringHolder	Specifies the String Holder object for capturing returned data.

Description

Creates a CA SDM Change Order (chg) object. You *must* use this function to create a change order (see page 4070); do not use createObject().

Returns

The new object handle with *all* of its attribute values. List and LREL types are also returned (see page 3980), but as empty elements.

XML Element	Type	Description
<UDSObject>	N/A	

XML Element	Type	Description
		Identifies the standard UDSObject element containing the handle and request attribute values.
<newChangeHandle>	String	Identifies the new change order handle.
<newChangeNumber>	String	Identifies the new change order number (its 'chg_ref_num' attribute).

createActivityLog

The following parameters apply to the createActivityLog method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
creator	String	Identifies the handle of the contact responsible for the activity.
objectHandle	String	Identifies the handle for a request, issue, or change order. Any other object type is rejected.
description	String	Identifies the description for the activity, which will appear in the activity log.
LogType	String	Identifies the type of log to create -- see the following Description.
TimeSpent	Integer	Sets the Time Spent field for the activity log, which is the duration of the activity. Pass zero for the default.
Internal	Boolean	Identifies the values that apply: True = Internal-only activity False = Non-internal activity that can be viewed by everyone.

Description

Creates an activity log for a specified request, issue or change order. This method corresponds to, "Activities - Log Comment/Research/Callback" on a Change/Request/Issue detail in the CA SDM interface. *LogType* is the code attribute for the activity type of the new log. The most common codes are as follows:

- "CB" (Callback)
- "RS" (Research)
- "LOG" (Log Comment)

The CA SDM Administrative Client also shows the code values. To access the code values, select from the Main Menu Administration, then select Notification, Activity Notifications.

Returns

The handle to the activity log object created.

XML Element	Type	Description
<LogHandle>	String	Identifies the handle for the new activity log.

transfer

The following parameters apply to the transfer method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
creator	String	Identifies the handle of the contact responsible for the activity.
objectHandle	String	Identifies the handle for a request, issue, or change order. Any other object type is rejected.
description	String	Identifies the description for the activity, which will appear in the activity log.
setAssignee	Boolean	Used to update the assignee field with the value in newAssignee, if the value is true.
newAssigneeHandle	String	Identifies the new assignee for the object.
setGroup	Boolean	Updates the group field, if true.
newGroupHandle	String	Identifies the new group for the object.
setOrganization	Boolean	Update the organization, if the value is true.
newOrgnizationHandle	String	(Issues and Change Orders only) Identifies the new organization for the object.

Description

Performs a transfer activity on an Issue, Request or Change Order. This method corresponds to the “Activities -- Transfer” command in the CA SDM interface. This method generates an activity log and optionally sets a new assignee, group, or organization.

The assignee, group or organization is not updated unless one or more of the corresponding *setAssignee/setGroup/setOrganization* parameters is set to true.

If the companion parameter is false, then transfer will not attempt to update the field, even if a value is passed for that field. For example, if *setAssignee* is passed as false, transfer will not update the assignee even if *newAssignee* specifies a value. If the *setXXXX* parameter is true, then the field is updated. Pass the empty string to set a field to empty/null.

Returns

One or more handles to the activity log objects created. The returns are under a parent element named <Logs>.

XML Element	Type	Description
<LogHandle>	String	Identifies the handle for the new activity log (zero or more of these can be returned).

escalate

The following parameters apply to the escalate method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
creator	String	Identifies the handle of the contact responsible for the activity.
objectHandle	String	Identifies the handle for a request, issue, or change order. Any other object type is rejected.
description	String	Identifies the description for the activity, which will appear in the activity log.
setAssignee	Boolean	Updates the assignee field, if true.
newAssigneeHandle	String	Identifies the handle of the new assignee for the object.
setGroup	Boolean	Updates the group field with the value in newGroupHandle, if true.
newGroupHandle	String	Identifies the handle of the new group for the object.
setOrganization	Boolean	Sets the organization field with the value specified in the newOrganizationHandle, if true.
newOrgnizationHandle	String	(Issues and Change Orders only) Identifies the handle of the new organization for the object.
setPriorityHandle	Boolean	Updates the priority field with the value specified in newPriority, if true.
newPriority	String	Identifies the handle of the new priority for the object.

Description

Performs an escalate activity on an Issue, Request or Change Order. This method generates an activity log and optionally sets a new assignee, group, priority and/or organization.

It corresponds to the “Activities -- Escalate” command in the CA SDM interface.

The assignee, group, or organization is not updated unless one or more of the corresponding *setAssignee/setGroup/setOrganization* parameters is set to true. If the companion parameter is false, then escalate will not attempt to update the field, even if a value is passed for that field. For example, if *setAssignee* is passed as false, escalate will not update the assignee even if *newAssignee* specifies a value. If the *setXXXX* parameter is true, then the field is updated. Pass the empty string to set a field to empty/null.

Note: Organization is not used for Requests.

Returns

One or more handles to the activity log objects created.

XML Element	Type	Description
<LogHandle>	String	Identifies the handle for the new activity log (zero or more of these can be returned).

changeStatus

The following parameters apply to the changeStatus method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
creator	String	Identifies the handle of the contact responsible for the activity.
objectHandle	String	Identifies the handle for a request, issue, or change order. Any other object type is rejected.
description	String	Identifies the description for the activity, which will appear in the activity log.
newStatusHandle	String	Identifies the handle of the status for the object.

Description

Performs a status change activity on an issue, request, or change order. This method generates an activity log and optionally sets the status value. It corresponds to the “Activites -- Update Status” command in the CA SDM interface.

Returns

The handle to the activity log object created.

XML Element	Type	Description
<LogHandle>	String	Identifies the handle for the new activity log (zero or more of these can be returned).

getPropertyInfoForCategory

The following parameters apply to the getPropertyInfoForCategory method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
categoryHandle	String	Identifies a category handle.
attributes	String[]	Identifies the names of one or more attributes from the property template object for which to fetch values. If this is empty, all value-based attributes are fetched.

Description

Information about Properties for the specified category. This method is used to help pre-populate Request/Issue/Change Order properties on insert operations with user-defined data.

Depending on the category, this method queries either the 'prptpl' or the 'cr_prptpl' object types. Both types are nearly identical. The suggested attributes to fetch are 'sequence', 'label', 'description' and 'required'.

Returns

A <UDSObject> element containing a sequence of <UDSObject> elements, in the order of the 'sequence' attribute.

logComment

The following parameters apply to the logComment method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
ticketHandle	String	Identifies the handle of the ticket where the activity log should be added.
Comment	String	Identifies the comment text.
internal_flag	String	Identifies the internal flag. Set to True if the new activity log should be marked as internal.

Description

Attaches a 'Log Comment' activity log to a ticket. It is a simplified version of createActivityLog().

Returns

Nothing.

notifyContacts Method

This article contains the following topics:

The following parameters apply to the notifyContacts method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
creator	String	Identifies the handle of the contact responsible for the activity.
contextObject	String	Identifies the handle for a request, issue, or change order. The following applies: It is the context for the notification. Any other object type is rejected. An activity log is added to the object to record the notification.
messageTitle	String	Identifies the title of the notification message.
messageBody	String	Identifies the body of the notification message.
notifyLevel	Integer	Indicates the notification level. Specify an integer from 1 (Low) to 4 (Emergency).
notifyees	String[]	Identifies the array of contact handles to notify.
Internal	Boolean	Indicates internal-only notification. Set to True to flag for an internal-only notification, which guarantees that the message is sent only to those who can view internal logs, and the resulting activity log is flagged as internal.

Description

Sends a notification to one or more contacts. This is equivalent to the Manual Notify activity on requests, issues, and change orders.

Returns

The following is returned:

XML Element	Type	Description
<LogHandle>	String	Identifies the handle for new activity log.

clearNotification

The following parameters apply to the clearNotification method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
lrObject	String	Identifies the handle to a Notify Log Header (lr) object.
clearBy	String	Identifies the name of the contact responsible for the clear operation.

Description

Clears a notification message.

Returns

The new status of the notification message.

attachChangeToRequest Method

This article contains the following topics:

The following parameters apply to the attachChangeToRequest method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
creator	String	Identifies the handle of the contact responsible for the activity.
requestHandle	String	Identifies the request to which you attach the change.
changeHandle	String	Identifies the handle of the change to add. If this is blank, a new change order is created.
changeAttrVals	String[]	Identifies the attribute-value pairs used to initialize a new change order if the changeHandle is blank.
description	String	(Optional) Identifies the description of the activity.

Description

Attaches a new or existing change order to a request. It corresponds with “Activities -- New Change Request” or “Activities -- Attach to Existing Request” on a Request detail in the CA SDM interface.

To create a new change order, pass the empty string in *changeHandle*. The system will create a new change order with values initialized from the request, including the change’s Requestor, Affected End User, Description, and Priority (you can see this effect in the CA SDM interface). You can override these or set additional values with *changeAttrVals,* which is a name-value array similar to what is passed for *createObject().*

To attach an existing change order, specify a handle in the *changeHandle* parameter. In this case, *changeAttrVals* is ignored.

If a new change order is created, *description* is used on the new change order’s activity log. If an existing change is attached, *description* is used on the request’s activity log.

If the request already has an attached change order, the following error is returned:

```
UDS_CREATION_ERROR
```

Note: This method works exactly the same for the ITIL methodology -- simply verify that you are passing the appropriate handle of an ITIL Incident or Problem to the method.

Returns

The following is returned:

XML Element	Type	Description
<changeHandle>	String	Identifies the handle for the change order, created or attached.

detachChangeFromRequest

The following parameters apply to the detachChangeFromRequest method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
creator	String	Identifies the handle of the contact responsible for the activity.
requestHandle	String	Identifies the handle of a request.
Description	String	(Optional) Identifies the description of the activity.

Description

Detaches a change order from a request. This method corresponds with “Activities -- Detach Change Order” on the CA SDM client. The change order is not deleted from the system.

There is no effect if the request did not have an attached change.

Returns

The handle of the request’s activity log marking the event.

createTicket Method

This article contains the following topics:

The following parameters apply to the createTicket method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
Description	String	(Optional) Identifies the description of the ticket.
problem_type	String	Specifies the code (not the persistent ID) for an existing problem type for the policy under which a Web Services application is running. If this is blank or contains a bad value, the default problem type is used.
Userid	String	(Optional) Specifies the user ID of the end user for the new ticket. If this is blank or the supplied user ID is not found, the proxy contact defined in the access policy is used and the ticket is still created.

Parameter	Type	Description
Asset	String	(Optional) Identifies the handle of an asset to be attached to the ticket.
DuplicationID	String	(Optional) Allows callers to assist the duplication handling routines used for classifying tickets as being unique or different. If duplicate handling is on, this string is inspected after other duplicate handling criteria match to determine whether this is a unique or duplicate call to this method.
newTicketHandle	String Holder	Identifies the String Holder object for capturing returned data. See the XML Element Return list on this page for details.
newTicketNumber	String Holder	Identifies the String Holder object for capturing returned data. See the XML Element Return list on this page for details.
returnUserData	String Holder	Identifies the String Holder object for capturing returned data. See the XML Element Return list on this page for details.
returnApplicationData	String Holder	Identifies the String Holder object for capturing returned data. See the XML Element Return list on this page for details.

Description

Creates a ticket based on the rules defined in both the Service Aware Policy and the specified Problem Type. The Problem Type specifies the type of ticket created by a Request/Change/Issue template. The supplied description is copied in and the user is set from the access policy proxy contact.

If input problem_type does not exist, the policy default problem type is used. The problem type also defines how to handle duplicate ticket creation, and additional returned data.

Returns

Returns the new ticket handle, ticket number, and the user-specified return data defined in the problem type that is used to create the ticket.

XML Element	Type	Description
<UDSObject>	N/A	Returns the XML element so that it is consistent with the returns of these other methods: createRequest() createChange() createIssue() The body of this tag is empty.
	String	Identifies the new ticket handle.

XML Element	Type	Description
<newTicketHandle>		
<newTicketNumber>	String	Identifies the new ticket number (its “ref_num” or “chg_ref_num” attribute).
<returnUserData>	String	Identifies the user-specified data for the problem type intended for display to the end user, or for log entries. You can set this value in the User Data Return field on the Returned Data tab of the Problem Type Detail window.
<returnApplicationData>	String	Identifies the user-specified data for the problem type intended for use within the application code, especially for actions. You can set this value in the Application Data Return field on the Returned Data tab of the Problem Type Detail window.

createQuickTicket

The following parameters apply to the createQuickTicket method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
customerHandle	String	Identifies the customer handle used to create the ticket.
description	String	(Optional) Identifies the description of the ticket.
newTicketHandle	String Holder	String Holder object for capturing returned data. See the XML Element Return list on this page for details.
newTicketNumber	String Holder	String Holder object for capturing returned data. See the XML Element Return list on this page for details.

Description

Creates a ticket based on the preferred document type of the user represented by customerHandle. Contact access rights are determined by an Access Type record, which also sets the contact preferred document type (Request, Incident, Problem, Issue or Change Order). If a contact document type is Issue, this method will create an Issue; if the document type is Request, a Request is created, and so on. The contact represented by customerHandle is used to set the end user/customer field of the new ticket. The ticket description is set to the input *description* value.

Returns

Returns the new ticket handle, ticket number, and a brief representation of the new ticket in <UDSObject> format.

XML Element	Type	Description
<UDSObject>	N/A	Returns a partial set of attributes because it is a high-level method designed to simplify the process. Their values come from the following methods, and the XML element is returned so it is consistent with the returns of these methods:

XML Element	Type	Description
		createRequest() createChange() createIssue()
<newTicketHandle>	String	Identifies the new ticket handle.
<newTicketNumber>	String	Identifies the new ticket number (its “ref_num” or “chg_ref_num” attribute).

closeTicket

The following parameters apply to the closeTicket method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
description	String	(Optional) Identifies the description of the ticket, which can be used in the Close activity log.
ticketHandle	String	Identifies the ticket to close.

Description

Sets the status of the ticket to “Closed” and adds an activity log with the input description.

Returns

The handle to the activity log object created. It provides the same return as the changeStatus() method.

XML Element	Type	Description
<LogHandle>	String	Specifies the handle for new activity log (0 or more of these can be returned).

Group Management Methods

This article contains the following topics:

This section explains the Web Services Group Management Methods.

addMemberToGroup

The following parameters apply to the addMemberToGroup method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
ContactHandle	String	Identifies the handle of the contact to add as a member.
GroupHandle	String	Identifies the group to which you will add the contact.

Description

Adds a contact to a group. Nothing happens if the contact is already a member.

Returns

Nothing.

removeMemberFromGroup

The following parameters apply to the remove MemberFromGroup method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
ContactHandle	String	Identifies the handle of the contact to remove.
GroupHandle	String	Identifies the group from which you will remove the contact.

Description

Removes a contact from a group. Nothing happens if the contact is not a member.

Returns

Nothing.

getGroupMemberListValues

The following parameters apply to the getGroupMemberListValues method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
whereClause	String	Identifies the SQL where clause.
numToFetch	Integer	Determines the maximum number of records to return. This cannot be zero (0). Use ‘1’ to return all.
attributes	String []	Identifies the array of attribute names for which to retrieve values.

Description

Functions similarly to getListValues(), except that it queries the system's group and member relationships. The system uses a special 'Group Member' (grpmem) object for each group/member relationship. The CA SDM system administers grpmem objects behind the scenes (you do not manipulate them directly), and they are essential for certain queries.

The grpmem object simply contains two pointers, one to a Contact and the other to a Group, which in itself is a Contact object. The attribute names are 'member' and 'group', respectively. Because these are pointers, you must use dot-notation to form a query as normal. For example, to find all Contacts with a last name beginning with 'B' and in a group with the name, "Seattle", you would use the following:

```
member.last_name LIKE 'B%' AND group.last_name = 'Seattle'
```

You may also use handles as normal, illustrated by the following:

```
member.last_name LIKE 'A%' AND group.id = U'555A043EDDB36D4F97524F2496B35E75'
```

It is important to note that this method can retrieve values from all members and groups, not just a single group. To simply get information about all the members of a specific group or member, just specify a handle in the where clause. For example, the following would retrieve values from a specific group:

```
group.id = U'555A043EDDB36D4F97524F2496B35E75'
```

The following concepts are important to remember:

- grpmem object contains two pointer attributes, one is to member and the other is to group
- grpmem object exists for each group/member relationship

The grpmem method actually queries the grpmem object table, thereby returning an object representing a relationship between two contacts. Therefore, the attribute values you want to fetch in attributes must use dot-notation from the grpmem object. To fetch values from the member, all your attribute names should be of the form, 'member.*ATTRNAME*', as illustrated by the following example:

```
'member.last_name'
```

To fetch values from the group, use 'group.*ATTRNAME*'.

Note: For an example of efficient querying of groups and members, see Where Clauses.

Returns

Automatically returns no handles. The <Handle> element in the return is always empty. To request the member or group handle for each row, use one of the following in the attributes parameter described in the table.

- “member.persistent_id”
- “group.persistent_id”

XML Element	Type	Description
<UDSObjectList>	N/A	Identifies the outer element, which contains an array of <UDSObject (see page 3980)> elements. Each object is really a grpmem object.

Contact Management Methods

This article contains the following topics:

This section explains the Web Services Contact Management methods.

login

The following parameters apply to the login method:

Parameter	Type	Description
username	String	Identifies the user ID.
password	String	Identifies the password.

Description

Login validates a user with CA SDM login validation and returns a unique session ID that is required for most other web method calls. This key should be freed with logout(). A SID may expire if it is not used before a time out elapses.

The username/password is validated exactly the same as the CA SDM Web client; the contact’s Access Type specifies the validation method. The default access policy will be applied to control and manage all subsequent accesses after a successful call of this function. The login user (not proxy contact specified in the default policy) is then responsible for subsequent web service activities. All function group security and data partition are enforced for the login user.

Returns

The following is returned:

Parameter	Type	Description
<SID>	Integer	Identifies the unique SID to use for all other Web Services calls.

loginService

The following parameters apply to the loginService method:

Parameter	Type	Description
username	String	Identifies the user ID.
password	String	Identifies the password.
policy	String	(Required) Identifies the policy code, which must be in plain text. Although it is required, it may be empty.

Description

Lets users log in with a conventional username/password authentication scheme where if valid, the system returns a unique session ID. This key should be freed with logout(). A SID may expire if it is not used before a timeout elapses.

User authentication is performed on the username and password while access control is applied based on the policy specified. The authentication is performed as described in login(). Empty policy will allow default policy to be applied automatically. The login user (not the proxy contact specified in the policy) is responsible for subsequent web service activities. All function group security and data partitions are enforced for the login user.

Returns

The following is returned:

Parameter	Type	Description
SID	Integer	Specifies the unique SID to use for all other Web Services calls.

impersonate

The following parameters apply to the impersonate method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
username	String	(Required) Identifies the user name of the user being impersonated.

Description

Lets an administrator switch the user responsible for all web services activities in a current web services session without additional user authentication. Invoking this method is allowed only if the current web services session is started by using the PKI access authentication scheme and the access policy is defined to allow impersonation.

The Access Type of the user to be impersonated is checked against the Access Type of the proxy user of the policy used in the current web services session. If the access_level of the new user's access type is less than or equal to the grant_level of the proxy user's access type, this method will replace the current user with the new user. A new web services session starts while the old session ends. A new SID is then returned. In addition, the new user is given the responsibility for all subsequent activities initiated in this new session. The function group security and data partition are enforced for the new user.

Returns

The following is returned:

Parameter	Type	Description
SID	Integer	Identifies the unique SID to use for all other Web Services calls.

logout

The following parameter applies to the logout method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.

Description

Invalidates a SID obtained from login(), loginService(), and loginServiceManaged().

Returns

Nothing.

loginWithArtifact

The following parameters apply to the loginWithArtifact method:

Parameter	Type	Description
userid	String	Identifies the user ID.
artifact	String	Identifies the Artifact obtained from CA EEM.

Description

Performs the user authentication by the provided CA EEM Artifact and opens a session with the back-end server. The Artifact can be used only once for authentication. The returned session ID (SID) can be used for subsequent web services method invocations. The Artifact can be acquired directly from CA EEM or can be obtained by the getArtifact method.

Note: Service Desk needs to be integrated with CA EEM to perform this operation.

The SID should be freed with logout(). A SID may expire if it is not used before a timeout elapses.

Returns

The following is returned:

Parameter	Type	Description
SID	String	Identifies the unique session ID (SID) to use for all other Web Services calls. It is in plain text format.

getPolicyInfo

This article contains the following topics:

The following parameters apply to the getPolicyInfo method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.

Description

Returns information about the access policy that is controlling and managing the current CA SDM Web Services session.

Returns

The following XML string:

XML Element	Type	Description
<SAPolicy>	N/A	Identifies the detailed information of this access policy and its related problem types.

The content of <SAPolicy> is shown as follows:

```
<SAPolicy>
<Name> name of policy </Name>
```

```
<Code> policy code </Code>
<ContactName> policy proxy contact's combo name </ContactName>
<ContactHandle> handle of policy's contact </ContactHandle>
<Access>
       <TicketCreation> limitation </TicketCreation>
       <ObjectCreation> limitation </ObjectCreation>
       <ObjectUpdate> limitation </ObjectUpdate>
       <Attachments> limitation </Attachments>
       <Queries> limitation </Queries>
       <Knowledge> limitation </Knowledge>
</Access>
<ProblemTypes> (zero or more <ProblemType> elements)
    <ProblemType>
        <Code>code of a problem type </Code>
        <Status>active or inactive </Status>
    </ProblemType>
</ProblemTypes>
</SAPolicy>
```

getTaskListValues

The following parameters apply to the getTaskListValues method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
objectHandle	String	Identifies the object handle for an issue or change order.
attributes	String	Identifies the sequence of attribute names for which to fetch values. Dotted-attributes are permitted. If this is blank, all attributes are fetched.

Description

Returns values for all the tasks associated with the specified issue or change order.

Note: This is a convenience method. The same list could be obtained using doSelect().

Returns

This method has the following returns:

XML Element	Type	Description
<UDSObjectList>	N/A	Outer element -- contains zero or more <UDSObject (see page 3980)> elements. Each <UDSObject> node represents a Task. The nodes are ordered by the Task's 'sequence' attribute.

getValidTaskTransitions

The following parameters apply to the getValidTaskTransitions method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
taskHandle	String	Identifies the handle to a Workflow task (for an issue or change order).
attributes	String[]	Identifies the names of attributes to fetch from the 'tskstat' object. If this field is empty, all value-based attributes are returned.

Description

Returns all of the possible values for the 'status' attribute of a particular task. The Status codes to which a task may be set depend upon several factors, such as the current status of the task, and restrictions set by the administrator.

Note: *taskHandle* can be a task owned by either a change order or an issue. The objects returned are Task Status ('tskstat') objects used for both types of tasks.

Returns zero or more Status objects to which a task can be set.

Returns

This method has the following returns:

XML Element	Type	Description
<UDSObjectList>	N/A	Identifies the outer element, which contains zero or more <UDSObject (see page 3980)> elements with the requested attribute values.

getValidTransitions

The getValidTransitions method lets you list the transitions for a ticket.

The following parameters apply:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
handle	String	Identifies the handle for a ticket or status. If a ticket handle is provided, the method retrieves the valid transitions for the current status of the ticket.

Parameter	Type	Description
ticketFactory	String	Identifies the factory of the ticket. Valid values are only “cr” for Request, “in” for Incident, “pr” for Problem, “chg” for Change Order and “iss” for Issue.

Description

Returns all of the possible transition values for the status of a ticket. Administrators can configure valid status transitions for all ticket types.

Returns zero or more request/incident/problem/change/issue transition objects, depending on the values passed for handle and ticketFactory. If zero objects are returned, there are no transitions on the status of the ticket.

Returns

This method has the following return:

XML Element	Type	Description
<UDSObjectList>	N/A	Identifies the outer element, which contains zero or more <UDSObject (see page 3980)> elements.

getDependentAttrControls

The getDependentAttrControls method lets you list the locked and required attributes for the Status record (either the ticket’s current status or any status record). At this time, the only attribute supported is the Status attribute. If the attrVals parameter is passed as empty, the method returns the dependent attributes for the current status of the ticket (assuming that a valid handle is used). Otherwise, you can request the dependent attributes for any status record by using the attrVals parameter.

Enter the attrVals parameter syntax as follows:

- Specify the word "status" for the first item.
- For the second item, specify the code of the status record, for example, WIP.

The following parameters apply:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
handle	String	Identifies the handle for a ticket.
attrVals	String	Identifies the name-value pairs of a ticket attribute for this method to get its dependent attribute controls.

Description

Returns all of the possible dependent attribute controls for the Status field of a ticket. Administrators can configure attribute restrictions.

Returns zero or more attribute control objects depending on the values specified. If zero objects are returned, there are no attribute restrictions on the object.

Returns

The following:

XML Element	Type	Description
<UDSObjectList>	N/A	Identifies the outer element, which contains zero or more <UDSObject (see page 3980)> elements.

getHandleForUserid

The following parameters apply to the getHandleForUserid method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
userID	String	Identifies the user ID upon which to query.

Description

Returns the persistent handle for a Contact represented by userID.

Returns

The following is returned:

Parameter	Type	Description
<Handle>	String	Identifies the contact's handle.

getAccessTypeForContact

The following parameters apply to the getAccessTypeForContact method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
ContactHandle	String	Identifies the contact handle upon which to query.

Description

Returns a handle for the Access Type for a Contact.

Every Contact is assigned an Access Type object, which defines a Contact's permissions and security. Note the access_type field on a Contact is not required. To accommodate this, a single Access Type is marked as the default for Contacts who do not have an object specifically assigned.

This method returns the Access Type directly assigned to a Contact (that is, the information to which the access_type field points in the Contact record) or it returns the default. Typical value methods, such as getObjectValues() or getListValues(), may not return the correct Access type; therefore, these are not the accurate methods for retrieving the Contact's Access.

Returns

A string handle for an Access Type object.

getContact

The following parameter applies to the getContact method:

Parameter	Type	Description
SID	String	Identifies the session retrieved from logging in.
contactId	String	Identifies the unique ID of the contact to retrieve. contactId is UUID in string format.

Description

Retrieves information on all contacts.

Returns

A <UDSObject> node with a <UDSObject> node describing a contact with some of the following child <Attributes> nodes:

XML Element Value	Type	Description
contactid	String	Specifies a unique ID of the contact. contactId is UUID in string format.
userid	String	Indicates the user name of the contact.
last_name	String	Indicates the last name of the contact.
first_name	String	Specifies the first name of the contact.
middle_name	String	Specifies the middle name of the contact.
location	String	Indicates the location of the contact.
dept	String	Identifies the department of the contact.
organization	String	Identifies the organization of the contact.
email_address	String	Identifies the email address of the contact.
pemail_address	String	Signifies the alternate email address of the contact.
phone_number	String	Indicates the phone number of the contact.
alt_phone	String	Indicates the alternate phone number of the contact.
address1	String	Specifies the address of the contact.
address2	String	Specifies the alternate address of the contact.
city	String	Identifies the city of the contact.

XML Element Value	Type	Description
state	String	Identifies the state of the contact.
zip	String	Indicates the ZIP code of the contact.
country	String	Indicates the country of the contact.
delete_flag	Integer	Indicates whether the contact is active: **0** -- Active **1** -- Inactive

findContacts

The following parameters apply to the findContacts method:

Parameter	Type	Description
SID	Integer	Identifies the session retrieved from logging in.
userName	String	Returns only the contacts with this user name. You can do wildcard searches by using the percent (%) sign. For example, to search for all contacts where the User Name begins with Smi, specify Smi%.
lastName	String	Returns only the contacts with this last name. You can do wildcard searches by using the percent (%) sign.
firstName	String	Returns only the contacts with this first name. You can do wildcard searches by using the percent (%) sign.
email	String	Returns only the contacts with this email address. You can do wildcard searches by using the percent (%) sign.
accessType	String	Returns only the contacts with this access type. You can specify multiple roles by separating them with commas. Specify the following: 10002 - Administration 10004 - Customer 10005 - Employee 10009 - IT Staff 10013 - Knowledge Management 10014 - Process Management 10010 - Service Desk Management 10008 - Service Desk Staff 10020 - Vendor Staff
inactiveFlag	Integer	Returns only the contacts that are inactive or active. Specify the following: 0 for active - 999 for all other for inactive

Description

Retrieves the list of contacts.

Returns

A <UDSObjectList> node with zero or more <UDSObject> nodes describing contacts with the following <Attributes> child nodes:

XML Element Value	Type	Description
id	UUID	Specifies the unique ID of the contact.
userid	String	Specifies the user name of the contact.
last_name	String	Identifies the last name of the contact.
first_name	String	Identifies the first name of the contact.
access_type	Integer	Specifies the Role ID of the contact.
delete_flag	Integer	Indicates whether the contact is active or inactive: 0 - Active 1 - Inactive

loginServiceManaged Method

This article contains the following topics:

The following parameters apply to the loginServiceManaged method:

Parameter	Type	Description
policy	String	(Required) Identifies the policy, which must be must be in plain text.
encrypted_policy	String	(Required) Identifies the digital signature of the policy code, encrypted with the policyholder's private key. It is in BASE64 text format.

Description

Performs the user authentication by locating the policy through the plain text policy code, finding the policyholder's public key associated with the policy, decrypting the encrypted policy code, matching decrypted content with the policy code, and finally, opening a session with a back-end server. The returned session ID (SID) can be used for subsequent web services method invocations. Proxy contact specified in the policy is responsible for all subsequent web service activities initiated. All function group security and data partition are enforced for the proxy contact defined in the policy.

It is also important to note that the encrypted_policy parameter is in the BASE64 text format, and it is necessary to perform proper conversion from the binary format. The SID should be freed with logout(). A SID may expire if it is not used before a timeout elapses.

Returns

The following is returned:

Parameter	Type	Description
SID	String	Identifies the unique session ID (SID) to use for all other Web Services calls. It is in plain text format.

Implement loginServiceManaged in Java

The following shows how to generate Certificates and then use these generated Certificates to access the CA SDM web services.

In the following example, the login process completes using the CA SDM Certificate and then performs two common web services calls. The getBopsid() web services method call allows you to obtain a token that is linked to a specific user. This token can be used to login to the CA SDM web interface as the linked user without being prompted for a password. This allows seamless integration to be enabled between different applications.

Important! The generated BOPSID token expires after 30 seconds, so it must be used promptly.

Important! There is a known issue when using the 1.4 version of the AXIS tool. For more information, see the *Release Notes*.

Follow these steps:

1. Generate the stub classes with AIXS Tool WSDL2Java. For more information, see the Generating Stub Classes with AXIS Tool WSDL2Java section from the PKI_loginServiceManaged_JAVA_steps file. Find the file in the following location:

   ```
   $NX_ROOT/samples/sdk/websvc/java/test1_pki
   ```

2. Start the CA SDM service.

3. Run pdm_pki -p DEFAULT.
   DEFAULT.p12 is created in the current directory. This policy will have the password equal to the policy name (in this case DEFAULT).

   Note: This command will also add the Certificate's public key to the field pub_key field (public_key attribute) in the sapolicy table/object.

4. Log into CA SDM

5. Select **SOAP Web Services Policy**, **Policies** on the **Administration** tab.
   The **SOAP Web Services Access Policy List** page opens.

6. Click **DEFAULT**.
   The **SOAP Web Services Access Policy Detail** page opens.

7. Complete the **Proxy Contact** field (in this example, ServiceDesk) and confirm that the DEFAULT policy record Has Key field displays "Yes."

8. Copy DEFAULT.p12 (from the directory where command pdm_pki is executed), the JSP file called *pkilogin.jsp* and the HTML file called *pkilogin.htm* (from the $NX_ROOT/samples/sdk /websvc/java/test1_pki directory) to the following directory:

   ```
   $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/axis
   ```

9. Open the HTML form (from the axis directory). For example, http://localhost:8080/axis /pkilogin.htm
   Complete the appropriate fields.

   Note: The Directory field identifies the location of the Certificate file. Modify the path to the correct location.

10. Click Log me in!
    The results page opens.

11. Click the BOPSID URL.

    Important! Click this immediately! The BOPSID has a limited life token of about 30 seconds.

    The format of a URL using a BOPSID is as follows:
    http://<server name>:CA Portal/CAisd/pdmweb.exe?BOPSID=<BOPSID value>

Note: In order to use the loginServiceManaged method for a Java client program running on AIX, you may need to replace a pair of security policy files within your JAVA_HOME. Go to http://www.ibm.com (http://www.ibm.com) and search for "developerworks java technology security information AIX". In the "developerWorks : Java technology : Security" document, follow the link to "IBM SDK Policy files". Download the unrestricted policy files, local_policy.jar and US_export_policy.jar. Use these files to replace the original files in your JAVA_HOME/lib/security directory."

Generate Stub Classes with WSDL2Java

You can generate the stub classes for the CA SDM web services.

To generate stub classes with WSDL2Java

1. Open a command prompt and navigate to the "<drive>:\program files\CA" directory.
   The directory appears.

2. Run the dir /x command.
   The short form of the CA SDM directory appears. For example, the short name is "SERVIC~1."

3. Search for javac.exe on all of the server's local drives. If you locate the file, make note of its location because you will need to reference it in a batch file.

   Note: If you do not locate javac.exe, go to Http://java.sun.com and search for Java J2SE SDK to download. This may require a reboot.

4. Build a batch file called build_wsdl.bat and place it in the following directory:

   ```
   $NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\axis
   ```

5. Use the following code for the batch file, updating the bold items as appropriate:

```
@echo off
::#####################################################################
::# Simple bat file to Build Unicenter Service Desk Version 11.0 USD Stub classes
::# Use it to create the required USD Unicenter Service Desk Version 11.0 Java Web
Services classes
::#
::#  Usage: build_wsdl
::#####################################################################
@REM Update this with the PATH to USD NX_ROOT location
@SET USD_SHORT_PATH=C:\Progra~1/CA/Servic~1/

@REM Update this with the PATH to the JDK javac.exe compiler
@REM (this is used in the 2nd part of this file)
@SET JAVAC_EXE="C:\j2sdk1.4.2_13\bin\javac.exe"
@REM Update this to the path to the USD <USDK> <rellevel> NX_ROOT/java/lib location
@SET USD_TOMCAT=%USD_SHORT_PATH%java/lib
@SET CP=%USD_TOMCAT%/axis.jar;%USD_TOMCAT%/commons-discovery.jar;%USD_TOMCAT%/commons-
logging.jar;%USD_TOMCAT%/jaxrpc.jar;%USD_TOMCAT%/saaj.jar;%USD_TOMCAT%/log4j-1.2.8.
jar;%USD_TOMCAT%/xml-apis.jar;%USD_TOMCAT%/xercesImpl.jar;%USD_TOMCAT%/wsdl4j.jar;%
USD_TOMCAT%/axis-ant.jar
@REM Please specify the path to java.exe file below
@REM You can obtain this by reviewing the NX.env file use the @NX_JRE_INSTALL_DUR
@REM variable to derive this info
@SET JAVA_PATH=C:\Program Files(x86)\CA\SC\JRE\1.6.0_30
@SET JAVA_EXE="%JAVA_PATH%\bin\java.exe"
@cd WEB-INF\classes
%JAVA_EXE% -cp %CP% org.apache.axis.wsdl.WSDL2Java http://localhost:8080/axis/services
/USD_Unicenter Service Desk Version 11.0_WebService?wsdl
@cd ..\..
::#####################################################################
::# This next section compiles the Service Desk stub code
::# Once complete, you should recycle tomcat with the following
::# commands or by recycling Service Desk:
::#       pdm_tomcat_nxd -c STOP
```

```
::#       pdm_tomcat_nxd -c START
::#####################################################################
@SET CP=".\classes;%CP%"
@SET STUBS_DIR=classes\com\ca\www\UnicenterServicePlus\ServiceDesk
@cd WEB-INF
%JAVAC_EXE% -classpath %CP% -deprecation -d classes %STUBS_DIR%\ArrayOfInt.java
%JAVAC_EXE% -classpath %CP% -deprecation -d classes %STUBS_DIR%\ArrayOfString.java
%JAVAC_EXE% -classpath %CP% -deprecation -d classes %STUBS_DIR%\ListResult.java
%JAVAC_EXE% -classpath %CP% -deprecation -d classes %STUBS_DIR%\USD_WebService.java
%JAVAC_EXE% -classpath %CP% -deprecation -d classes %STUBS_DIR%\USD_WebServiceLocator.
java
%JAVAC_EXE% -classpath %CP% -deprecation -d classes %STUBS_DIR%\USD_WebServiceSoap.
java
%JAVAC_EXE% -classpath %CP% -deprecation -d classes %STUBS_DIR%
\USD_WebServiceSoapSoapBindingStub.java
@cd ..
```

After running the batch file from the command prompt, the stub classes are in place and compiled.

- Recycle Tomcat as follows:
  - pdm_tomcat_nxd -c STOP
  - pdm_tomcat_nxd -c START

Using the Automated Tasks Editor

This article contains the following topics:

You can author, debug, test, and upload automated tasks in your support environment using the Automated Tasks Editor. You can create automated tasks by customizing default templates and components. Modifying these defaults requires minimal or no coding, but if any errors occur, the application displays the line of code reporting the error.

The editor uses web services to access automated tasks depending on provided credentials during CA SDM authentication. An Administrator can permit analysts to access the server with the Automated Task Editor, and allow analysts to modify and upload public or tenant-specific scripts. The editor provides dialogs to edit the basic automated task settings, security settings, and dependencies on libraries and static content items. The automated task framework implements three objects used by the automated task author: Task, Step, and Logger.

You can do the following with automated tasks:

- Create and customize steps based on automated task step templates provided by CA Technologies.
- Customize an automated task by editing the step template properties in a property sheet, or by editing the code directly. The code editor supports syntax highlighting and automatic code completion functionality while typing.

- An Administrator can run reports that show whether automated tasks were successful or not. The definition of success varies considerably depending on what the automated task is trying to do. CA SDM provides the *Functions.SetExecutionState()* function call that enables the task to declare its execution state as being success, fail, or not setting it at all. The automated task execution state field filters the report.

- Send emails to end users or to an external system using the CA SDM mail daemon.

Localize automated tasks by declaring all strings to localize as automated task step properties. You can edit these step properties in the Automated Task Editor for each supported locale separately. The values of these properties are accessed from automated task step script code using Step. GetProperty() which returns the correct localized version of the specified property based on the localization ID of the customer running the automated task.

Edit an Automated Task

You can download automated tasks from the server and edit them in the Automated Task Editor. Any content that is newer in the version than the existing content on the server is imported into the database and made available to administrators of that tenant.

To edit an automated task

1. Open the Automated Task Editor.
   The Support Automation Task Editor appears.

2. On the toolbar, select the Upload Automated Task icon.
   The Open Automated Task from Server pane appears.

3. Select the automated task that you want to download.
   Note: If you are a privileged user in a multi-tenancy environment, you can edit public or tenant-specific automated tasks.

4. Click Open Task.
   The Support Automation Task Editor downloads the task to the client and opens it in the application.
   The download creates a text file on the computer of the task author that contains the dependent content.

Upload an Automated Task

You can upload automated tasks that you created in the application. When you select a task, all dependent content automatically uploads, such as libraries and static content.

To upload an automated task

1. Open the Automated Task Editor.
   The Support Automation Task Editor appears.

2. Select the automated task you want to upload.

3. Select the classification where you want to upload the task.
   Note: If you are a privileged user in a multi-tenancy environment, select the appropriate tenant when uploading the automated task, or make the task public.

4. On the toolbar, select the Upload Automated Task icon.
   The Support Automation Task Editor uploads the task to the server.

How an Automated Task Runs

This article contains the following topics:

CA SDM provides a framework which is a block of script code responsible for the code that deals with presenting user interfaces and retrieving user input from user interface steps. The framework exists so that you can do complex things with automated tasks, interface-related, using simple code, rather than complex code that would otherwise be necessary. The framework includes two objects (Task and Step). You can use these objects to interact with the framework and control how automated tasks execute, including setting up and accessing the user interface.

Note: When running an automated task in the Automated Task Editor, the editor acts as both server and client.

The following process describes what happens when you execute an automated task:

1. Use the framework to assemble the script code to execute together with the step code in the automated task definition, and any dependent library code.

2. The server assembles and distributes the code to the end-user environments.

3. Both the end user and the analyst receive the entire assembled automated task.

4. The server initiates each step in turn at the relevant client.

How Analysts Receive Data

You can have an automated task gather data and store it in the Support Automation database associated to the specific task execution. The data can be picked up by a post session integration that can use the data or pass it to an external system. In such a case, typically you construct this data as an XML fragment.

Use Functions.SetAcquiredData() to store data (text), associated with a task execution. Support Automation allows one such text field of any length to be stored for each execution of an automated task. You can store data in one step and access it in a subsequent step as follows:

1. The server sends the initial state of this data storage to the client with the instruction to execute a step.

2. At the end of the step, the client sends the persisted data state back to the server so the server can send this data to whichever client is executing the next step.

3. An analyst user interface step can gather input from the analyst and store it.

4. The end-user user interface step can access the data that was supplied by the analyst.

Automated Task Elements

This article contains the following topics:

You create automated tasks by defining steps in an automated process. Automated tasks predefine routines with specific actions on the end-user computer without the need for the analyst or end user to do the process. Common routines include gathering telemetry information, diagnosing problems, and implementing resolutions.

An automated task consists of the following elements:

- **Task Settings**
  Specifies the title, description, dimensions of the step windows, HTML headers and footers, and a CSS style sheet applied to the end-user interface.

- **Dependencies**
  Specifies the libraries and static content items that the task depends on, such as images or CSS files.

- **Task Steps**
  Specifies the executed code for each step. You can author steps by selecting automated task step templates and modify them to fit your needs.

- **Security Settings**
  Specifies the appropriate security settings to run the automated task on an end-user computer, such as read/write permissions, registry privileges, and so on.

- **XSDF Files**
  Specifies automated task definitions saved to an XML schema in XSDF files (XML Script Definition Format). The XSDF file contains all automated task settings, dependencies, security settings, and step code information.
  If the automated task is dependent on a particular library, the full script code of that library is written to the XSDF file, not only the dependency information. Dependencies are also imported when XSDF files are loaded into the Automated Task Editor or imported into CA SDM, unless a later version of the same dependent library exists in the target environment. The same is true for dependent static content. Script libraries can also be saved on their own to XSDF files for distribution between systems.

The editor lets you define CSS styles for all automated task elements. You can control the appearance by using CSS Styles.

Example Default CSS Styles

The following CSS styles are defined by default.

Note: If you use a custom CSS file, you can override the default values.

```
#header {
                padding: 2px 8px;
                font-size: 16pt;
                font-weight: bold;
                border-bottom: 2px solid green;
}
#title {
                background-color: #eee;
                padding: 2px 8px;
                font-size: 12pt;
                font-weight: bold;
                border-bottom: 1px solid green;
}
#content {
                padding: 8px;
}
#buttons {
                background-color: #eee;
                border-top: 1px solid green;
                text-align: right;
                padding: 2px 8px;
}
#buttons input {
                font-family: Verdana;
                font-size: 10pt;
}
#footer {
                border-top: 2px solid green;
                padding: 2px 8px;
                font-size: 9pt;
}
```

The supplied HTML components declare a CSS Style for an HTML DIV that encloses the component. This declaration allows all elements of the components to be styled through CSS.

The name of this style can usually be set through automated task step template properties for steps that use these HTML components.

Task Object Reference

The task object is directly referenced as Task [e.g., Task.End();]

Methods

Task	Description
End()	Ends the Task immediately.
GetNamedDataItem(key)	Returns the value previously stored with the specified key.
SetNamedDataItem(key, value)	Stores the value against the specified key. These values can be stored in one step and accessed in another using GetNamedDataItem(). The specified value can be JavaScript primitive type (number, boolean, string) or an object or an array of objects. In VBScript, only primitive types can be stored.
GetNextElementId()	Returns a unique identifier that can be used for HTML DOM objects.
GetPageBodyElementById(id)	Returns the HTML DOM object corresponding to the specified ID.
ReplaceDataItems(string)	Returns a copy of the specified string with all instances of stored data items in the format ${key} replaced by their stored values.
CloseIEWindow()	Closes the UI window if it is open.

Properties

Property	Description
Title	The title of the automated task.
HeaderHtml	The HTML placed in the header section of the UI window.
FooterHtml	The HTML placed in the footer section of the UI window.
Height	The height, in pixels, of the UI window.
Width	The width, in pixels, of the UI window.
NextStepIndex	The index (0-based) of the next step to be executed.

Step Object Reference

The step object is directly referenced as Step [e.g., Step.End();]

Methods

Step Object	Description
End()	Ends the step immediately. The next step will be invoked.
Controls.Add()	Adds a string or HTML component to the UI content. Strings are automatically converted to Label HTML components.
GetProperty (propertyKey)	Returns the value of the specified property key for the current localization. If no value exists for the current localization, the value of the property in the default localization will be returned.

SetProperty (localizationID, propertyKey, value)	Sets the value of the specified property to the specified value for the specified localization ID.
RegisterEventHandler(controlId, eventHandler, tag)	Registers the specified event handler as the function to be invoked when the IE window's raiseUIEvent(controlId) function is called. Any data passed as tag will be made available when the event handler is dispatched as Step.EventData.
IsUIStep()	Returns true if the current step is a UI step; false otherwise.

Properties

Property	Description
Title	The title of the step - displayed in the UI header section.
NextButtonLabel	The label for the "Next" button. Defaults to "Next".
NextButtonVisible	True to show the "Next" button. False to hide it.
PreviousButtonLabel	The label for the "Previous" button. Defaults to "Previous."
PreviousButtonVisible	True to show the "Previous" button. False to hide it.
FinishButtonLabel	The label for the "Finish" button. Defaults to "Finish."
FinishButtonVisible	True to show the "Finish" button. False to hide it.
EventData	When a UI event is raised (by calling raiseUIEvent() from HTML within the IE window) the event handler function previously registered with RegisterEvenHandler() is invoked. The data stored as the "tag" when the event handler was registered will be available as Step.EventData when the handler is dispatched.

Logger Object Reference

The Logger object is accessed as Trace.Framework.

Example:

Trace. Framework.Level = TraceLevels.Info

Trace.Framework.Error("An error has occurred")

Methods

Logger Object	Description
Fatal(msg)	Log the specified message if the current trace level is set at Fatal, Error, Warning, Info, Debug, or Verbose.
Error(msg)	Log the specified message if the current trace level is set at Error, Warning, Info, Debug, or Verbose.
Warning (msg)	Log the specified message if the current trace level is set at Warning, Info, Debug, or Verbose.
Info(msg)	Log the specified message if the current trace level is set at Info, Debug, or Verbose.
Debug (msg)	Log the specified message if the current trace level is set at Debug or Verbose.
Verbose (msg)	Log the specified message if the current trace level is set at Verbose.

Properties

Property	Description
Level	The current trace level. Set to one of the values in the TraceLevels enumeration (None, Fatal, Error, Warning, Info, Debug, or Verbose).

Global Functions

The following global functions are used in Support Automation procedures.

Function	Description
AnyArrayToVBArray(array)	Converts any array (VBScript or JavaScript) to a VBArray. Arrays in JavaScript are different objects to VBScript arrays so it is necessary to convert between them.
AnyArrayToJSArray(array)	Converts any array to JavaScript array.
CreateHashMap()	Returns an object that can be used as a hashmap for storing arbitrary data (key/value pairs). The returned object implements the following methods:
	Get(key) - Returns the value stored against the specified key.
	Set(key,value) - Stores the value for the specified key.
	GetAllKeys() - Returns an array of the keys.

Automated Task Step Templates

Automated task step templates are the script code for a given automated task step that can also define automated task step properties. You can customize the behavior of the automated task step template by changing the values of automated task step properties in the property sheet. You can accomplish more extensive customization by editing the code directly, but the intent is to minimize the amount of coding you do.

Steps are end-user action steps or user interface steps that show either to the end user or analyst. The automated task step templates are either end-user action, analyst interface, or end-user interface templates. CA Technologies provides automated task step templates, both action and user interface, to form the building blocks of tasks and enable you to create functional automated tasks with minimal coding.

For steps that define properties, you are prompted to provide values for these properties when the step is first created from the template. You can modify these values using the property sheet.

User Interface Steps

All user interface steps must implement an OnLoad function called by the framework before the step is displayed. The OnLoad function sets up the user interface. The step object exposes several properties and methods that you can use to set up the user interface.

You can control the visibility of the buttons on the step footer using Step.NextButtonVisible, Step. FinishButtonVisible, and Step.PreviousButtonVisible. When you set these properties to True, it makes the button appear. If a button is shown, a handler must be implemented for it. You can add the actual user interface controls to the page body using HTML components.

Example Text Input Box as an HTML Component

The step object has a controls array that is populated with a series of HTML components. These script objects render in HTML, and when the framework renders a user interface page, each HTML component in its controls array renders itself and adds the returned HTML fragment to the HTML body of the page.

HTML components let you write complex user interfaces without extensive HTML knowledge. Using an HTML component, you can create and configure commonly used controls with minimal coding.

Example: Text Input box as an HTML Component

An example of an HTML component is a text input box. The following example combines a label called PromptText and an HTML input box. If you want to prompt the customer or technician to supply a user name for example, the user interface page is constructed in an OnLoad function as follows:

```
Function OnLoad
    Dim myInputBox
    Set myInputBox = UI.MakeInputBox()
    myInputBox.PromptText = "Please enter your name:"
    Step.Controls.Add(myInputBox)
End Function
```

CA Technologies supplies samples, but you can also create custom HTML components. An HTML component is a script object that implements a method called GetHtml. Here, for example, is the implementation of that *MakeInputBox()* method call used in the previous example:

```
function InputBox() {
    // public properties
    this.PromptText = "";
    this.CssClass = "UIInputBox";
    this.InputMaxLength =50;
    this.InputSize = 50;

    // private member props
    var textboxId = Task.GetNextElementId();

    // privileged methods
    // (For example, publicly accessible with access to private props)
    this.GetHtml = function () {
        var inputHtml =
            "<DIV class = '" + this.CssClass + "'>\n";
        if(this.PromptText.length>0) {
            inputHtml +=
"<SPAN class ='PromptText'>" + this.PromptText + "</SPAN>\n" +
                "<BR>\n";
        }
        inputHtml +=
            "<INPUT type = text class = 'InputText' id = '"+textboxId+
            "' size = '"+this.InputSize+
"' maxlength='"+this.InputMaxLength+"'></INPUT>" +
            "<BR><BR>\n" +
            "</DIV>\n";
        return inputHtml;
    }

    this.GetUserInput = function() {
        var textBox = Task.GetPageBodyElementById(textboxId);
        if (textBox) {
            return textBox.value;
        }
        else {
            throw new Exception (Severity.Error,
"Could not read textbox value",
"Could not read textbox value");
        }
    }
}
return new InputBox();
```

This automated task library function defines a constructor for an object of type InputBox. The last line of the function constructs an instance of the InputBox class and returns it.

Object definitions differ in JavaScript and VBScript. In VBScript, the class keyword is used to declare a class. In JavaScript the function keyword declares the class, because in JavaScript functions are objects. Both languages let the class have public and private member variables and methods. A full description of how object syntax is handled in the two languages is beyond the scope of this chapter, but the internet can provide examples and tutorials on this subject.

In the example above, the code declares the InputBox class with some public and private properties and two public methods, GetHtml and GetUserInput.

The Framework calls GetHtml when rendering user interface steps. The InputBox control also exposes GetUserInput which you can use to access the value that the end user enters into the text box. Each HTML component can expose different methods for configuring it and accessing any user input values.

The HTML coding is abstracted from you by these HTML components so that creating user interface pages is simplified.

You can write your own HTML entirely for a particular automated task. In such a case, you have two choices: Write a new HTML component for the case you require, or construct the HTML code in a string variable and wrap it in a special HTML component called RawHTMLContainer as follows:

```
Function OnLoad
    Dim myRawHtmlContainer, myHtml
    myHtml = "<H1>Hello <B>World</B></H1>"
    Set myRawHtmlContainer = UI.MakeRawHtmlContainer(myHtml)
    Step.Controls.Add(myRawHtmlContainer)
End Function
```

Example End-User Input Handling

After the user interface page displays, in many cases it is necessary to handle end-user input when the user clicks one of the footer buttons, such as Next, Previous, or Finish. You implement handler functions to handle end-user input. You implement a function named *NextButtonHandler* to handle the clicking of the Next button. You can use the *PreviousButtonHandler* and *FinishButtonHandler* functions to handle the Previous and Finish buttons.

The handler performs the following actions:

- Retrieves input data from HTML components on the page
- Validates the end-user input
- If end-user input is invalid, display an error message and refresh the page
- If end-user input is valid, logs stores it for use in a later step
- Controls the sequence of step execution

Example: End-User Input Handling

HTML components that wrap input controls, such as the InputBox component, expose methods to access the values supplied by the end user. In this case, the *GeUserInput()* function is exposed.

You can control the next step that the framework presents as follows:

- Return True from the handler to present the default next step (currentStep+1 for NextButtonHandler, currentStep-1 for PreviousButtonHandler, end the automated task for FinishButtonHandler).
- Return False from the handler to refresh the current step.
- Set Step.NextStepIndex to the step index (1 based) to skip or repeat steps.

You can handle the Next button being clicked by supplying a NextButtonHandler. Because the NextButtonHandler has to access the HTML component that was created in the OnLoad, the declaration (Dim statement) of this variable is placed outside these functions. Thus, the entire step code would look as follows:

```
Dim myInputBox

Function OnLoad
    Set myInputBox = UI.MakeInputBox()
    myInputBox.PromptText = "Please enter your name:"
    Step.Controls.Add(myInputBox)
End Function
Function NextButtonHandler
    Dim userInputValue

    ' Retrieve the data supplied by the user
userInputValue = myInputBox.GetUserInput()

' Validate the data
If Len(userInputValue) = 0 Then
    ' Show error message
    Functions.ShowMessage "You must supply a name"

    ' Re-present current step
    NextButtonHandler=False
Else
    ' Log the data
    Functions.LogMessage "User name set to: " & userInputValue

    ' Store the data
    Task.SetNamedDataItem "UserName", userInputValue

' Proceed to next step
NextButtonHandler=True
End If
End Function
```

Script Library Management

This article contains the following topics:

You can use the same script functionality that gathers specific data or impacts certain changes on a remote machine in many various automated tasks. Support Automation provides the concept of script library to package such reusable code. You use script libraries to help you reuse and maintain code. These libraries contain functions written in JavaScript or VBScript that automated tasks can call. The automatic code completion feature of the Automated Task Editor provides a function description text and argument descriptions when you edit automated task step script code.

You can create your own libraries. The Automated Task Editor displays defined JavaScript and VBScript libraries on the left pane. Script libraries let you do the following:

- Create libraries and functions
- Provide descriptions of the Function arguments
- Export and Import from XSDF files or directly from the Support Automation server
- Define the function name, description, arguments, and script text

Return Objects from Library Functions

You can return an instance of an object from a library function, such as for library functions that manufacture HTML Components. Returning an object requires you to declare a class and instantiate an instance of that class. Class declarations are done differently in JavaScript and VBScript.

In JavaScript, you define classes by declaring a function that is actually the constructor for the class. Public properties and methods are added to the class using the *this* keyword. You declare private properties by using the *var* keyword. In JavaScript, you can declare a class inside a function definition.

In VBScript, class definitions are not permitted inside functions, however, you can provide the code that forms the implementation of a given function. You create class definitions using one of the following techniques:

- Constructing the class definition code in a string and executing it with *ExecuteGlobal*.
- Calling a second function and returning whatever it returns. End the function. Declare the class, then the second function.

Local File System/Registry Access

Many automated tasks require reading or modifying the file system or registry. The Windows Script Host (WSH) provides some scriptable COM components (such as FileSystemObject) to enable scripts to read or modify the file system or registry. Some antivirus programs implement script blocker utilities that interfere with those COM components, often flagging any script that tries to instantiate the relevant component as being malicious. Clearly, it is not desirable to have script blockers interfere with the activities of analysts who are trusted and trying to repair a problem. The CA SDM functions library contains functions for interacting with the file system and registry that enable much the same functionality that the Windows components expose, without being subject to the action of script blocker programs.

The standard WSH components are used when you write automated tasks for an internal corporate environment where the end-user computer state is known, and assumed that script blockers are not present. You can use the functionality in the CA SDM Functions COM component to implement any file system or registry activity for external environments (customers at home or on the public Internet) when the organization that is providing support does not control the end-user computer configuration.

Windows Management Instrumentation (WMI) Support

Automated tasks support Windows Management Instrumentation (WMI), a component of the Windows operating system that provides management information and control in an enterprise environment. By using industry standards, you can use WMI to query and set information about desktop systems, applications, networks, and other enterprise components.

WMI lets you access and modify the operating system. WMI is based upon SQL-style queries that allow an automated task to query information from the operating system and then, using objects, to manipulate that data. WMI is a powerful system and is often the preferred method for automated tasks to carry out their purposes.

Example: Script fragment that enumerates the currently configured Operating System Services.

```
strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
    & "{impersonationLevel=impersonate}!\\" & strComputer & "\root\cimv2")

Set colRunningServices = objWMIService.ExecQuery("Select * from Win32_Service")

For Each objService in colRunningServices
    Wscript.Echo objService.DisplayName  & VbTab & objService.State
Next
```

Static Content Management

Automated tasks can present a user interface that requires you to use images or CSS files to appear correctly. This static content (images and CSS files) is associated with the automated task definition as the task is dependent on them. You can do the following:

- Import static content and associate it to automated tasks.
- Add, edit, delete, and upload to the Support Automation server.
- Select an image or text file to import and assign a globally unique identifier (GUID).
- Use the Automated Task Editor to assign static content items to automated tasks.

When you assign the static content item, you associate the automated task and it is saved in the XSDF with the task. The static content automatically deploys to the server when the dependent automated task deploys.

Static content is stored in the Support Automation database on the server. A servlet provides access to these images based on their ID. The Functions library call *Functions.GetStaticContentItemRef()* returns the URL to that servlet, which takes the ID as a parameter. The Automated Task Editor provides a toolbar button that brings up the Static Content Items dialog, which allows you to select the desired item. When you click OK, the *Functions.GetStaticContentItemRef()* call is automatically inserted into the code with the relevant ID.

Note: Status content has a limit of 50 KB per item.

Functions and WScript Usage

The framework provides two scriptable COM components that are accessible to all automated tasks running in CA SDM. These COM components are Functions and WScript.

Functions

The functions component is a collection of procedure calls that are used for the following:

- Accessing the local file system and or registry without triggering antivirus script blocker programs
- Accessing the Support Automation server functionality such as:
  - Writing session log entries
  - Storing automated task acquired data
  - Setting automated task execution state
  - Sending email
  - Escalating between products
  - Executing custom server routines

Functions COM Object Methods

This article contains the following topics:

The following Functions COM Object Methods are available for use in Support Automation automated tasks.

Function	Description
B64Encode (BSTR data, VARIANT *varResult)	Base64 encodes the specified data.
B64Decode (BSTR data, VARIANT *varResult)	Decodes the specified data.

CheckIfServerExists (BSTR URL, USHORT port, VARIANT *varResult)	Makes a request on the specified server to determine if it is accepting connections.
Eof (LONG fileno, VARIANT *varResult)	Determines if there is unread data in the specified text file
EscalateToLive (VARIANT *varResult)	Escalates the customers session from Self-Serve to Live Session
ExecuteRC (BSTR MethodName, BSTR ParamStr, int ParamCount, VARIANT *varResult)	Executes a RuleConduit call on the server allowing arbitrary server methods to be executed.
ExecuteWaitAndCaptureStream (BSTR strProg, int nStream, VARIANT *varResult)	Executes the specified command and waits for the process to exit, capturing the output from the process execution.
FileAddAttributes (BSTR szFilePath, LONG dwAttr, VARIANT *bvarResult)	Call to add attributes (Read-Only, Compressed, Archived, etc…) to a file without changing attributes already there.
FileCloseTextFile (LONG fileno)	Closes a text file previously opened with FileCreateTextFile or FileOpenTextFile.
FileCopyTo (BSTR szSourceFilePath, BSTR szDestFilePath, VARIANT_BOOL bcanOverwrite, VARIANT *bvarResult)	Call FileCopyTo to copy a file from one place to another.
FileCreateTextFile (BSTR szFilePath, BOOL overwrite, VARIANT *varResult)	Creates a new text file in the specified location returning a handle that can be used to interact with the file.
FileDelete (BSTR szFilePath, VARIANT *bvarResult)	Call to permanently delete a file.
FileExecute (BSTR szCommand, VARIANT *bvarResult)	Call to execute a file.
FileExecuteAndWait (BSTR szCommand, LONG dwMilliseconds, VARIANT *bvarResult)	Call to execute a file and wait for it to exit.
FileExists (BSTR szFilePath, VARIANT *bvarResult)	Checks whether a file exists or not.
FileGetAttributes (BSTR szFilePath, VARIANT *dwvarResult)	Call to retrieve the attributes (Read-only, archive, compressed, etc…) of a file.
FileGetDirectoryContents (BSTR pathName, BOOL showFiles, BOOL showDirs, VARIANT *varResult)	Returns the selected contents of the specified directory.
FileGetDrives (VARIANT *varResult)	Call to get a list of drives mounted.
FileGetDriveType (BSTR driveName, VARIANT *varResult)	Returns the type of the specified drive.
FileGetInfo (BSTR szFilePath, VARIANT *varResult)	Call to get the size and date information for a file.
FileGetINISectionContents (BSTR filename, BSTR sectionName, VARIANT *varResult)	Gets a pipe delimited list of the contents of the specified INI section.
	Gets the value of the specified item in the INI file.

FileGetINIValue (BSTR fileName, BSTR sectionName, BSTR keyName, BSTR defaultValue, VARIANT *varResult)	
FileGetInternetFile (BSTR szURL, BSTR szFilePath, VARIANT *bvarResult)	Call to download a file from the internet.
FileGetSize (BSTR szPath, VARIANT *varResult)	Gets the size of a file in bytes.
FileGetVersion (BSTR szFilePath, VARIANT *szvarResult)	Retrieves the version number of a file.
FileGetVolumeInfo (BSTR szVolumeRootPath, VARIANT *varResult)	Gets the information for a drive.
FileMakeDir (BSTR szDirPath, VARIANT *bvarResult)	Creates a directory.
FileMoveTo (BSTR szSourceFilePath, BSTR szDestFilePath, VARIANT_BOOL bcanOverwrite, VARIANT *bvarResult)	Moves a file from one place to another.
FileOpenTextFile (BSTR szFilePath, BSTR szMode, VARIANT *varResult)	Opens the specified text file returning a handle that can be used to interact with the file.
FileReadLine (LONG fileno, VARIANT *varResult)	Reads a line of text from the text file.
FileRecycle (BSTR szFilePath, VARIANT *bvarResult)	Recycles a file. Recycling places the file in the recycle bin and removes it from its original folder.
FileRenameTo (BSTR szSourceFilePath, BSTR szDestFilePath, VARIANT_BOOL bcanOverwrite, VARIANT *bvarResult)	Call FileRenameTo to change the name of a file.
FileSetAttributes (BSTR szFilePath, LONG dwAttr, VARIANT *bvarResult)	Sets the attributes (Read-only, archived, compressed, etc…) of a file.
FileSetINIData (BSTR filename, BSTR sectionName, BSTR keyName, BSTR data, VARIANT *varResult)	Sets the data for the specified key in the INI file.
FileWriteLine (LONG fileno, BSTR value, VARIANT *varResult)	Writes a line of text into the text file.
GetChildWindowCaption (int index, VARIANT *varResult)	Gets the caption for the specified child window.
GetChildWindowHandle (int index, VARIANT *varResult)	Gets the handle for the specified child window.
GetChildWindowProcessName (int index, VARIANT *varResult)	Gets the name of the process that owns the specified child window.
GetChildWindows (int hwnd, VARIANT *varResult)	Enumerates the windows that are children of the specified window storing the results for future querying, returning the count.
GetExecutionEnvironment (VARIANT *varResult)	Gets a string indicating where the script is being executed.
GetLocalization (VARIANT *varResult)	Gets the localization of the current user.
GetRootUrl (VARIANT *result)	Return the Server Root URL.

GetStaticContentUrl (VARIANT *result)	Return the Server Static Content URL.
GetStaticItemURL (BSTR itemGuid, VARIANT *varResult)	Retrieves the root URL of the given static content item.
GetSupportDeskOpen (VARIANT *varResult)	Gets the hours of operation status of the support desk.
GetWindowCaption (int index, VARIANT *varResult)	Gets the caption for the specified window.
GetWindowHandle (int index, VARIANT *varResult)	Gets the handle for the specified window.
GetWindowProcessName (int index, VARIANT *varResult)	Gets the name of the process that owns the specified window.
GetWindows (VARIANT *varResult)	Enumerates the system top level window handles, stores the results for future calls and returns the count.
HttpGet (BSTR szUrl, VARIANT *varResult)	Makes a request on the specified URL and returns the results.
HttpPost (BSTR szUrl, BSTR szBody)	Posts the specified request body to the specified URL.
InternetCheckConnection (VARIANT *varResult)	Determines if the customer machine appears to have a working internet connection.
LogMessage (BSTR szMessage)	Adds a message to the session log for the script execution.
OutlookGetPSTContents (BSTR szPSTPath, VARIANT *varResult)	Gets the contents of the specified Outlook PST file.
PromptUser (LONG Timeout, BOOL DefaultResult, BSTR Message, VARIANT *varResult)	Prompts the user with given message.
ReadLine (LONG fileno, VARIANT *varResult)	Reads a line of text from the text file. (deprecated, use FileReadLine instead).
RegCopyKey (BSTR szSourceRoot, BSTR szSourceKey, BSTR szDestRoot, BSTR szDestKey, VARIANT_BOOL bCanOverwrite, VARIANT *varResult)	Copies the entire contents of one key to another.
RegCopyValue (BSTR szSourceRoot, BSTR szSourceKey, BSTR szSourceValue, BSTR szDestRoot, BSTR szDestKey, BSTR szDestValue, VARIANT *bvarResult)	Copy the contents of one key/value to another. The user must have the ability to query keys for the root specified.
RegCreateKey (BSTR szRootPath, BSTR szKeyPath, VARIANT *bvarResult)	Creates a key entry in the user's registry.
RegDeleteKey (BSTR szRootPath, BSTR szKeyPath, VARIANT *bvarResult)	Removes a key from the registry. The user must have the ability to remove keys from the root specified.
RegDeleteValue (BSTR szRootPath, BSTR szKeyPath, BSTR szValueName, VARIANT *bvarResult)	Removes a key value from the registry. The user must have the ability to query keys for the root specified.
RegGetDWORD (BSTR szRootPath, BSTR szKeyPath, BSTR szValueName, VARIANT *dwvarResult)	Retrieves the a DWORD value from a specified key in the registry. The user must have the ability to query keys for the root specified.

RegGetString (BSTR szRootPath, BSTR szKeyPath, BSTR szValueName, VARIANT *szvarResult)	Retrieves a string value from a registry key. The user must have the ability to query keys for the root specified.
RegGetSubkeyByIndex (BSTR szRoot, BSTR szKey, LONG idxSubkey, VARIANT *varResult)	Retrieves the name of a subkey based on its index. The user must have the ability to query keys for the root specified.
RegGetSubkeysCount (BSTR szRoot, BSTR szKey, VARIANT *varResult)	Gets the number of keys underneath any given key. The user must have the ability to query keys for the root specified.
RegGetValueByIndex (BSTR szRoot, BSTR szKey, LONG idxValue, VARIANT *varResult)	Retrieves a key value given its index. The user must have the ability to query keys for the root specified.
RegGetValuesCount (BSTR szRoot, BSTR szKey, VARIANT *varResult)	Gets the number of values for a given key. The user must have the ability to query keys for the root specified.
RegGetValueType (BSTR szRootPath, BSTR szKeyPath, BSTR szValueName, VARIANT *dwvarResult)	Finds out the type of value for a given Registry key. The user must have the ability to query keys for the root specified.
RegKeyExists (BSTR szRootPath, BSTR szKeyPath, VARIANT *bvarResult)	Queries a key from the registry. The user must have the ability to query keys from the root specified.
RegMoveKey (BSTR szSourceRoot, BSTR szSourceKey, BSTR szDestRoot, BSTR szDestKey, VARIANT_BOOL bCanOverwrite, VARIANT *varResult)	Moves the entire contents of one key to another.
RegMoveValue (BSTR szSourceRoot, BSTR szSourceKey, BSTR szSourceValue, BSTR szDestRoot, BSTR szDestKey, BSTR szDestValue, VARIANT *bvarResult)	Moves the contents of one key value to another. The user must have the ability to query keys for the root specified and write to the destination.
RegRenameValue (BSTR szRootPath, BSTR szKeyPath, BSTR szOldValueName, BSTR szNewValueName, VARIANT *bvarResult)	Changes the name of a registry value. Note: The user must have the ability to query keys for the root specified.
RegRestoreKeyFromFile (BSTR szRootPath, BSTR szKeyPath, BSTR szFilePath, VARIANT *bvarResult)	Restores the entire contents of a key from a file into the registry. The user must have the ability to query and write keys for the root specified.
RegSaveKeyToFile (BSTR szRootPath, BSTR szKeyPath, BSTR szFileName, VARIANT *bvarResult)	Saves the entire contents of a key from the registry into a file. This file may then be restored using RegRestoreKeyFromFile. The user must have the ability to query keys from the root specified.
RegSetDWORD (BSTR szRootPath, BSTR szKeyPath, BSTR szValueName, LONG dwValue, VARIANT *bvarResult)	Sets a DWORD value in the registry. The user must have the ability to query keys for the root specified.
RegSetString (BSTR szRootPath, BSTR szKeyPath, BSTR szValueName, BSTR szValue, VARIANT *bvarResult)	Sets a string value for a key in the registry. The user must have the ability to query keys for the root specified.
RegValueExists (BSTR szRootPath, BSTR szKeyPath, BSTR szValueName, VARIANT *bvarResult)	Checks for the existence of a key/value pair in the registry. The user must have the ability to query keys for the root specified.

RunCommandAsImpersonatedUser (BSTR bapp, BSTR bargs, VARIANT_BOOL block, LONG timeout, VARIANT *varResult)	Runs an application with the same credentials the script has (deprecated). Returns 0 on success.
RunCommandAsUser (BSTR domain, BSTR user, BSTR password, BSTR app, BSTR args, VARIANT_BOOL block, LONG timout, VARIANT *varResult)	Runs an application as another user. Returns 0 on success.
SaveLog (BSTR fileName)	Saves the session log.
SendEmail (BSTR toAddress, BSTR emailSubject, BSTR emailBody)	Sends an email via CA Service Desk Manager mail daemon.
SetAcquiredData (BSTR data)	Save a chunk of script specific character data on the server for later use.
SetScriptSuccess (BOOL bSuccess, VARIANT *varResult)	Indicates whether the script executed successfully from the script's point of view.
ShowFileBrowseDlg (BSTR browseType, BSTR fileExt, VARIANT *varResult)	Shows the standard windows file browse dialog and returns the selected file.
ShowMessage (BSTR szMessage)	Displays the message to the user in a message box.
Sleep (LONG time)	Causes the execution thread to sleep.
TransferToQueue (BSTR queueID, BSTR queueName)	Sets the customer's current queue, this is the queue that the customer will enter if escalated to live.
UtilAttachDll (BSTR szDllPath, BSTR szHTTPLocation, VARIANT *varResult)	Loads a dll into the process space so that functions may be called from it.
UtilCloseTask (BSTR szProcName, VARIANT *bvarResult)	Closes a running task.
UtilDetachDll (LONG idDll, VARIANT *varResult)	Unloads a DLL from memory.
UtilEndProcess (BSTR szProcName, VARIANT *bvarResult)	Terminates the process with the specified name.
UtilExitWindows (LONG lAction, VARIANT_BOOL bForce, VARIANT_BOOL bRelogin)	Exits windows either by log off, restart, or shutdown.
UtilExternalMethodCall (LONG idDll, BSTR szFuncName, LONG lFuncType, BSTR szParams, VARIANT *varResult)	Executes a function from a loaded DLL.
UtilGetComputerName (VARIANT *varResult)	Gets the current computer name.
UtilGetEnvironmentVariable (BSTR szVarName, VARIANT *varResult)	Gets the value of a defined environment variable.
UtilGetOSVersion (VARIANT *varResult)	Gets the OS version.
UtilGetProcessByIndex (LONG idxProcess, VARIANT *varResult)	Retrieves process information for the specified process.
UtilGetProcesses (VARIANT *varResult)	Gets a list of all processes running on the customer machine.

UtilGetProcessesCount (VARIANT *varResult)	Gets the number of processes currently running on the customer machine.
UtilGetProcessMemory (LONG processID, VARIANT *varResult)	Gets the amount of memory used by the specified process.
UtilGetRunningTask (LONG idxWnd, VARIANT *varResult)	Gets information related to a task running on the customer machine. UtilGetRunningTasksCount should be called first to determine the number of tasks available.
UtilGetRunningTasksCount (VARIANT *varResult)	Gets a count of the tasks running on the customer machine.
UtilGetSystemDir (VARIANT *varResult)	Gets the windows system directory.
UtilGetSystemMetrics (LONG nIndex, VARIANT *varResult)	Gets the value of the specified system metric.
UtilGetUserName (VARIANT *varResult)	Gets the current user's logon name.
UtilGetWindowsDir (VARIANT *varResult)	Gets the directory for windows.
UtilGlobalMemoryStatus (VARIANT *varResult)	Gets information on global memory availability.

WScript

Many public domain script examples are available from sources such as Microsoft TechNet ScriptCenter, which are typically aimed at a system administrator audience, but are often useful for use in automated tasks. They often assume that the existence of an object called WScript, which Microsoft provides as part of their command-line script execution engine, but not part of the Windows Script Host in itself.

CA SDM implements a simple version of the WScript object providing the Echo, Sleep, GetObject, and CreateObject methods, providing compatibility for the most commonly used WScript methods. WScript.Echo(), which usually writes to the command line, is implemented in CA SDM to write to the automated task log, and thus WScript.Echo() is synonymous with Functions.LogMessage().

WScript COM Object Methods

The following WScript COM Object Methods are available for use in Support Automation automated tasks.

Object Method	**Description**
CreateObject (objDescription)	Creates an instance of the specified COM object.
Echo(msg)	Logs the specified message. Equivalent to Functions.LogMessage(msg).
GetObject (objDescription)	Used to get an instance of an object from a string reference to it.
Quit()	Ends the executing task immediately.
Sleep(time)	Pauses execution for the specified number of milliseconds. Equivalent to Functions.Sleep(time).

EBR_DICTIONARY Table

This article contains the following topic:

- **SQL Name** -- EBR_DICTIONARY
- **Object** -- EBR_DICTIONARY

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE KEY		
WORD_ID	INTEGER		
WORD	STRING 50 NOT_NULL S_KEY		
WORD_TYPE	INTEGER		
WORD_TOTAL_COUNT	INTEGER		
DF	INTEGER		
WORD_IDF	INTEGER		
last_mod_dt	LOCAL_TIME		

EBR_DICTIONARY_ADM Table

- **SQL Name** -- EBR_DICTIONARY_ADM
- **Object** -- EBR_DICTIONARY_ADM

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE KEY		
WORD_ID	INTEGER		
WORD	STRING 50 NOT_NULL S_KEY		
WORD_TYPE	INTEGER		
WORD_TOTAL_COUNT	INTEGER		
DF	INTEGER		
WORD_IDF	INTEGER		
last_mod_dt	LOCAL_TIME		

EBR_FULLTEXT Table

This topic contains the following topics:

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_FULLTEXT
- **Object** -- EBR_FULLTEXT

Field	Data Type	Reference	Remarks
DOC_TYPE	INTEGER		
ENTITY_ID	INTEGER		
FULL_WORD	STRING 50		
FULL_WORD_ REVERSE	STRING 50		
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
PERMISSION_INDEX_ID	INTEGER		
PRODUCT	STRING 50		
SHORT_WORD	STRING 50		
TABLE_ID	INTEGER		
WORD_COUNT	INTEGER		
WORD_COUNT_ PROBLEM	INTEGER		
WORD_COUNT_ RESOLUTION	INTEGER		
WORD_COUNT_ SUMMARY	INTEGER		
WORD_COUNT_ TITLE	INTEGER		
WORD_IDF	INTEGER		
WORD_ORDER	INTEGER		
WORD_TYPE	INTEGER		

EBR_FULLTEXT_ADM Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_FULLTEXT_ADM
- **Object** -- EBR_FULLTEXT_ADM

Field	Data Type	Reference	Remarks
DOC_TYPE	INTEGER		
ENTITY_ID	INTEGER		
FULL_WORD	STRING 50		
FULL_WORD_ REVERSE	STRING 50		
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
PERMISSION_ INDEX_ID	INTEGER		
PRODUCT	STRING 50		
SHORT_WORD	STRING 50		
TABLE_ID	INTEGER		

Field	Data Type	Reference	Remarks
WORD_COUNT	INTEGER		
WORD_COUNT_ PROBLEM	INTEGER		
WORD_COUNT_ RESOLUTION	INTEGER		
WORD_COUNT_ SUMMARY	INTEGER		
WORD_COUNT_ TITLE	INTEGER		
WORD_IDF	INTEGER		
WORD_ORDER	INTEGER		
WORD_TYPE	INTEGER		

EBR_FULLTEXT_SD Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_FULLTEXT_SD
- **Object** -- EBR_FULLTEXT_SD

Field	Data Type	Reference	Remarks
ENTITY_ID	INTEGER		
FULL_WORD	INTEGER		
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
SHORT_WORD	STRING 50		
TABLE_ID	INTEGER		
WORD_COUNT	INTEGER		
WORD_COUNT_ PROBLEM	INTEGER		
WORD_COUNT_ RESOLUTION	INTEGER		
WORD_COUNT_ SUMMARY	INTEGER		
WORD_COUNT_ TITLE	INTEGER		
WORD_IDF	INTEGER		
WORD_ORDER	INTEGER		
WORD_TYPE	INTEGER		

EBR_FULLTEXT_SD_ADM Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_FULLTEXT_SD_ADM
- **Object** -- EBR_FULLTEXT_SD_ADM

Field	Data Type	Reference	Remarks
ENTITY_ID	INTEGER		
FULL_WORD	INTEGER		
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
SHORT_WORD	STRING 50		
TABLE_ID	INTEGER		
WORD_COUNT	INTEGER		
WORD_COUNT_ PROBLEM	INTEGER		
WORD_COUNT_ RESOLUTION	INTEGER		
WORD_COUNT_ SUMMARY	INTEGER		
WORD_COUNT_TITLE	INTEGER		
WORD_IDF	INTEGER		
WORD_ORDER	INTEGER		
WORD_TYPE	INTEGER		

EBR_INDEX Table

This article contains the following topics:

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_INDEX
- **Object** -- EBR_INDEX

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE KEY		
ENTITY_ID	INTEGER NOT_NULL S_KEY		
WORD_ID	INTEGER NOT_NULL S_KEY		
WORD_TYPE	INTEGER NOT_NULL S_KEY		
WORD_ORDER	INTEGER		
WORD_COUNT	INTEGER		
WORD_COUNT_ TITLE	INTEGER		

WORD_COUNT_ SUMMARY	INTEGER
WORD_COUNT_ PROBLEM	INTEGER
WORD_COUNT_ RESOLUTION	INTEGER

EBR_INDEX_ADM Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_INDEX_ADM
- **Object** -- EBR_INDEX_ADM

Field	Data Type	Reference	Remarks
id	INTEGER UNIQUE KEY		
ENTITY_ID	INTEGER NOT_NULL S_KEY		
WORD_ID	INTEGER NOT_NULL S_KEY		
WORD_TYPE	INTEGER NOT_NULL S_KEY		
WORD_ORDER	INTEGER		
WORD_COUNT	INTEGER		
WORD_COUNT_ TITLE	INTEGER		
WORD_COUNT_ SUMMARY	INTEGER		
WORD_COUNT_ PROBLEM	INTEGER		
WORD_COUNT_ RESOLUTION	INTEGER		

EBR_INDEXING_QUEUE Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_INDEXING_QUEUE
- **Object** -- EBR_INDEXING_QUEUE

Field	Data Type	Reference	Remarks
ACTION	INTEGER		
ACTION_DATE	DATE		
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
INDEXED	INTEGER		
OBJ_PERSID	STRING 30		Persistent ID (SystemObjectName:id)
PRIORITY	INTEGER		
TEXT	STRING 32768		
TEXT	STRING 32768		

EBR_SYNONYMS Table

This article contains the following topics:

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_SYNONYMS
- **Object** -- EBR_SYNONYMS

Field	Data Type	Reference	Remarks
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
KEYWORD1	STRING 50		
KEYWORD2	STRING 50		
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.

EBR_SYNONYMS_ADM Table

Program control table used by Knowledge Management.

- **SQL Name** -- EBR_SYNONYMS_ADM
- **Object** -- EBR_SYNONYMS_ADM

Field	Data Type	Reference	Remarks
ID	INTEGER NOT_NULL KEY		Unique (to the table) Numeric ID
KEYWORD1	STRING 50		
KEYWORD2	STRING 50		
LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.

bop_sinfo--Display System Information

The bop_sinfo utility displays information about a single Majic-defined object. You can run this utility on the objects listed under Technical Reference (see page 3821).

Syntax

This command has the following format:

```
bop_sinfo [-s server] [-p] [-l] [-d] [f] [-q] [-t] [-m] [-a] object [-h]
```

- **-s server**
  Specifies the server to query.

- **-p**
  Displays the producer information.
- **-l**
  Displays the domset list.
- **-d**
  Displays database object information, including the name and type of all attributes.
- **-f**
  Displays factory information, including the rel_attr and common_name.
- **-q**
  Displays the schema name of the associated table.
- **-t**
  Displays triggers on the object.
- **-m**
  Displays methods used by the object.
- **-a**
  Displays attribute details.
- **object**
  The name of the object to query
- **-h**
  Displays help on the utility.

Example: Display System Information for the dmn object

```
bop_sinfo -d dmn
Factory dmn
 Attributes
   id            INTEGER
   producer_id    LOCAL STRING(20)
   persistent_id    STRING(30)
   sym            STRING(60) REQUIRED
   delete_flag    SREL -> actbool.enum REQUIRED
   desc        STRING(40)
   tables        BREL <- dcon.dom_id {dom_id = ?}
   last_mod       DATE
   last_mod_by    SREL -> cnt.id
   audit_userid    LOCAL SREL -> cnt.id
```

ES_CONSTANTS Object

This article contains the following topics:

The object details are as follows:

1. Associated Table: ES_CONSTANTS
2. Factories: default
3. REL_ATTR: id
4. Common Name: NAME
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Comments	COMMENTS	STRING		
id	ID	INTEGER		REQUIRED KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Name	NAME	STRING		
Property ID	PROPERTYID	INTEGER		
Property Value	PROPVALUE	INTEGER		

ES_NODES Object

The object details are as follows:

1. Associated Table: ES_NODES
2. Factories: default
3. REL_ATTR: id
4. Common Name: NODE_SHORT_DESC
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
DISPLAYED_TEXT	DISPLAYED_TEXT	STRING		
id	ID	INTEGER		REQUIRED KEY
last_mod_dt	LAST_MOD_DT	LOCAL_TIME		
LINK_ID	LINK_ID	INTEGER	ES_NODES id	
NODE_ID	NODE_ID	INTEGER		
NODE_SHORT_ DESC	NODE_SHORT_ DESC	STRING		
NODE_TYPE	NODE_TYPE	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
PARENT_NODE_ID	PARENT_NODE_ID	INTEGER		
QUERY_RESP_ NUMBER	QUERY_RESP_ NUMBER	INTEGER		
QUERY_RESP_ TYPE	QUERY_RESP_ TYPE	STRING		
RESPLINKID1	RESPLINKID1	INTEGER		
RESPLINKID2	RESPLINKID2	INTEGER		
RESPLINKID3	RESPLINKID3	INTEGER		
RESPLINKID4	RESPLINKID4	INTEGER		
RESPLINKID5	RESPLINKID5	INTEGER		
RESPLINKID6	RESPLINKID6	INTEGER		
RESPLINKID7	RESPLINKID7	INTEGER		
RESPONSE1	RESPONSE1	STRING		
RESPONSE2	RESPONSE2	STRING		
RESPONSE3	RESPONSE3	STRING		
RESPONSE4	RESPONSE4	STRING		
RESPONSE5	RESPONSE5	STRING		
RESPONSE6	RESPONSE6	STRING		
RESPONSE7	RESPONSE7	STRING		
ROOT_ID	ROOT_ID	INTEGER	ES_NODES id	
TREE_ID	TREE_ID	INTEGER	SKELETONS id	

ES_RESPONSES Object

The object details are as follows:

1. Associated Table: ES_RESPONSES
2. Factories: default
3. REL_ATTR: id
4. Common Name: RESPONSE_LINK_TEXT
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		REQUIRED KEY
last_mod_dt	LAST_MOD_ DT	LOCAL_TIME		
PARENT_ NODE_ID	PARENT_ NODE_ID	INTEGER	ES_NODES id	
RESPONSE_LINK_ID	RESPONSE_ LINK_ID	INTEGER	ES_NODES id	

Attribute	DB Field	Data Type	SREL References	Flags
RESPONSE_ LINK_ORDER	RESPONSE_ LINK_ORDER	INTEGER		
RESPONSE_ LINK_TEXT	RESPONSE_ LINK_TEXT	STRING		

ES_SESSIONS Object

The object details are as follows:

1. Associated Table: ES_SESSIONS
2. Factories: default
3. REL_ATTR: id
4. Common Name: EXTERNAL_ID
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
COMMENT_TEXT	COMMENT_TEXT	STRING		
EVALUATION	EVALUATION	INTEGER		
EXTERNAL_ID	EXTERNAL_ID	STRING		
id	ID	INTEGER		REQUIRED KEY
last_mod_dt	LAST_MOD_DT	LOCAL_TIME		
PATH_IDS	PATH_IDS	STRING		
PATH_QAS	PATH_QAS	STRING		
SESSION_ID	SESSION_ID	INTEGER		
TREE_ID	TREE_ID	INTEGER	ES_NODES id	

BSVC--func_access Object

This article contains the following topics:

The object details are as follows:

1. Associated Table: usp_functional_access
2. Factories: default
3. REL_ATTR: code

4. Common Name: sym
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
code	code	STRING 30		REQUIRED UNIQUE
type	type	SREL	func_access_type.id	REQUIRED
sym	sym	STRING 60		REQUIRED
description	description	STRING 1000		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	UUID	cnt.id	

BSVC--func_access_level Object

The object details are as follows:

1. Associated Table: usp_functional_access_level
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
access_level	access_level	INTEGER		REQUIRED
type	type	SREL	func_access_type.id	REQUIRED
sym	sym	STRING 60		REQUIRED
description	description	STRING 1000		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	UUID	cnt.id	

BSVC--func_access_role Object

The object details are as follows:

1. Associated Table: usp_functional_access_role
2. Factories: default

3. REL_ATTR: id
4. Common Name: sym
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
access_level	access_level	SREL	func_access_level.id	
func_access	func_access	SREL	func_access.code	
role	role	SREL	role.id	
description	description	STRING 1000		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	UUID	cnt.id	

func_access_type Object

The object details are as follows:

1. Associated Table: usp_functional_access_type
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
sym	sym	STRING 60		
default_access	default_access	SREL	func_access_level.id	
description	description	STRING 1000		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	UUID	cnt.id	

Table and Object Cross-References

This article contains the following topics:

This chapter provides several tables that allow you to easily cross-reference table names, SQL names, and object names. The chapter “Data Element Dictionary” lists a complete definition of the tables in the schema. The chapter “Objects and Attributes” lists the object definitions.

Table to SQL Name and Object

This table provides a cross-reference of each table in the database schema to its corresponding SQL and object names:

Table	SQL Name (AKA)	Object
Access_Levels	acc_lvls	acc_lvls
Access_Type_v2	acctyp_v2	acctyp
Act_Log	act_log	alg
Act_Type	act_type	aty
Act_Type_Assoc	atyp_asc	act_type_assoc
Active_Boolean_Table	actbool	actbool
Active_Reverse_Boolean_Table	actrbool	actrbool
admin_tree	admin_tree	ADMIN_TREE
Am_Asset_Map	am_map	am_asset_map
Animator	anima	ANI
Archive_Purge_History	arcpur_hist	arcpur_hist
Archive_Purge_Rule	arcpur_rule	arcpur_rule
Asset_Assignment	hier	hier
Atomic_Condition	atomic_cond	atomic_cond
Attached_Events	att_evt	atev
Attached_SLA	attached_sla	attached_sla
Attachment	attmnt	attmnt
attmnt_folder	attmnt_folder	attmnt_folder
Attribute_Name	atn	
Audit_Log	audit_log	audlog
Behavior_Template	bhvtpl	bhvtpl
Boolean_Table	bool_tab	bool
Bop_Workshift	bpwshft	wrkshft
BU_TRANS	BU_TRANS	BU_TRANS
Business_Management	busmgt	bmhier
Business_Management_Class	buscls	bmcls
Business_Management_Repository	busrep	bmrep
Business_Management_Status	busstat	bms
ca_asset_type	ca_asset_type	

Table	SQL Name (AKA)	Object
ca_company	ca_company	ca_cmpny
ca_company_type	ca_company_type	vpt
ca_contact	ca_contact	cnt
ca_contact_type	ca_contact_type	ctp
ca_country	ca_country	country
ca_job_function	ca_job_function	job_func
ca_job_title	ca_job_title	position
ca_location	ca_location	loc
ca_model_def	ca_model_def	mfrmod
ca_organization	ca_organization	org
ca_owned_resource	ca_owned_resource	nr
ca_resource_class	ca_resource_class	grc
ca_resource_cost_center	ca_resource_cost_center	cost_cntr
ca_resource_department	ca_resource_department	dept
ca_resource_family	ca_resource_family	nrf
ca_resource_gl_code	ca_resource_gl_code	gl_code
ca_resource_operating_system	ca_resource_operating_system	opsys
ca_resource_status	ca_resource_status	rss
ca_schema_info	ca_schema_info	
ca_site	ca_site	site
ca_state_province	ca_state_province	state
ca_tenant	ca_tenant	tenant
ca_tenant_group	ca_tenant_group	tenant_group
ca_tenant_group_member	ca_tenant_group_member	tenant_group_member
Call_Req	call_req	cr
Call_Req_Type	crt	crt
Call_Solution	crsol	crsol
Change_Act_Log	chgalg	chgalg
Change_Category	chgcat	chgcat
Change_Request	chg	chg
Change_Status	chgstat	chgstat
Chg_Template	chg_template	chg_tpl
CI_ACTIONS	CI_ACTIONS	CI_ACTIONS
CI_ACTIONS_ALTERNATE	CI_ACTIONS_ALTERNATE	CI_ACTIONS_ALTERNATE
CI_BOOKMARKS	CI_BOOKMARKS	CI_BOOKMARKS
CI_DOC_LINKS	CI_DOC_LINKS	CI_DOC_LINKS

Table	SQL Name (AKA)	Object
CI_DOC_TEMPLATES	CI_DOC_TEMPLATES	CI_DOC_TEMPLATES
CI_DOC_TYPES	CI_DOC_TYPES	CI_DOC_TYPES
CI_PRIORITIES	CI_PRIORITIES	CI_PRIORITIES
CI_STATUSES	CI_STATUSES	CI_STATUSES
CI_WF_TEMPLATES	CI_WF_TEMPLATES	CI_WF_TEMPLATES
Column_Name	cn	
Contact_Method	ct_mth	cmth
Controlled_Table	ctab	ctab
Cr_Call_Timers	crctmr	ctimer
Cr_Status	cr_stat	crs
Cr_Stored_Queries	crsq	crsq
Cr_Template	cr_template	cr_tpl
D_PAINTER	D_PAINTER	
Delegation_Server	dlgtsrv	dlgsrvr
Document_Repository	doc_rep	doc_rep
Domain	dmn	dmn
Domain_Constraint	dcon	dcon
Domain_Constraint_Type	dcon_typ	dcon_typ
EBR_ACRONYMS	EBR_ACRONYMS	EBR_ACRONYMS
EBR_FULLTEXT	EBR_FULLTEXT	EBR_FULLTEXT
EBR_FULLTEXT_ADM	EBR_FULLTEXT_ADM	EBR_FULLTEXT_ADM
EBR_FULLTEXT_SD	EBR_FULLTEXT_SD	EBR_FULLTEXT_SD
EBR_FULLTEXT_SD_ADM	EBR_FULLTEXT_SD_ADM	EBR_FULLTEXT_SD_ADM
EBR_INDEXING_QUEUE	EBR_INDEXING_QUEUE	EBR_INDEXING_QUEUE
EBR_KEYWORDS	EBR_KEYWORDS	EBR_KEYWORDS
EBR_LOG	EBR_LOG	EBR_LOG
EBR_METRICS	EBR_METRICS	EBR_METRICS
EBR_NOISE_WORDS	EBR_NOISE_WORDS	EBR_NOISE_WORDS
EBR_PATTERNS	EBR_PATTERNS	EBR_PATTERNS
EBR_PREFIXES	EBR_PREFIXES	EBR_PREFIXES
EBR_PROPERTIES	EBR_PROPERTIES	EBR_PROPERTIES
EBR_SUBSTITS	EBR_SUBSTITS	EBR_SUBSTITS
EBR_SUFFIXES	EBR_SUFFIXES	EBR_SUFFIXES
EBR_SYNONYMS	EBR_SYNONYMS	EBR_SYNONYMS
EBR_SYNONYMS_ADM	EBR_SYNONYMS_ADM	EBR_SYNONYMS_ADM
ES_CONSTANTS	ES_CONSTANTS	ES_CONSTANTS

Table	SQL Name (AKA)	Object
ES_NODES	ES_NODES	ES_NODES
ES_RESPONSES	ES_RESPONSES	ES_RESPONSES
ES_SESSIONS	ES_SESSIONS	ES_SESSIONS
Event_Delay	evt_dly	evtdly
Event_Delay_Type	evtdlytp	evtdlytp
event_log	event_log	event_log
event_type	event_type	event_type
Events	evt	evt
ext_appl	ext_appl	
External_Entity_Map	xent_map	ext_entity_map
Form_Group	frmgrp	fmgrp
Global_Change_Extension	g_chg_ext	g_chg_ext
Global_Change_Queue	g_chg_queue	g_chg_queue
Global_Contact	g_contact	g_cnt
Global_Issue_Extension	g_iss_ext	g_iss_ext
Global_Issue_Queue	g_iss_queue	g_iss_queue
Global_Location	g_loc	g_loc
Global_Organization	g_org	g_org
Global_Product	g_product	g_prod
Global_Queue_Names	g_queue_names	g_qname
Global_Request_Extension	g_req_ext	g_cr_ext
Global_Request_Queue	g_req_queue	g_cr_queue
Global_Servers	g_srvr	g_srvrs
Global_Table_Map	g_tbl_map	g_tblmap
Global_Table_Rule	g_tbl_rule	g_tblrule
Group_Member	grpmem	grpmem
Impact	impact	imp
INDEX_DOC_LINKS	INDEX_DOC_LINKS	INDEX_DOC_LINKS
Interface	interface	intfc
Iss_Template	iss_template	iss_tpl
Issue	issue	iss
Issue_Act_Log	issalg	issalg
Issue_Category	isscat	isscat
Issue_Property	issprp	iss_prp
Issue_Status	issstat	issstat
Issue_Workflow_Task	isswf	iss_wf

Table	SQL Name (AKA)	Object
KD_ATTMNT	KD_ATTMNT	KD_ATTMNT
kdlinks	kdlinks	kdlinks
Key_Control	kc	
Knowledge_Keywords	km_kword	kwrd
KT_REPORT_CARD	KT_REPORT_CARD	KT_REPORT_CARD
LONG_TEXTS	LONG_TEXTS	LONG_TEXTS
Managed_Survey	managed_survey	mgs
Mgs_Act_Log	mgsalg	mgsalg
Mgs_Status	mgsstat	mgsstat
Note_Board	cnote	cnote
NOTIFICATION	NOTIFICATION	NOTIFICATION
Notification_Urgency	noturg	noturg
Notify_Log_Header	not_log	lr
Notify_Object_Attr	ntfl	ntfl
NR_Comment	nr_com	nr_com
Object_Promotion	object_promotion	object_promotion
O_COMMENTS	O_COMMENTS	O_COMMENTS
O_EVENTS	O_EVENTS	O_EVENTS
O_INDEXES	O_INDEXES	KCAT
Options	options	options
Promo_Hist	promo_hist	promo_hist
P_GROUPS	P_GROUPS	P_GROUPS
Pcat_Loc	pcat_loc	pcat_loc
Person_Contacting	perscon	perscnt
Priority	pri	pri
Prob_Category	prob_ctg	pcat
Product	product	prod
Property	prp	prp
Property_Template	prptpl	prptpl
Queued_Notify	not_que	notque
Quick_Template_Types	quick_tpl_types	quick_tpl_types
Remote_Ref	rem_ref	rrf
Reporting_Method	repmeth	rptmeth
Req_Property	cr_prp	cr_prp
Req_Property_Template	cr_prptpl	cr_prptpl
Response	response	response

Table	SQL Name (AKA)	Object
Reverse_Boolean_Table	rbooltab	rev_bool
Rootcause	rootcause	rc
Rpt_Meth	rptmth	rptm
SA_Policy	sapolicy	sapolicy
SA_Prob_Type	saprobtyp	saprobtyp
Sequence_Control	seqctl	seq
Server_Aliases	srvr_aliases	srvr_aliases
Server_Zones	srvr_zones	srvr_zones
Service_Contract	svc_contract	svc_contract
Service_Desc	srv_desc	sdsc
session_log	session_log	session_log
session_type	session_type	session_type
Severity	sevrty	sev
SHOW_OBJ	SHOW_OBJ	SHOW_OBJ
SKELETONS	SKELETONS	KD
SLA_Contract_Map	sdsc_map	sdsc_map
SLA_Template	slatpl	slatpl
Spell_Macro	splmac	macro
Spell_Macro_Type	splmactp	macro_type
SQL_Script	sql_tab	
Survey	survey	survey
Survey_Answer	survey_answer	svy_ans
Survey_Answer_Template	survey_atpl	svy_atpl
Survey_Question	survey_question	svy_ques
Survey_Question_Template	survey_qtpl	svy_qtpl
Survey_Stats	survey_statistics	svystat
Survey_Template	survey_tpl	svy_tpl
Survey_Tracking	survey_tracking	svytrk
Table_Name	tn	
target_tgttpls_srvtypes	target_tgttpls_srvtypes	tgt_tgttpls_srvtypes
target_time	target_time	tgt_time
target_time_tpl	target_time_tpl	tgt_time_tpl
Task_Status	tskstat	tskstat
Task_Type	tskty	tskty
Timespan	tspan	tspan
Timezone	tz	tz

Table	SQL Name (AKA)	Object
Transition_Points	nottrn	
True_False_Table	True_False_Table	true_false
Type_Of_Contact	toc	typecnt
Urgency	urgncy	urg
User_Query	usq	usq
usp_caextwf_instances	usp_caextwf_instances	caextwf_inst
usp_caextwf_start_forms	usp_caextwf_start_forms	caextwf_sfrm
usp_ci_window	usp_ci_window	ci_window
usp_contact	usp_contact	cnt
usp_functional_access	usp_functional_access	func_access
usp_functional_access_level	usp_functional_access_level	func_access_level
usp_functional_access_role	usp_functional_access_role	func_access_role
usp_functional_access_type	usp_functional_access_type	func_access_type
usp_kpi	usp_kpi	kc
usp_kpi_data	usp_kpi_data	kcd
usp_lrel_asset_chgnr	usp_lrel_asset_chgnr	lrel_asset_chgnr
usp_lrel_asset_issnr	usp_lrel_asset_issnr	lrel_asset_issnr
usp_lrel_att_cntlist_macro_ntf	usp_lrel_att_cntlist_macro_ntf	lrel_att_cntlist_macro_ntf
usp_lrel_att_ctplist_macro_ntf	usp_lrel_att_ctplist_macro_ntf	lrel_att_ctplist_macro_ntf
usp_lrel_att_ntflist_macro_ntf	usp_lrel_att_ntflist_macro_ntf	lrel_att_ntflist_macro_ntf
usp_lrel_attachments_changes	usp_lrel_attachments_changes	lrel_attachments_changes
usp_lrel_attachments_issues	usp_lrel_attachments_issues	lrel_attachments_issues
usp_lrel_attachments_requests	usp_lrel_attachments_requests	lrel_attachments_requests
usp_lrel_aty_events	usp_lrel_aty_events	lrel_aty_events
usp_lrel_bm_reps_assets	usp_lrel_bm_reps_assets	lrel_bm_reps_assets
usp_lrel_bm_reps_bmhiers	usp_lrel_bm_reps_bmhiers	lrel_bm_reps_bmhiers
usp_lrel_cenv_cntref	usp_lrel_cenv_cntref	lrel_cenv_cntref
usp_lrel_false_action_act_f	usp_lrel_false_action_act_f	lrel_false_action_act_f
usp_lrel_dist_cntlist_mgs_ntf	usp_lrel_dist_cntlist_mgs_ntf	lrel_dist_cntlist_mgs_ntf
usp_lrel_dist_ctplist_mgs_ntf	usp_lrel_dist_ctplist_mgs_ntf	lrel_dist_ctplist_mgs_ntf
usp_lrel_dist_ntflist_mgs_ntf	usp_lrel_dist_ntflist_mgs_ntf	lrel_dist_ntflist_mgs_ntf
usp_lrel_false_bhv_false	usp_lrel_false_bhv_false	lrel_false_bhv_false
usp_lrel_kwrds_crsolref	usp_lrel_kwrds_crsolref	lrel_kwrds_crsolref
usp_lrel_notify_list_cntchgntf	usp_lrel_notify_list_cntchgntf	lrel_notify_list_cntchgntf
usp_lrel_notify_list_cntissntf	usp_lrel_notify_list_cntissntf	lrel_notify_list_cntissntf
usp_lrel_notify_list_cntntf	usp_lrel_notify_list_cntntf	lrel_notify_list_cntntf

Table	SQL Name (AKA)	Object
usp_lrel_ntfr_cntlist_att_ntfrlist	usp_lrel_ntfr_cntl_att_ntfrl	lrel_ntfr_cntlist_att_ntfrlist
usp_lrel_ntfr_ctplist_att_ntfrlist	usp_lrel_ntfr_ctplist_att_ntfrl	lrel_ntfr_ctplist_att_ntfrlist
usp_lrel_ntfr_macrolist_att_ntfrl	usp_lrel_ntfr_macrolist_att_ntfrl	lrel_ntfr_macrolist_att_ntfrl
usp_lrel_ntfr_ntflist_att_ntfrlist	usp_lrel_ntfr_ntflist_att_ntfrl	lrel_ntfr_ntflist_att_ntfrlist
usp_lrel_oenv_orgref	usp_lrel_oenv_orgref	lrel_oenv_orgref
usp_lrel_status_codes_tsktypes	usp_lrel_status_codes_tsktypes	lrel_status_codes_tsktypes
usp_lrel_svc_grps_svc_chgcat	usp_lrel_svc_grps_svc_chgcat	lrel_svc_grps_svc_chgcat
usp_lrel_svc_grps_svc_isscat	usp_lrel_svc_grps_svc_isscat	lrel_svc_grps_svc_isscat
usp_lrel_svc_grps_svc_pcat	usp_lrel_svc_grps_svc_pcat	lrel_svc_grps_svc_pcat
usp_lrel_svc_grps_svc_wftpl	usp_lrel_svc_grps_svc_wftpl	lrel_svc_grps_svc_wftpl
usp_lrel_svc_locs_svc_chgcat	usp_lrel_svc_locs_svc_chgcat	lrel_svc_locs_svc_chgcat
usp_lrel_svc_locs_svc_groups	usp_lrel_svc_locs_svc_groups	lrel_svc_locs_svc_groups
usp_lrel_svc_locs_svc_isscat	usp_lrel_svc_locs_svc_isscat	lrel_svc_locs_svc_isscat
usp_lrel_svc_locs_svc_pcat	usp_lrel_svc_locs_svc_pcat	lrel_svc_locs_svc_pcat
usp_lrel_svc_schedules_chgcat_svc	usp_lrel_svc_sch_chgcat_svc	lrel_svc_schedules_chgcat_svc
usp_lrel_svc_schedules_isscat_svc	usp_lrel_svc_sch_isscat_svc	lrel_svc_schedules_isscat_svc
usp_lrel_svc_schedules_pcat_svc	usp_lrel_svc_sch_pcat_svc	lrel_svc_schedules_pcat_svc
usp_lrel_true_action_act_t	usp_lrel_true_action_act_t	lrel_true_action_act_t
usp_lrel_true_bhv_true	usp_lrel_true_bhv_true	lrel_true_bhv_true
usp_kpi_ticket_data	usp_kpi_ticket_data	ktd
usp_organization	usp_organization	org
usp_owned_resource	usp_owned_resource	nr
usp_pri_cal	usp_pri_cal	
USP_PREFERENCES	USP_PREFERENCES	USP_PREFERENCES
USP_PROPERTIES	USP_PROPERTIES	USP_PROPERTIES
Workflow_Task	wf	wf
Workflow_Task_Template	wftpl	wftpl
wspcol	wspcol	wspcol
wsptbl	wsptbl	wsptbl
Request_Workflow_Task	crwf	cr_wf

SQL Name to Table and Object

This table provides a cross-reference of the SQL name of each table in the database schema to its corresponding table and object names:

SQL Name (AKA)	Table	Object
acc_lvls	Access_Levels	acc_lvls

SQL Name (AKA)	Table	Object
acctyp_v2	Access_Type_v2	acctyp
act_log	Act_Log	alg
act_type	Act_Type	aty
actbool	Active_Boolean_Table	actbool
actrbool	Active_Reverse_Boolean_Table	actrbool
admin_tree	admin_tree	ADMIN_TREE
am_map	Am_Asset_Map	am_asset_map
anima	Animator	ANI
arcpur_hist	Archive_Purge_History	arcpur_hist
arcpur_rule	Archive_Purge_Rule	arcpur_rule
atn	Attribute_Name	
atomic_cond	Atomic_Condition	atomic_cond
att_evt	Attached_Events	atev
attached_sla	Attached_SLA	attached_sla
attmnt	Attachment	attmnt
attmnt_folder	attmnt_folder	attmnt_folder
atyp_asc	Act_Type_Assoc	act_type_assoc
audit_log	Audit_Log	audlog
bhvtpl	Behavior_Template	bhvtpl
bool_tab	Boolean_Table	bool
bpwshft	Bop_Workshift	wrkshft
BU_TRANS	BU_TRANS	BU_TRANS
buscls	Business_Management_Class	bmcls
busmgt	Business_Management	bmhier
busrep	Business_Management_Repository	bmrep
busstat	Business_Management_Status	bms
ca_asset_type	ca_asset_type	
ca_company	ca_company	ca_cmpny
ca_company_type	ca_company_type	vpt
ca_contact	ca_contact	cnt
ca_contact_type	ca_contact_type	ctp
ca_country	ca_country	country
ca_job_function	ca_job_function	job_func
ca_job_title	ca_job_title	position
ca_location	ca_location	loc
ca_model_def	ca_model_def	mfrmod

SQL Name (AKA)	Table	Object
ca_organization	ca_organization	org
ca_owned_resource	ca_owned_resource	nr
ca_resource_class	ca_resource_class	grc
ca_resource_cost_center	ca_resource_cost_center	cost_cntr
ca_resource_department	ca_resource_department	dept
ca_resource_family	ca_resource_family	nrf
ca_resource_gl_code	ca_resource_gl_code	gl_code
ca_resource_operating_system	ca_resource_operating_system	opsys
ca_resource_status	ca_resource_status	rss
ca_schema_info	ca_schema_info	
ca_site	ca_site	site
ca_state_province	ca_state_province	state
ca_tenant	ca_tenant	tenant
ca_tenant_group	ca_tenant_group	tenant_group
ca_tenant_group_member	ca_tenant_group_member	tenant_group_member
call_req	Call_Req	cr
chg	Change_Request	chg
chg_template	Chg_Template	chg_tpl
chgalg	Change_Act_Log	chgalg
chgcat	Change_Category	chgcat
chgstat	Change_Status	chgstat
CI_ACTIONS	CI_ACTIONS	CI_ACTIONS
CI_ACTIONS_ALTERNATE	CI_ACTIONS_ALTERNATE	CI_ACTIONS_ALTERNATE
CI_BOOKMARKS	CI_BOOKMARKS	CI_BOOKMARKS
CI_DOC_LINKS	CI_DOC_LINKS	CI_DOC_LINKS
CI_DOC_TEMPLATES	CI_DOC_TEMPLATES	CI_DOC_TEMPLATES
CI_DOC_TYPES	CI_DOC_TYPES	CI_DOC_TYPES
CI_PRIORITIES	CI_PRIORITIES	CI_PRIORITIES
CI_STATUSES	CI_STATUSES	CI_STATUSES
CI_WF_TEMPLATES	CI_WF_TEMPLATES	CI_WF_TEMPLATES
cn	Column_Name	
cnote	Note_Board	cnote
cr_prp	Req_Property	cr_prp
cr_prptpl	Req_Property_Template	cr_prptpl
cr_stat	Cr_Status	crs
cr_template	Cr_Template	cr_tpl

SQL Name (AKA)	Table	Object
crctmr	Cr_Call_Timers	ctimer
crsol	Call_Solution	crsol
crsq	Cr_Stored_Queries	crsq
crt	Call_Req_Type	crt
ct_mth	Contact_Method	cmth
ctab	Controlled_Table	ctab
D_PAINTER	D_PAINTER	
dcon	Domain_Constraint	dcon
dcon_typ	Domain_Constraint_Type	dcon_typ
dlgtsrv	Delegation_Server	dlgsrvr
dmn	Domain	dmn
doc_rep	Document_Repository	doc_rep
EBR_ACRONYMS	EBR_ACRONYMS	EBR_ACRONYMS
EBR_FULLTEXT	EBR_FULLTEXT	EBR_FULLTEXT
EBR_FULLTEXT_ADM	EBR_FULLTEXT_ADM	EBR_FULLTEXT_ADM
EBR_FULLTEXT_SD	EBR_FULLTEXT_SD	EBR_FULLTEXT_SD
EBR_FULLTEXT_SD_ADM	EBR_FULLTEXT_SD_ADM	EBR_FULLTEXT_SD_ADM
EBR_INDEXING_QUEUE	EBR_INDEXING_QUEUE	EBR_INDEXING_QUEUE
EBR_KEYWORDS	EBR_KEYWORDS	EBR_KEYWORDS
EBR_LOG	EBR_LOG	EBR_LOG
EBR_METRICS	EBR_METRICS	EBR_METRICS
EBR_NOISE_WORDS	EBR_NOISE_WORDS	EBR_NOISE_WORDS
EBR_PATTERNS	EBR_PATTERNS	EBR_PATTERNS
EBR_PREFIXES	EBR_PREFIXES	EBR_PREFIXES
EBR_PROPERTIES	EBR_PROPERTIES	EBR_PROPERTIES
EBR_SUBSTITS	EBR_SUBSTITS	EBR_SUBSTITS
EBR_SUFFIXES	EBR_SUFFIXES	EBR_SUFFIXES
EBR_SYNONYMS	EBR_SYNONYMS	EBR_SYNONYMS
EBR_SYNONYMS_ADM	EBR_SYNONYMS_ADM	EBR_SYNONYMS_ADM
ES_CONSTANTS	ES_CONSTANTS	ES_CONSTANTS
ES_NODES	ES_NODES	ES_NODES
ES_RESPONSES	ES_RESPONSES	ES_RESPONSES
ES_SESSIONS	ES_SESSIONS	ES_SESSIONS
event_log	event_log	event_log
event_type	event_type	event_type
evt	Events	evt

SQL Name (AKA)	Table	Object
evt_dly	Event_Delay	evtdly
evtdlytp	Event_Delay_Type	evtdlytp
ext_appl	ext_appl	
frmgrp	Form_Group	fmgrp
g_chg_ext	Global_Change_Extension	g_chg_ext
g_chg_queue	Global_Change_Queue	g_chg_queue
g_contact	Global_Contact	g_cnt
g_iss_ext	Global_Issue_Extension	g_iss_ext
g_iss_queue	Global_Issue_Queue	g_iss_queue
g_loc	Global_Location	g_loc
g_org	Global_Organization	g_org
g_product	Global_Product	g_prod
g_queue_names	Global_Queue_Names	g_qname
g_req_ext	Global_Request_Extension	g_cr_ext
g_req_queue	Global_Request_Queue	g_cr_queue
g_srvr	Global_Servers	g_srvrs
g_tbl_map	Global_Table_Map	g_tblmap
g_tbl_rule	Global_Table_Rule	g_tblrule
grpmem	Group_Member	grpmem
hier	Asset_Assignment	hier
impact	Impact	imp
INDEX_DOC_LINKS	INDEX_DOC_LINKS	INDEX_DOC_LINKS
interface	Interface	intfc
iss_template	Iss_Template	iss_tpl
issalg	Issue_Act_Log	issalg
isscat	Issue_Category	isscat
issprp	Issue_Property	iss_prp
issstat	Issue_Status	issstat
issue	Issue	iss
isswf	Issue_Workflow_Task	iss_wf
kc	Key_Control	
KD_ATTMNT	KD_ATTMNT	KD_ATTMNT
kdlinks	kdlinks	kdlinks
km_kword	Knowledge_Keywords	kwrd
KT_REPORT_CARD	KT_REPORT_CARD	KT_REPORT_CARD
LONG_TEXTS	LONG_TEXTS	LONG_TEXTS

SQL Name (AKA)	Table	Object
managed_survey	Managed_Survey	mgs
mgsalg	Mgs_Act_Log	mgsalg
mgsstat	Mgs_Status	mgsstat
not_log	Notify_Log_Header	lr
not_que	Queued_Notify	notque
NOTIFICATION	NOTIFICATION	NOTIFICATION
nottrn	Transition_Points	
noturg	Notification_Urgency	noturg
nr_com	NR_Comment	nr_com
ntfl	Notify_Object_Attr	ntfl
O_COMMENTS	O_COMMENTS	O_COMMENTS
O_EVENTS	O_EVENTS	O_EVENTS
O_INDEXES	O_INDEXES	KCAT
object_promotion	Object_Promotion	object_promotion
options	Options	options
P_GROUPS	P_GROUPS	P_GROUPS
pcat_loc	Pcat_Loc	pcat_loc
perscon	Person_Contacting	perscnt
pri	Priority	pri
promo_hist	Promo_Hist	promo_hist
prob_ctg	Prob_Category	pcat
product	Product	prod
prp	Property	prp
prptpl	Property_Template	prptpl
quick_tpl_types	Quick_Template_Types	quick_tpl_types
rbooltab	Reverse_Boolean_Table	rev_bool
rem_ref	Remote_Ref	rrf
repmeth	Reporting_Method	rptmeth
response	Response	response
rootcause	Rootcause	rc
rptmth	Rpt_Meth	rptm
sapolicy	SA_Policy	sapolicy
saprobtyp	SA_Prob_Type	saprobtyp
sdsc_map	SLA_Contract_Map	sdsc_map
seqctl	Sequence_Control	seq
session_log	session_log	session_log

SQL Name (AKA)	Table	Object
session_type	session_type	session_type
sevrty	Severity	sev
SHOW_OBJ	SHOW_OBJ	SHOW_OBJ
SKELETONS	SKELETONS	KD
slatpl	SLA_Template	slatpl
splmac	Spell_Macro	macro
splmactp	Spell_Macro_Type	macro_type
sql_tab	SQL_Script	
srv_desc	Service_Desc	sdsc
srvr_aliases	Server_Aliases	srvr_aliases
srvr_zones	Server_Zones	srvr_zones
survey	Survey	survey
survey_answer	Survey_Answer	svy_ans
survey_atpl	Survey_Answer_Template	svy_atpl
survey_qtpl	Survey_Question_Template	svy_qtpl
survey_question	Survey_Question	svy_ques
survey_statistics	Survey_Stats	svystat
survey_tpl	Survey_Template	svy_tpl
survey_tracking	Survey_Tracking	svytrk
svc_contract	Service_Contract	svc_contract
tn	Table_Name	
toc	Type_Of_Contact	typecnt
tskstat	Task_Status	tskstat
tskty	Task_Type	tskty
tspan	Timespan	tspan
tz	Timezone	tz
urgncy	Urgency	urg
usp_caextwf_instances	usp_caextwf_instances	caextwf_inst
usp_caextwf_start_forms	usp_caextwf_start_forms	caextwf_sfrm
usp_ci_window	usp_ci_window	ci_window
usp_contact	usp_contact	cnt
usp_functional_access	usp_functional_access	func_access
usp_functional_access_level	usp_functional_access_level	func_access_level
usp_functional_access_role	usp_functional_access_role	func_access_role
usp_functional_access_type	usp_functional_access_type	func_access_type
usp_kpi	usp_kpi	kc

SQL Name (AKA)	Table	Object
usp_kpi_data	usp_kpi_data	kcd
usp_kpi_ticket_data	usp_kpi_ticket_data	ktd
usp_lrel_asset_chgnr	usp_lrel_asset_chgnr	lrel_asset_chgnr
usp_lrel_asset_issnr	usp_lrel_asset_issnr	lrel_asset_issnr
usp_lrel_att_cntlist_macro_ntf	usp_lrel_att_cntlist_macro_ntf	lrel_att_cntlist_macro_ntf
usp_lrel_att_ctplist_macro_ntf	usp_lrel_att_ctplist_macro_ntf	lrel_att_ctplist_macro_ntf
usp_lrel_att_ntflist_macro_ntf	usp_lrel_att_ntflist_macro_ntf	lrel_att_ntflist_macro_ntf
usp_lrel_attachments_changes	usp_lrel_attachments_changes	lrel_attachments_changes
usp_lrel_attachments_issues	usp_lrel_attachments_issues	lrel_attachments_issues
usp_lrel_attachments_requests	usp_lrel_attachments_requests	lrel_attachments_requests
usp_lrel_aty_events	usp_lrel_aty_events	lrel_aty_events
usp_lrel_bm_reps_assets	usp_lrel_bm_reps_assets	lrel_bm_reps_assets
usp_lrel_bm_reps_bmhiers	usp_lrel_bm_reps_bmhiers	lrel_bm_reps_bmhiers
usp_lrel_cenv_cntref	usp_lrel_cenv_cntref	lrel_cenv_cntref
usp_lrel_false_action_act_f	usp_lrel_false_action_act_f	lrel_false_action_act_f
usp_lrel_dist_cntlist_mgs_ntf	usp_lrel_dist_cntlist_mgs_ntf	lrel_dist_cntlist_mgs_ntf
usp_lrel_dist_ctplist_mgs_ntf	usp_lrel_dist_ctplist_mgs_ntf	lrel_dist_ctplist_mgs_ntf
usp_lrel_dist_ntflist_mgs_ntf	usp_lrel_dist_ntflist_mgs_ntf	lrel_dist_ntflist_mgs_ntf
usp_lrel_false_bhv_false	usp_lrel_false_bhv_false	lrel_false_bhv_false
usp_lrel_kwrds_crsolref	usp_lrel_kwrds_crsolref	lrel_kwrds_crsolref
usp_lrel_notify_list_cntchgntf	usp_lrel_notify_list_cntchgntf	lrel_notify_list_cntchgntf
usp_lrel_notify_list_cntissntf	usp_lrel_notify_list_cntissntf	lrel_notify_list_cntissntf
usp_lrel_notify_list_cntntf	usp_lrel_notify_list_cntntf	lrel_notify_list_cntntf
usp_lrel_ntfr_cntlist_att_ntfrl	usp_lrel_ntfr_cntlist_att_ntfrlist	lrel_ntfr_cntlist_att_ntfrlist
usp_lrel_ntfr_ctplist_att_ntfrl	usp_lrel_ntfr_ctplist_att_ntfrlist	lrel_ntfr_ctplist_att_ntfrlist
usp_lrel_ntfr_macrolist_att_ntfrl	usp_lrel_ntfr_macrolist_att_ntfrlist	lrel_ntfr_macrolist_att_ntfrl
usp_lrel_ntfr_ntflist_att_ntfrl	usp_lrel_ntfr_ntflist_att_ntfrlist	lrel_ntfr_ntflist_att_ntfrlist
usp_lrel_oenv_orgref	usp_lrel_oenv_orgref	lrel_oenv_orgref
usp_lrel_status_codes_tsktypes	usp_lrel_status_codes_tsktypes	lrel_status_codes_tsktypes
usp_lrel_svc_grps_svc_chgcat	usp_lrel_svc_grps_svc_chgcat	lrel_svc_grps_svc_chgcat
usp_lrel_svc_grps_svc_isscat	usp_lrel_svc_grps_svc_isscat	lrel_svc_grps_svc_isscat
usp_lrel_svc_grps_svc_pcat	usp_lrel_svc_grps_svc_pcat	lrel_svc_grps_svc_pcat
usp_lrel_svc_grps_svc_wftpl	usp_lrel_svc_grps_svc_wftpl	lrel_svc_grps_svc_wftpl
usp_lrel_svc_locs_svc_chgcat	usp_lrel_svc_locs_svc_chgcat	lrel_svc_locs_svc_chgcat
usp_lrel_svc_locs_svc_groups	usp_lrel_svc_locs_svc_groups	lrel_svc_locs_svc_groups
usp_lrel_svc_locs_svc_isscat	usp_lrel_svc_locs_svc_isscat	lrel_svc_locs_svc_isscat

SQL Name (AKA)	Table	Object
usp_lrel_svc_locs_svc_pcat	usp_lrel_svc_locs_svc_pcat	lrel_svc_locs_svc_pcat
usp_lrel_svc_sch_chgcat_svc	usp_lrel_svc_schedules_chgcat_svc	lrel_svc_schedules_chgcat_svc
usp_lrel_svc_sch_isscat_svc	usp_lrel_svc_schedules_isscat_svc	lrel_svc_schedules_isscat_svc
usp_lrel_svc_sch_pcat_svc	usp_lrel_svc_schedules_pcat_svc	lrel_svc_schedules_pcat_svc
usp_lrel_true_action_act_t	usp_lrel_true_action_act_t	lrel_true_action_act_t
usp_lrel_true_bhv_true	usp_lrel_true_bhv_true	lrel_true_bhv_true
usp_organization	usp_organization	org
usp_pri_cal	usp_pri_cal	
usp_owned_resource	usp_owned_resource	nr
USP_PREFERENCES	USP_PREFERENCES	USP_PREFERENCES
USP_PROPERTIES	USP_PROPERTIES	USP_PROPERTIES
usq	User_Query	usq
wf	Workflow_Task	wf
wftpl	Workflow_Task_Template	wftpl
wspcol	wspcol	wspcol
wsptbl	wsptbl	wsptbl
xent_map	External_Entity_Map	ext_entity_map
crwf	Request_Workflow_Task	cr_wf

Object to Table and SQL Name

This table provides a cross-reference of each object to its corresponding table and SQL name in the database schema:

Object	Table	SQL Name (AKA)
acc_lvls	Access_Levels	acc_lvls
acctyp	Access_Type_v2	acctyp_v2
act_type_assoc	Act_Type_Assoc	atyp_asc
actbool	Active_Boolean_Table	actbool
actrbool	Active_Reverse_Boolean_Table	actrbool
ADMIN_TREE	admin_tree	admin_tree
alg	Act_Log	act_log
am_asset_map	Am_Asset_Map	am_map
ANI	Animator	anima
arcpur_hist	Archive_Purge_History	arcpur_hist
arcpur_rule	Archive_Purge_Rule	arcpur_rule
atev	Attached_Events	att_evt
atomic_cond	Atomic_Condition	atomic_cond

Object	Table	SQL Name (AKA)
attached_sla	Attached_SLA	attached_sla
attmnt	Attachment	attmnt
attmnt_folder	attmnt_folder	attmnt_folder
aty	Act_Type	act_type
audlog	Audit_Log	audit_log
bhvtpl	Behavior_Template	bhvtpl
bmcls	Business_Management_Class	buscls
bmhier	Business_Management	busmgt
bmrep	Business_Management_Repository	busrep
bms	Business_Management_Status	busstat
bool	Boolean_Table	bool_tab
BU_TRANS	BU_TRANS	BU_TRANS
ca_cmpny	ca_company	ca_company
caextwf_inst	usp_caextwf_instances	usp_caextwf_instances
caextwf_sfrm	usp_caextwf_start_forms	usp_caextwf_start_forms
chg	Change_Request	chg
chg_tpl	Chg_Template	chg_template
chgalg	Change_Act_Log	chgalg
chgcat	Change_Category	chgcat
chgstat	Change_Status	chgstat
CI_ACTIONS	CI_ACTIONS	CI_ACTIONS
CI_ACTIONS_ALTERNATE	CI_ACTIONS_ALTERNATE	CI_ACTIONS_ALTERNATE
CI_BOOKMARKS	CI_BOOKMARKS	CI_BOOKMARKS
CI_DOC_LINKS	CI_DOC_LINKS	CI_DOC_LINKS
CI_DOC_TEMPLATES	CI_DOC_TEMPLATES	CI_DOC_TEMPLATES
CI_DOC_TYPES	CI_DOC_TYPES	CI_DOC_TYPES
CI_PRIORITIES	CI_PRIORITIES	CI_PRIORITIES
CI_STATUSES	CI_STATUSES	CI_STATUSES
CI_WF_TEMPLATES	CI_WF_TEMPLATES	CI_WF_TEMPLATES
ci_window	usp_ci_window	usp_ci_window
cmth	Contact_Method	ct_mth
cnote	Note_Board	cnote
cnt	ca_contact	ca_contact
cnt	usp_contact	usp_contact
cost_cntr	ca_resource_cost_center	ca_resource_cost_center
country	ca_country	ca_country

Object	Table	SQL Name (AKA)
cr	Call_Req	call_req
cr_prp	Req_Property	cr_prp
cr_prptpl	Req_Property_Template	cr_prptpl
cr_tpl	Cr_Template	cr_template
crs	Cr_Status	cr_stat
crsol	Call_Solution	crsol
crsq	Cr_Stored_Queries	crsq
crt	Call_Req_Type	crt
ctab	Controlled_Table	ctab
ctimer	Cr_Call_Timers	crctmr
ctp	ca_contact_type	ca_contact_type
dblocks		
dcon	Domain_Constraint	dcon
dcon_typ	Domain_Constraint_Type	dcon_typ
dept	ca_resource_department	ca_resource_department
dlgsrvr	Delegation_Server	dlgtsrv
dmn	Domain	dmn
doc_rep	Document_Repository	doc_rep
EBR_ACRONYMS	EBR_ACRONYMS	EBR_ACRONYMS
EBR_FULLTEXT	EBR_FULLTEXT	EBR_FULLTEXT
EBR_FULLTEXT_ADM	EBR_FULLTEXT_ADM	EBR_FULLTEXT_ADM
EBR_FULLTEXT_SD	EBR_FULLTEXT_SD	EBR_FULLTEXT_SD
EBR_FULLTEXT_SD_ADM	EBR_FULLTEXT_SD_ADM	EBR_FULLTEXT_SD_ADM
EBR_INDEXING_QUEUE	EBR_INDEXING_QUEUE	EBR_INDEXING_QUEUE
EBR_KEYWORDS	EBR_KEYWORDS	EBR_KEYWORDS
EBR_LOG	EBR_LOG	EBR_LOG
EBR_METRICS	EBR_METRICS	EBR_METRICS
EBR_NOISE_WORDS	EBR_NOISE_WORDS	EBR_NOISE_WORDS
EBR_PATTERNS	EBR_PATTERNS	EBR_PATTERNS
EBR_PREFIXES	EBR_PREFIXES	EBR_PREFIXES
EBR_PROPERTIES	EBR_PROPERTIES	EBR_PROPERTIES
EBR_SUBSTITS	EBR_SUBSTITS	EBR_SUBSTITS
EBR_SUFFIXES	EBR_SUFFIXES	EBR_SUFFIXES
EBR_SYNONYMS	EBR_SYNONYMS	EBR_SYNONYMS
EBR_SYNONYMS_ADM	EBR_SYNONYMS_ADM	EBR_SYNONYMS_ADM
ES_CONSTANTS	ES_CONSTANTS	ES_CONSTANTS

Object	Table	SQL Name (AKA)
ES_NODES	ES_NODES	ES_NODES
ES_RESPONSES	ES_RESPONSES	ES_RESPONSES
ES_SESSIONS	ES_SESSIONS	ES_SESSIONS
event_log	event_log	event_log
event_type	event_type	event_type
evt	Events	evt
evtdly	Event_Delay	evt_dly
evtdlytp	Event_Delay_Type	evtdlytp
ext_entity_map	External_Entity_Map	xent_map
fmgrp	Form_Group	frmgrp
func_access	usp_functional_access	usp_functional_access
func_access_level	usp_functional_access_level	usp_functional_access_level
func_access_role	usp_functional_access_role	usp_functional_access_role
func_access_type	usp_functional_access_type	usp_functional_access_type
g_chg_ext	Global_Change_Extension	g_chg_ext
g_chg_queue	Global_Change_Queue	g_chg_queue
g_cnt	Global_Contact	g_contact
g_cr_ext	Global_Request_Extension	g_req_ext
g_cr_queue	Global_Request_Queue	g_req_queue
g_iss_ext	Global_Issue_Extension	g_iss_ext
g_iss_queue	Global_Issue_Queue	g_iss_queue
g_loc	Global_Location	g_loc
g_org	Global_Organization	g_org
g_prod	Global_Product	g_product
g_qname	Global_Queue_Names	g_queue_names
g_srvrs	Global_Servers	g_srvr
g_tblmap	Global_Table_Map	g_tbl_map
g_tblrule	Global_Table_Rule	g_tbl_rule
gl_code	ca_resource_gl_code	ca_resource_gl_code
grc	ca_resource_class	ca_resource_class
grpmem	Group_Member	grpmem
hier	Asset_Assignment	hier
imp	Impact	impact
INDEX_DOC_LINKS	INDEX_DOC_LINKS	INDEX_DOC_LINKS
intfc	Interface	interface
iss	Issue	issue

Object	Table	SQL Name (AKA)
iss_prp	Issue_Property	issprp
iss_tpl	Iss_Template	iss_template
iss_wf	Issue_Workflow_Task	isswf
issalg	Issue_Act_Log	issalg
isscat	Issue_Category	isscat
issstat	Issue_Status	issstat
job_func	ca_job_function	ca_job_function
kc	usp_kpi	usp_kpi
KCAT	O_INDEXES	O_INDEXES
kcd	usp_kpi_data	usp_kpi_data
KD	SKELETONS	SKELETONS
KD_ATTMNT	KD_ATTMNT	KD_ATTMNT
kdlinks	kdlinks	kdlinks
KT_REPORT_CARD	KT_REPORT_CARD	KT_REPORT_CARD
ktd	usp_kpi_ticket_data	usp_kpi_ticket_data
kwrd	Knowledge_Keywords	km_kword
loc	ca_location	ca_location
LONG_TEXTS	LONG_TEXTS	LONG_TEXTS
lr	Notify_Log_Header	not_log
lrel_asset_chgnr	usp_lrel_asset_chgnr	usp_lrel_asset_chgnr
lrel_asset_issnr	usp_lrel_asset_issnr	usp_lrel_asset_issnr
lrel_att_cntlist_macro_ntf	usp_lrel_att_cntlist_macro_ntf	usp_lrel_att_cntlist_macro_ntf
lrel_att_ctplist_macro_ntf	usp_lrel_att_ctplist_macro_ntf	usp_lrel_att_ctplist_macro_ntf
lrel_att_ntflist_macro_ntf	usp_lrel_att_ntflist_macro_ntf	usp_lrel_att_ntflist_macro_ntf
lrel_attachments_changes	usp_lrel_attachments_changes	usp_lrel_attachments_changes
lrel_attachments_issues	usp_lrel_attachments_issues	usp_lrel_attachments_issues
lrel_attachments_requests	usp_lrel_attachments_requests	usp_lrel_attachments_requests
lrel_aty_events	usp_lrel_aty_events	usp_lrel_aty_events
lrel_bm_reps_assets	usp_lrel_bm_reps_assets	usp_lrel_bm_reps_assets
lrel_bm_reps_bmhiers	usp_lrel_bm_reps_bmhiers	usp_lrel_bm_reps_bmhiers
lrel_cenv_cntref	usp_lrel_cenv_cntref	usp_lrel_cenv_cntref
lrel_dist_cntlist_mgs_ntf	usp_lrel_dist_cntlist_mgs_ntf	usp_lrel_dist_cntlist_mgs_ntf
lrel_dist_ctplist_mgs_ntf	usp_lrel_dist_ctplist_mgs_ntf	usp_lrel_dist_ctplist_mgs_ntf
lrel_dist_ntflist_mgs_ntf	usp_lrel_dist_ntflist_mgs_ntf	usp_lrel_dist_ntflist_mgs_ntf
lrel_false_action_act_f	usp_lrel_false_action_act_f	usp_lrel_false_action_act_f
lrel_false_bhv_false	usp_lrel_false_bhv_false	usp_lrel_false_bhv_false

Object	Table	SQL Name (AKA)
lrel_kwrds_crsolref	usp_lrel_kwrds_crsolref	usp_lrel_kwrds_crsolref
lrel_notify_list_cntchgntf	usp_lrel_notify_list_cntchgntf	usp_lrel_notify_list_cntchgntf
lrel_notify_list_cntissntf	usp_lrel_notify_list_cntissntf	usp_lrel_notify_list_cntissntf
lrel_notify_list_cntntf	usp_lrel_notify_list_cntntf	usp_lrel_notify_list_cntntf
lrel_ntfr_cntlist_att_ntfrlist	usp_lrel_ntfr_cntlist_att_ntfrlist	usp_lrel_ntfr_cntlist_att_ntfrl
lrel_ntfr_ctplist_att_ntfrlist	usp_lrel_ntfr_ctplist_att_ntfrlist	usp_lrel_ntfr_ctplist_att_ntfrl
lrel_ntfr_macrolist_att_ntfrl	usp_lrel_ntfr_macrolist_att_ntfrl	usp_lrel_ntfr_macrolist_att_ntfrl
lrel_ntfr_ntflist_att_ntfrlist	usp_lrel_ntfr_ntflist_att_ntfrlist	usp_lrel_ntfr_ntflist_att_ntfrl
lrel_oenv_orgref	usp_lrel_oenv_orgref	usp_lrel_oenv_orgref
lrel_status_codes_tsktypes	usp_lrel_status_codes_tsktypes	usp_lrel_status_codes_tsktypes
lrel_svc_grps_svc_chgcat	usp_lrel_svc_grps_svc_chgcat	usp_lrel_svc_grps_svc_chgcat
lrel_svc_grps_svc_isscat	usp_lrel_svc_grps_svc_isscat	usp_lrel_svc_grps_svc_isscat
lrel_svc_grps_svc_pcat	usp_lrel_svc_grps_svc_pcat	usp_lrel_svc_grps_svc_pcat
lrel_svc_grps_svc_wftpl	usp_lrel_svc_grps_svc_wftpl	usp_lrel_svc_grps_svc_wftpl
lrel_svc_locs_svc_chgcat	usp_lrel_svc_locs_svc_chgcat	usp_lrel_svc_locs_svc_chgcat
lrel_svc_locs_svc_groups	usp_lrel_svc_locs_svc_groups	usp_lrel_svc_locs_svc_groups
lrel_svc_locs_svc_isscat	usp_lrel_svc_locs_svc_isscat	usp_lrel_svc_locs_svc_isscat
lrel_svc_locs_svc_pcat	usp_lrel_svc_locs_svc_pcat	usp_lrel_svc_locs_svc_pcat
lrel_svc_schedules_chgcat_svc	usp_lrel_svc_schedules_chgcat_svc	usp_lrel_svc_sch_chgcat_svc
lrel_svc_schedules_isscat_svc	usp_lrel_svc_schedules_isscat_svc	usp_lrel_svc_sch_isscat_svc
lrel_svc_schedules_pcat_svc	usp_lrel_svc_schedules_pcat_svc	usp_lrel_svc_sch_pcat_svc
lrel_true_action_act_t	usp_lrel_true_action_act_t	usp_lrel_true_action_act_t
lrel_true_bhv_true	usp_lrel_true_bhv_true	usp_lrel_true_bhv_true
macro	Spell_Macro	splmac
macro_type	Spell_Macro_Type	splmactp
mfrmod	ca_model_def	ca_model_def
mgs	Managed_Survey	managed_survey
mgsalg	Mgs_Act_Log	mgsalg
mgsstat	Mgs_Status	mgsstat
NOTIFICATION	NOTIFICATION	NOTIFICATION
notque	Queued_Notify	not_que
noturg	Notification_Urgency	noturg
nr	ca_owned_resource	ca_owned_resource
nr	usp_owned_resource	usp_owned_resource
nr_com	NR_Comment	nr_com
nrf	ca_resource_family	ca_resource_family

Object	Table	SQL Name (AKA)
ntfl	Notify_Object_Attr	ntfl
O_COMMENTS	O_COMMENTS	O_COMMENTS
O_EVENTS	O_EVENTS	O_EVENTS
object_promotion	Object_Promotion	object_promotion
opsys	ca_resource_operating_system	ca_resource_operating_system
options	Options	options
org	ca_organization	ca_organization
org	usp_organization	usp_organization
P_GROUPS	P_GROUPS	P_GROUPS
pcat	Prob_Category	prob_ctg
pcat_loc	Pcat_Loc	pcat_loc
perscnt	Person_Contacting	perscon
position	ca_job_title	ca_job_title
pri	Priority	pri
promo_hist	Promo_Hist	promo_hist
prod	Product	product
prp	Property	prp
prptpl	Property_Template	prptpl
quick_tpl_types	Quick_Template_Types	quick_tpl_types
rc	Rootcause	rootcause
response	Response	response
rev_bool	Reverse_Boolean_Table	rbooltab
rptm	Rpt_Meth	rptmth
rptmeth	Reporting_Method	repmeth
rrf	Remote_Ref	rem_ref
rss	ca_resource_status	ca_resource_status
sapolicy	SA_Policy	sapolicy
saprobtyp	SA_Prob_Type	saprobtyp
sdsc	Service_Desc	srv_desc
sdsc_map	SLA_Contract_Map	sdsc_map
seq	Sequence_Control	seqctl
session_log	session_log	session_log
session_type	session_type	session_type
sev	Severity	sevrty
SHOW_OBJ	SHOW_OBJ	SHOW_OBJ
site	ca_site	ca_site

Object	Table	SQL Name (AKA)
slatpl	SLA_Template	slatpl
srvr_aliases	Server_Aliases	srvr_aliases
srvr_zones	Server_Zones	srvr_zones
state	ca_state_province	ca_state_province
survey	Survey	survey
svc_contract	Service_Contract	svc_contract
svy_ans	Survey_Answer	survey_answer
svy_atpl	Survey_Answer_Template	survey_atpl
svy_qtpl	Survey_Question_Template	survey_qtpl
svy_ques	Survey_Question	survey_question
svy_tpl	Survey_Template	survey_tpl
svystat	Survey_Stats	survey_statistics
svytrk	Survey_Tracking	survey_tracking
target_tgttpls_srvtypes	target_tgttpls_srvtypes	tgt_tgttpls_srvtypes
target_time	target_time	tgt_time
target_time_tpl	target_time_tpl	tgt_time_tpl
tenant	ca_tenant	ca_tenant
tenant_group	ca_tenant_group	ca_tenant_group
tenant_group_member	ca_tenant_group_member	ca_tenant_group_member
True_False_Table	True_False_Table	true_false
tskstat	Task_Status	tskstat
tskty	Task_Type	tskty
tspan	Timespan	tspan
typecnt	Type_Of_Contact	toc
tz	Timezone	tz
urg	Urgency	urgncy
USP_PREFERENCES	USP_PREFERENCES	USP_PREFERENCES
USP_PROPERTIES	USP_PROPERTIES	USP_PROPERTIES
usq	User_Query	usq
vpt	ca_company_type	ca_company_type
wf	Workflow_Task	wf
wftpl	Workflow_Task_Template	wftpl
wrkshft	Bop_Workshift	bpwshft
wspcol	wspcol	wspcol
wsptbl	wsptbl	wsptbl
	Attribute_Name	atn

Object	Table	SQL Name (AKA)
	ca_asset_type	ca_asset_type
	ca_schema_info	ca_schema_info
	Column_Name	cn
	D_PAINTER	D_PAINTER
	ext_appl	ext_appl
	Key_Control	kc
	Transition_Points	nottrn
	SQL_Script	sql_tab
	Table_Name	tn
cr_wf	Request_Workflow_Task	crwf

CA SDM Object List Table for Multi-Tenancy

The following table lists all CA SDM objects and indicates whether each object has a tenant attribute, and if so, if it is optional or required.

Note: The Rel_attr must be unique, regardless of tenant.

Object	Rel_Attr	Description	Tenancy
acc_lvls	enum	Access Level	No
acctyp	id	Access Type	No
acctyp_role	id	Access Type Role	No
act_type_assoc	code	Activity Type Association	Optional
actbool	enum	Active Boolean	No
actlog_prod_list	sym	actlog_prod_list	No
actrbool	enum	Active Reverse Boolean	No
ADMIN_TREE	id	Administration Tree	No
agt	id	Analyst contacts	Required
alg	persistent_id	Request Activity Log	Required
all_fmgrp	id	all_fmgrp	No
all_lr	persistent_id	all_lr	Required
am_asset_map	persistent_id	AM Asset Map	No
ANI	persistent_id	Animator	Optional

Object	Rel_Attr	Description	Tenancy
api	persistent_id	api	No
app_extx	id	app_extx	Optional
app_inhx	id	app_inhx	Optional
arcpur_hist	persistent_id	Archive Purge History	No
arcpur_rule	persistent_id	Archive Purge Rule	No
arg_history	persistent_id	arg_history	No
asset	id	asset	No
assetx_prod_list	sym	assetx_prod_list	No
atev	persistent_id	Attached Event	Required
atomic_cond	id	Atomic Condition	Optional
attached_sla	id	Attached Service Type	Required
attmnt	id	Attachment	Optional
attmnt_folder	id	Attachments Folder	Optional
attmnt_lrel	persistent_id	Attachment LREL	No
attr_alias	id	Attribute Alias	No
aty	code	Activity Type	Optional
audlog	persistent_id	Audit Log	Required
bhvtpl	id	Behavior Template	Optional
bhvtpl_wftpl	id	bhvtpl_wftpl	Optional
bm_task	id	bm_task	Optional
bmcls	id	Business Management Class	No
bmhier	id	Business Management Hierarchy	Optional
bmlrel	persistent_id	Business Management LREL	No
bmrep	id	Business Management Repository	No
bms	status_no	Business Management Status	No
bool	enum	Boolean	No
BU_TRANS	id	Bubble Up Transaction	Optional
ca_application_registration	id	ca_application_registration	No
ca_asset	id	Asset	No
ca_asset_source	id	Asset Source	No
ca_asset_source_unrestricted	id	ca_asset_source_ unrestricted	No
ca_asset_subschema	id	Asset Subschema	No
ca_asset_type	id	Asset Type	No
ca_cmpny	id	Company	Optional

Object	Rel_Attr	Description	Tenancy
ca_logical_assst	id	Logical Asset	No
ca_logical_asset_property	id	Logical Asset Property	No
chg	id	chg	Required
chg_tpl	template_name	Change Template	Required
chgalg	id	Change Order Activity Log	Required
chgaty	code	chgaty	Optional
chgcat	code	Change Category	Optional
chgcat_grp	persistent_id	Change Category Group LREL	No
chgcat_loc	persistent_id	Change Category Location LREL	No
chgcat_workshift	persistent_id	Change Category Workshift LREL	No
chgstat	code	Change Status	Optional
chgtype	id	Change Type	No
CI_ACTIONS	id	Knowledge Workflow Task	Optional
CI_ACTIONS_ALTERNATE	id	Alternate Knowledge Workflow Task	Optional
CI_BOOKMARKS	id	Knowledge Document Bookmark	Optional
CI_DOC_LINKS	id	Knowledge Document Link	Optional
CI_DOC_TEMPLATES	id	Knowledge Document Template	Optional
CI_DOC_TYPES	id	Knowledge Document Type	No
ci_mdr_idmap	id	ci_mdr_idmap	Optional
ci_mdr_provider	id	ci_mdr_provider	Optional
CI_PRIORITIES	id	Approval Process Template	Optional
ci_rel_type	id	ci_rel_type	No
CI_STATUSES	id	Knowledge Status	No
CI_WF_TEMPLATES	id	Knowledge Workflow Template	No
cmth	id	Contact Method	No
cnote	persistent_id	Announcement	Optional
cnt	id	Contact	Required
cnt_role	id	Contact Role	Required
cntx	id	cntx	Optional
conx	id	conx	Optional
cost_cntr	id	Cost Center	Optional
country	id	Country	No
cr	persistent_id	Request	

Object	Rel_Attr	Description	Tenancy
			Required
cr_prp	id	Request Property	Required
cr_prptpl	id	Request Property Template	Optional
cr_tpl	template_name	Request Template	Required
craty	code	craty	Optional
crs	code	Request Status	Optional
crs_cr	code	crs_cr	Optional
crs_in	code	crs_in	Optional
crs_pr	code	crs_pr	Optional
crsol	persistent_id	Request Solution	No
crsq	code	Stored Query	Optional
crt	code	Request Type	No
cst	id	Customer contacts	Required
ctab	id	Controlled Table	No
ctimer	persistent_id	Request Timer	No
ctp	id	Contact Type	No
dat_basx	id	dat_basx	Optional
dcon	id	Data Partition Constraint	No
dcon_typ	enum	Data Partition Constraint Type	No
dept	id	Department	Optional
dlgsrvr	id	Delegation Server	No
dmn	id	Data Partition	No
doc_rep	persistent_id	Attachments Repository	Optional
DOC_VERSIONS	id	Document Version	Optional
docx	id	docx	Optional
EBR_ACRONYMS	id	EBR Acronym	No
EBR_DICTIONARY	id	EBR Dictionary	No
EBR_DICTIONARY_ADM	id	EBR Dictionary Alternate	No
EBR_FULLTEXT	id	EBR Knowledge Document Index	No
EBR_FULLTEXT_ADM	id	EBR Knowledge Document Index Alternate	No
EBR_KS	id	Knowledge Source	No
EBR_KS_ACCESS	id	Knowledge Source Access	No
EBR_KS_INDEXING_QUEUE	id	Knowledge Source Indexing Queue	No

Object	Rel_Attr	Description	Tenancy
EBR_LOG	id	EBR Log	No
EBR_METRICS	id	EBR Metric	No
EBR_NOISE_WORDS	id	EBR Noise Word	No
EBR_PATTERNS	id	EBR Pattern	No
EBR_PREFIXES	id	EBR Prefix	No
EBR_PROPERTIES	id	EBR Property	No
EBR_SUBSTITS	id	EBR Substitution	No
EBR_SUFFIXES	id	EBR Suffix	No
EBR_SYNONYMS	id	EBR Synonym	No
EBR_SYNONYMS_ADM	id	EBR Synonyms Alternate	No
edit_macros	persistent_id	edit_macros	No
entservx	id	entservx	Optional
enttx	id	enttx	Optional
ES_CONSTANTS	id	ES_CONSTANTS	No
ES_NODES	id	Decision Tree Node	Optional
ES_RESPONSES	id	ES_RESPONSES	Optional
ES_SESSIONS	id	ES_SESSIONS	Optional
event_log	id	Event Log	No
event_prod_list	sym	event_prod_list	No
event_type	id	Event Type	No
evt	persistent_id	Event	Optional
evtdly	persistent_id	Event Delay	Optional
evtdlytp	enum	Event Delay Type	No
ext_entity_map	persistent_id	External Entity Map	No
fac_acx	id	fac_acx	Optional
fac_firex	id	fac_firex	Optional
fac_furnx	id	fac_furnx	Optional
fac_othx	id	fac_othx	Optional
fac_upsx	id	fac_upsx	Optional
fmgrp	id	Form Group	No
g_chg_ext	id	Global Change Extension	Required
g_chg_queue	id	Global Change Queue	No
g_cnt	id	Global Contact	No
g_cr_ext	id	Global Request Extension	Required
g_cr_queue	id	Global Request Queue	No

Object	Rel_Attr	Description	Tenancy
g_iss_ext	id	Global Issue Extension	Required
g_iss_queue	id	Global Issue Queue	No
g_loc	id	g_loc	No
g_org	id	Global Organization	No
g_prod	id	Global Product	No
g_qname	id	Global Queue	No
g_srvrs	remote_sys_id	Global Server	No
g_tblmap	id	Global Table Map	No
g_tblrule	id	Global Table Rule	No
g_tenant	id	Global Tenant	No
gl_code	id	Resource Code	No
grc	id	Resource Class	No
grp	id	Group Contacts	Required
grpmem	persistent_id	Group Member	Required
har_lparx	id	har_lparx	Optional
har_maix	id	har_maix	Optional
har_monx	id	har_monx	Optional
har_othx	id	har_othx	Optional
har_prix	id	har_prix	Optional
har_serx	id	har_serx	Optional
har_stox	id	har_stox	Optional
har_virx	id	har_virx	Optional
har_worx	id	har_worx	Optional
help_content	name	help_content	No
help_item	id	help_item	No
help_lookup	id	help_lookup	No
help_set	id	help_set	No
hier	id	Asset Relation	Optional
ical_alarm	id	iCalendar Alarm	No
ical_event_prod_list	sym	ical_event_prod_list	No
ical_event_template	id	iCalendar Event	No
imp	enum	Impact	No
in	persistent_id	Incident	Required
INDEX_DOC_LINKS	id	Knowledge Category-Document Link	Optional

interface_type	id	interface_type	No
intfc	id	interface	No
invidex	id	invidex	Optional
invothx	id	invothx	Optional
invprjx	id	invprjx	Optional
iss	persistent_id	iss	Required
iss_prp	id	Issue Property	Required
iss_tpl	template_name	Issue Template	Required
iss_wf	id	Issue Workflow Task	Required
issalg	id	Issue Activity Log	Required
issaty	code	issaty	Optional
isscat	code	Issue Category	Optional
isscat_grp	persistent_id	Issue Category Group LREL	No
isscat_loc	persistent_id	Issue Category Location LREL	No
isscat_workshift	persistent_id	Issue Category Workshift LREL	No
issstat	code	Issue Status	Optional
job_func	id	Job Function	Optional
kc	id	KPI	Optional
KCAT	id	Knowledge Category	Optional
kcd	id	KPI Data	Optional
KD	id	Knowledge Document	Optional
KD_ALL	id	KD_ALL	Optional
KD_ATTMNT	id	Document-Attachment Link	Optional
KD_FILE	id	KD_FILE	Optional
KD_QA	id	KD_QA	Optional
KD_SAVE_AS	persistent_id	KD_SAVE_AS	No
KD_TASK	persistent_id	KD_TASK	Optional
kdaty	code	kdaty	Optional
kdlinks	persistent_id	Document-Ticket Link	Optional
KEIT_IMPORT_PACKAGES	id	Knowledge Import Packages	No
KEIT_TEMPLATES	id	Knowledge Export/Import Template	Optional
KEIT_TRANSACTION_STATUSES	id	Knowledge Transaction Statuses	No

Object	Rel_Attr	Description	Tenancy
KEIT_TRANSACTIONS	id	Knowledge Import Transactions	Optional
kmlrel	persistent_id	Knowledge LREL	No
KT_ACT_CONTENT	id	Action Content	Optional
KT_BLC	id	Recommended Document	Optional
KT_BLC_TYPE	id	KT_BLC_TYPE	No
KT_FILE_TYPE	id	File Type	No
KT_FLG_STATUS	id	Flag Status	No
KT_FLG_TYPE	id	Comment Type	Optional
KT_FREE_TEXT	persistent_id	Free Text	No
KT_KCAT_NTF	id	Category Notification	Optional
KT_LIFE_CYCLE_REP	id	KT Life Cycle Report	Optional
KT_QA_RESP_TYPE	id	Forum Response Type	No
KT_QA_STATUS	id	Forum Status	No
KT_REPORT_CARD	id	Knowledge Report Card	No
KT_STATUS_ROLE	id	Status Role	No
ktd	id	KPI Ticket Data	Required
kwrd	id	Keyword	No
ldap	id	LDAP	No
ldap_group	id	LDAP Group	No
loc	id	Location	Optional
locx	id	locx	Optional
LONG_TEXTS	id	Forum Reply	Optional
lr	persistent_id	Notification Log	Required
macro	persistent_id	Macro	Optional
macro_prod_list	sym	macro_prod_list	No
macro_type	code	Macro Type	No
menu_bar	id	Menu Bar	No
menu_tree	id	Menu Tree Node	No
menu_tree_name	id	Menu Tree	No
menu_tree_res	id	Menu Tree Resource	No
mfrmod	id	Model Definition	Optional
mgs	id	Managed Survey	Optional
mgsalg	id	Managed Survey Activity Log	Optional
mgsaty	code	mgsaty	Optional
mgsstat	code	Managed Survey Status	No

Object	Rel_Attr	Description	Tenancy
MSysConf	Config	MSysConf	No
net_brix	id	net_brix	Optional
net_clux	id	net_clux	Optional
net_conx	id	net_clux	Optional
net_frox	id	net_frox	Optional
net_gatx	id	net_gatx	Optional
net_hubx	id	net_hubx	Optional
net_nicx	id	net_nicx	Optional
net_othx	id	net_othx	Optional
net_perx	id	net_perx	Optional
net_porx	id	net_porx	Optional
net_rgrpx	id	net_rgrpx	Optional
net_roux	id	net_roux	Optional
net_rsrcx	id	net_rsrcx	Optional
no_contract_sdsc	code	no_contract_sdsc	Optional
node_prod_list	sym	node_prod_list	No
NOTIFICATION	id	Notification	Optional
notque	persistent_id	Queued Notification	No
noturg	enum	Notification Urgency	No
nr	id	Configuration Item	Optional
nr_com	id	Asset comment	Optional
nrf	id	Resource Family	No
ntfl	id	Notification Log	No
ntfm	persistent_id	Notification Message Template	Optional
ntfm_prod_list	sym	ntfm_prod_list	No
ntfr	id	Notification Rule	Optional
ntfr_prod_list	sym	ntfr_prod_list	No
O_COMMENTS	id	Knowledge Document Comment	Optional
O_EVENTS	id	Document History	Optional
OA_COLUMNS	COLUMN_NAME	OA_COLUMNS	No
OA_FKEYS	PKCOLUMN_NAME	OA_FKEYS	No
OA_INFO	INFO_NAME	OA_INFO	No
OA_STATISTICS	COLUMN_NAME	OA_STATISTICS	No
OA_TABLES	TABLE_NAME	OA_TABLES	No
OA_TYPES	TYPE_NAME	OA_TYPES	No
object_notify_prod_list	sym	object_notify_prod_list	No

Object	Rel_Attr	Description	Tenancy
opsys	id	Operating System	Optional
opsysx	id	opsysx	Optional
options	persistent_id	Option	No
org	id	Organization	Required
orgx	id	orgx	Optional
P_GROUPS	id	KT Permission Group	Optional
pcat	persistent_id	Request Area	Optional
pcat_cr	persistent_id	pcat_cr	Optional
pcat_in	persistent_id	pcat_in	Optional
pcat_loc	persistent_id	Request Area Location LREL	No
pcat_pr	persistent_id	pcat_pr	Optional
pcat_workshift	persistent_id	Request Area Workshift LREL	No
perscnt	id	Person Contacting	Optional
position	id	Position	Optional
pr	persistent_id	Problem	Required
pri	enum	Priority	No
prio_service_type	id	Priority Service Type	Required
prod	id	Product	Optional
prod_list	sym	Object Name	No
projex	id	projex_detail	Optional
prp	id	Property	Required
prptpl	id	Property Template	Optional
prptpl_chgcat	id	prptpl_chgcat	Optional
prptpl_isscat	id	prptpl_isscat	Optional
prpval	id	Property Value	No
prpval_rule	id	Property Validation Rule	No
prpval_type	id	Property Validation Type	No
QUERY_POLICY	id	Query Policy	Optional
QUERY_POLICY_ACTIONS	id	Query Policy Actions	Optional
quick_tpl_types	enum	Quick Template Type	No
rc	id	Root Cause	Optional
response	id	Personalized Response	Optional
rev_bool	enum	Reverse Boolean	No
role	id	Role	No

role_go_form	id	Role Go Form	No
role_tab	id	Role Tab	No
role_web_form	id	Role Web Form	No
rptm	persistent_id	Report Method	No
rptmeth	id	Reporting Method	No
rrf	code	Remote Reference	No
rss	id	Resource Status	No
sapolicy	id	Web Services Access Policy	Optional
saprobtyp	id	Web Services Error Type	Optional
sd_chg_map	persistent_id	sd_chg_map	No
sd_cr_map	persistent_id	sd_cr_map	No
sdsc	code	Service Type	Optional
sdsc_map	id	Service Type Map	Required
secx	id	secx	Optional
seq	id	Sequence	Optional
serx	id	serx	Optional
session_log	id	Session Log	No
session_type	id	Session Type	No
sev	enum	Severity	No
SHOW_OBJ	id	Show Object	No
site	id	Site	Optional
slatpl	id	SLA Template	Required
slax	id	slax	Optional
sqchg	code	sqchg	Optional
sqcr	code	sqcr	Optional
sqiss	code	sqiss	Optional
srvr_aliases	id	Server Alias	No
srvr_zones	id	Server Zone	No
state	id	State	No
stored_query_prod_list	sym	stored_query_prod_list	No
survey	id	Survey	Optional
svc_contract	id	Service Contract	Required
svy_ans	id	Survey Answer	Optional
svy_atpl	id	Survey Answer Template	Optional

Object	Rel_Attr	Description	Tenancy
svy_qtpl	id	Survey Question Template	Optional
svy_ques	id	Survey Question	Optional
svy_tpl	id	Survey Template	Optional
svystat	id	Survey Statistic	Optional
svytrk	id	Survey Tracking	Required
tab	id	Tab	No
tel_cirx	id	tel_cirx	Optional
tel_othx	id	tel_othx	Optional
tel_radx	id	tel_radx	Optional
tel_voix	id	tel_voix	Optional
tel_wirx	id	tel_wirx	Optional
tenant	id	Tenant	Required
tenant_group	id	Tenant Group	No
tenant_group_member	persistent_id	Tenant Group Member	Required
text_api	persistent_id	text_api	No
tgm_groups	persistent_id	Tenant Groups	Required
tgm_members	persistent_id	Tenant Group Members	Required
tkt	persistent_id	tkt	Required
tskstat	code	Task Status	Optional
tskty	code	Task Type	Optional
tspan	sym	Time Span	No
ttv_slas	id	ttv_slas	Required
typecnt	id	Reason	No
tz	code	Time Zone	No
urg	enum	Urgency	No
url	persistent_id	URL	No
USP_PREFERENCES	id	Preference	No
USP_PROPERTIES	id	Property	Optional
usp_servers	id	usp_servers	No
usq	id	User Stored Query	Optional
vis_configuration	persistent_id	vis_configuration	Optional

Object	Rel_Attr	Description	Tenancy
vis_graph_metadata	persistent_id	vis_graph_metadata	Optional
vis_object_store_criteria	persistent_id	vis_object_store_criteria	Optional
vis_object_store_master	persistent_id	vis_object_store_master	Optional
vpt	id	Company Type	No
web_form	id	Web Form	No
web_form_pref	id	Web Form Preference	Required
wf	id	Workflow Task	Required
wftpl	id	Workflow Task Template	Optional
wftpl_chgcat	id	wftpl_chgcat	Optional
wftpl_isscat	id	wftpl_isscat	Optional
workflow_prod_list	sym	workflow_prod_list	No
wrkshft	persistent_id	Workflow Template Workshift LREL	No
wspcol	id	Web Screen Painter Column	No
wspdomset	id	wspdomset	No
wsptbl	id	Web Screen Painter Table	No
cr_wf	id	Request Workflow Task	Required

CMDB Technical Reference

This article contains the following topics:

Introduction

This section is intended for implementers who perform the following configuration management database (CMDB) tasks:

- Map your data into the CMDB.
- Manage CMDB configuration items.

- Use the Advantage Data Transformer (ADT) to write a Federation Adapter.
- Use the CMDBf Web Services to interact with CMDB.

The information in this page can assist you as you plan your CMDB implementation. You can print and have the printouts handy while performing these tasks.

CI Families and Classes

Configuration item (CI) *families* categorize your business assets by type and assign meaningful attributes for each CI in the family. Families are general categories of CIs, such as hardware, software, and services CIs.

CI *classes* are specific categories within the family categories. For example, the Hardware family contains CI classes such as modem, router, repeater, and bridge.

You can organize your CIs into families and classes to make them easier to manage. For example, you can generate a list of CIs that belong to a particular family or class.

You use the following sequence to categorize your business assets:

1. Define CI families.
2. Define CI classes.
3. Define CIs.

List Configuration Item Families

You can list CMDB CI families and view their descriptions.

To list configuration item families

1. Log into CA SDM as an administrator.
   The web interface appears.
2. Click Administration.
   The Administration tree appears.
3. Navigate the folder structure by clicking CMDB, CI Families.
   The CI families and their descriptions are listed.
4. (Optional) Click a CI family name.
   CI family details appear.

Generate a Configuration Item Families Summary

You can list CMDB CI families and view their descriptions in a report format.

To list configuration item families

1. Log into CA SDM as an administrator.
   The web interface appears.

2. Click Administration.
   The Administration tree appears.

3. Navigate the folder structure by clicking CA SDM, CI Families.
   The CI families and their descriptions are listed.

4. Click Reports, Summary.
   A summary report appears in a separate window.

5. (Optional) Click Print to select a printer and print the report.
   The report prints.

MDB Extension Tables

Each CI family has a set of family-specific attributes that reside in an *extension table* in the MDB. The family-specific attributes describe the unique characteristics of each type of CI. For example, a CI in the Hardware.Server family has attributes that represent the following:

- swap_size -- The size of the disk space allocated on a hardware or network device to store the state of a process that has been swapped out.
- mem_capacity -- The total amount of memory that can be installed and made available.
- slot_total_mem -- The total amount of memory available on memory cards in a hardware or network device.

When you implement CA SDM, you can determine the types of CIs that you want to manage and the attributes that you can track for them.

Common Attributes

The following attributes are common to various families.

Object Name	Description
acquire_date	Date the resource was acquired.
alarm_id	IP address. (hardware only)
asset_count	Resource quantity.
asset_num	Alternate resource identifier, for example, an alternate ID located on sticker placed on a computer.
class	In the object, this is the name of the class. In the table, this is a foreign key to a record in the ca_resource_class table (SREL integer to grc).
company_bought_for_uuid	In the object, this is the name of the company for which the CI was bought. In the table, this is a foreign key to the ca_company table (SREL uuid to ca_cmpny).

Object Name	Description
contact_1	In the object, this is a user-defined contact field. In the table, this is a foreign key to the ca_contact table (SREL uuid to cnt).
contact_2	In the object, this is a user-defined contact field. In the table, this is a foreign key to the ca_contact table (SREL uuid to cnt).
contact_3	In the object, this is a user-defined contact field. In the table, this is a foreign key to the ca_contact table (SREL uuid to cnt).
creation_date	Timestamp (pdmtime) indicating the date and time that the CI was created.
creation_user	User ID of the contact who created the CI
delete_flag	Active|FALSE|0 (zero)|No: CI is active and displays in display lists (the default). Inactive|TRUE|1 (one)|Yes: CI is not active and does not appear in display lists.
department	In the object, this is the name of the department. In the table, this is a foreign key to the ca_resource_department table (SREL integer to dept).
description	Longer name or description of the resource.
dns_name	The name by which this device is know in the domain name server.
exclude_registration	Exclude Registration.
expense_code	In the object, this is the CI cost center. In the table, this is a foreign key to the ca_resource_cost_center table (SREL integer to cost_cntr).
expiration_date	Date the license, lease, and so on, expires.
family	In the object, this is the name of the family. In the table, this is a foreign key to a record in the ca_resource_family table (SREL integer to nrf). Used to extend at a high level, for example, hardware.server, network.router, software.database.
financial_num	Financial number.
install_date	Date resource was installed in organization or network.
is_asset	Boolean flag that can be set to categorize an Asset for filtering purposes and to control display in CA CMDB or other products such as CA Asset Portfolio Management. CA CMDB does not allow the Asset flag to be changed to NO when an asset is managed by CA Asset Portfolio Management.
is_ci	Boolean flag that can be set to categorize a CI for filtering purposes and to control display in CA CMDB or other products such as CA Asset Portfolio Management. By default, a CI created by CA CMDB is flagged as a CI but not as an Asset.
	User ID of the contact who last modified the CI

Object Name	Description
last_mod_by	
license_number	License Information.
loc_cabinet	Cabinet location.
loc_floor	Floor location.
loc_room	Room location.
loc_shelf	Shelf location.
loc_slot	Slot location.
location	In the object, this is the name of the location. In the table, this is a foreign key to a record in the location table (SREL uuid to loc).
mac_address	MAC address. (hardware only)
manufacturer	In the object, this is the name of the company who manufactured the CI. In the table, this is a foreign key to a record in the ca_company table (SREL uuid to ca_cmpny).
model	In the object, this is the model name for the CI. In the table, this is a foreign key to the ca_model_def table (SREL uuid to mfrmod).
name	The name of the resource.
name_type	Foreign key to the ca_asset_type table to represent Hardware, Software, and so on.
org_bought_for_uuid	In the object, this is the name of the organization for which the CI was bought. In the table, this is a foreign key to the ca_organization table (SREL uuid to org).
priority	Enumerated value for this entry, it specifies ordering in lists and relative values (SREL integer to pri).
product_version	Product release.
repair_org	In the object, this is the name of the organization responsible for maintenance of the CI. In the table, this is a foreign key to the ca_organization table (SREL uuid to org).
resource_alias	Resource alias.
resource_contact	In the object, this is the name of the contact responsible for the CI. In the table, this is a foreign key to the ca contact table (SREL uuid to cnt).
resource_owner_uuid	In the object, this is the name of the owner for the CI. In the table, this is a foreign key to the ca_contact table (SREL uuid to cnt).

serial_number	Serial number.
service_org	In the object, this is the name of the organization ultimately responsible for the resource. In the table, this is a foreign key to the ca_organization table (SREL uuid to org).
service_type	Noneditable enum (SREL string to no_contract_sdsc).
sla	The SLA value for this usp_owned_resource.
smag_1	User-defined string field.
smag_2	User-defined string field.
smag_3	User-defined string field.
smag_4	User-defined string field.
smag_5	User-defined string field.
smag_6	User-defined string field.
standard_ci	Standard configuration for comparison.
status	In the object, this is the status indicator for the CI. In the table, this is a foreign key to the ca_resource_status table (SREL integer to rss).
supplier	In the object, this is the name of the vendor responsible for supplying the CI. In the table, this is a foreign key to the ca_company table (SREL uuid to ca_cmpny).
system_name	Computer name. (hardware only)
tenant	Tenant assignment for the CI
vendor_repair	In the object, this is the name of the vendor providing maintenance for the CI. In the table, this is a foreign key to the ca_company table (SREL uuid to ca_cmpny).
vendor_restore	In the object, this is the name of the company ultimately responsible for the resource. In the table, this is a foreign key to the ca_company table (SREL uuid to ca_cmpny).
warranty_end	Warranty end date.
warranty_start	Warranty start date.

Relationship Types

Relationships are *directional* connections between CIs.

Provider /Dependent	Dependent /Provider	Relationship Description
administers	is administered by	A responsible entity, usually a person, performs day-to-day administration of other entities.

Provider /Dependent	Dependent /Provider	Relationship Description
approves	is approved by	A responsible entity grants approval for another entity to proceed with a planned or desired activity.
authorizes	is authorized by	A responsible entity ratifies activities of other entities.
authors	is authored by	A responsible person writes/creates document CIs.
backs up	is backed up by	For data recovery and preservation, one entity's critical information is stored upon another entity.
communicates with	communicates with	A peer-to-peer relationship where two entities which have a logical or physical connection convey data or information back and forth.
complies to	is complied to by	One entity abides by regulations (COBIT, SOX, and so on) set forth by another entity.
connects to	connects to	A peer-to-peer relationship where two entities have a logical or physical connection.
contains	is contained by	If one entity physically or logically houses another entity, then it contains that entity. The contained entity provides a service to the container.
controls	is controlled by	One entity, typically an SLA, specifies the levels of service that another entity is expected to provide.
defines	is defined by	If one entity describes another's actual or desired state, then it defines the other.
deploys	is deployed by	A responsible entity assembles and distributes other entities.
documents	is documented by	One entity, usually a document, describes the operation or other aspects of another entity. The 'documents' relationship is primarily descriptive instead of normative.
fails over	fails over	A peer-to-peer relationship between two entities where one entity can replace the other, usually in response to a disastrous interruption in service.
fronts	is fronted by	An entity is responsible for accepting and responding to requests for another physical entity. For example, a web server fronts an application.
governs	is governed by	A governing body (NIST, SOX PCAOB, SEC) typically issues regulations and rulings to which a governed entity, usually a service, must comply.
has an assignee	is assigned to	An entity, usually a person, has been designated responsible for another entity.
hosts	is hosted by	One entity hosts another entity which is continuous. The hosted entity uses services provided by the host entity.

Provider /Dependent	Dependent /Provider	Relationship Description
is business owner of	is owned by	An entity, usually a person, has been designated as the responsible business contact for another entity.
is gateway for	has for gateway	An entity, a hardware (computer) or network component, allows or controls access to another management device.
is high availability server for	has for high availability server	Uses clustering and database mirroring to provide very rapid recovery from system failures.
is location for	located at	An entity, in this case a physical location, has been designated as the place where another entity resides.
is primary contact for	has primary contact of	One entity is the primary contact for another entity.
is proxy for	is proxied by	An entity serves as a substitute pathway for connection to a network or remote storage device. For example, this gateway is a proxy for the clients on this LAN.
is recovery server of	has for recovery server	A service or application and a server that is configured to restore the specific service or application. Generally, recovery servers are an alternative to a cluster and are used when slower recovery is acceptable.
is required by	requires	An entity that cannot function properly without another entity.
is server of	is client of	A server-client relationship where the server responds to requests from the client. Alternative for "serves - is served by" relationship.
is source code for	source code is from	An entity, application code or an application library, provides the instructions that are executable in another entity.
is subscribed to by	subscribes to	An entity, either a group of users or a single user, "signs up" to have access to or use of another entity.
is the parent of	is the child of	One entity is the parent of another entity if the other entity cannot exist without the parent entity.
manages	is managed by	One entity manages another entity.
monitors	is monitored by	One entity monitors another entity if it tracks aspects of the other entity.
notifies	is notified by	An entity advises another entity that pertinent information of specific interest is now available.
provides to	is provided by	An entity is responsible for making another entity, usually a service, available to customers. For example, user, organization, or other entity provides a service.
regulates		One entity periodically adjusts some parameter of another entity. A time server which periodically regulates the time on other devices is an example.

Provider /Dependent	Dependent /Provider	Relationship Description
	is regulated by	
runs	runs on	One entity runs another transient entity.
secures	is secured by	An entity guards another entity against risks.
serves	is served by	Alternative for "is server of - is client of" relationship.
services	is serviced by	An entity, typically a maintenance organization or vendor, is responsible for responding to service calls for a physical entity.
supports	is supported by	An entity, usually an organization, is responsible for responding to incidents that emanate from another entity, usually a service.
updates	is updated by	An entity brings another entity's data up-to-date.
is used by	uses	An entity consumes data or services from another entity.

List Relationship Types

You can list CMDB relationship types to see the *directional* connections between CIs.

To list relationship types

1. Log into CA SDM as an administrator.
   The web interface appears.

2. Click Administration.
   The Administration tree appears.

3. Navigate the folder structure by clicking CMDB, CI Relationship Types.
   The relationship types are listed in columns: Provider To Dependent, Dependent to Provider, and Peer-to-Peer.

4. (Optional) Click a relationship type.
   Relationship type details appear in a separate window, and you can edit the relationship type.

Families and Classes

This section contains the following articles:

Base Families

The following CA SDM and CA APM base families do not have their own CMDB extension tables:

- Computer
- Hardware
- Other
- Projects (includes a CA Service Desk extension table)
- Software

In CMDB, CIs in these base families receive CMDB CI Detail pages with some extraneous fields and lacking an Attributes tab. You can use the Change Family and Class capability to convert these CIs to CMDB families to take advantage of CMDB advanced features such as the ability to track family-specific attributes, versioning, snapshots, and baselines.

Cluster Families

Contents

The Cluster families include the following:

- **Cluster**
  Identifies multiple servers linked together to handle variable workloads or if one or more devices fail, to provide continued operation.
- **Cluster.Resource**
  Identifies a member of a cluster resource group.

- **Cluster.Resource Group**
  Identifies a group of devices in a cluster.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Cluster	Cluster	net_clux	ci_network_cluster	Failover Cluster
Cluster.Resource	Resource	net_rsrcx	ci_network_resource	Resource Cluster
Cluster.Resource Group	Resource Group	net_rgrpx	ci_network_resource_group	Resource Group Cluster

Cluster Attributes

The Cluster family includes the following attributes that correspond to the net_clux extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
channel_address	Channel Address	The tag used to identify a channel on a port.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
gateway_id	Gateway ID	The unique identifier for a network point that acts as an entrance (gateway) to another network.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_effective_date	Lease Effective Date	The date on which a lease begins.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
		The time frame for which a maintenance contract is active.

Object Name	Label	Description
maintenance_period	Maintenance Period	
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI (for example, vendor or in-house).
network_address	Network Address	The IP address at which this CI resides (for example, 192.168.0.4)
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
os_version	OS Version	The version number of a CIs operating system.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
quorum	Quorum	The name of the definitive repository for all configuration information relating to a cluster.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
virtual_ip	Virtual IP Address	The designation of the IP address that is shared among multiple domain names or multiple servers.

Cluster.Resource Attributes

The Cluster.Resource family includes the following attributes that correspond to the net_rsrcx extension table:

Object Name	Label	Description
resource_disk	Resource Disk	The identifier for a shared disk to which access can be requested by a server or cluster node.
resource_file	Resource File	The identifier for a file folder whose subfolders can be shared among cluster resources.

Object Name	Label	Description
resource_group_type	Resource Group Type	The type of recovery domain for a cluster (for example, data resiliency, application resiliency, or device resiliency).
resource_mount_point	Resource Mount Point	The name of the directory where the device must be mounted.
resource_type	Resource Type	The categorization of a cluster resource (for example, physical disk, print spooler, file share, network name, local quorum, and so on).

Cluster.Resource Group Attributes

The Cluster.Resource Group family include the following attribute that correspond to the net_rgrpx extension table:

Object Name	Label	Description
resource_group_type	Resource Group Type	The type of recovery domain for a cluster (for example, data resiliency, application resiliency, or device resiliency).

Contact Family

Contents

The Contact family identifies a person or role that is active in the IT infrastructure.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Contact	Executive	cntx	ci_contact	A company executive
Contact	External Contact	cntx	ci_contact	A person or role from outside
Contact	Managerial	cntx	ci_contact	A manager
Contact	Other Contact	cntx	ci_contact	Miscellaneous person or role
Contact	Technical	cntx	ci_contact	A technician

Contact Attributes

The Contact family includes the following that correspond to the cntx extension table:

- **base_contact**
  Specifies the person or group that the CI represents (SREL uuid to cnt). Represents an exclusive relationship where only one CI represents a contact in the Contact family.

Object Name	Label
access_type	Access Type
available	Available
bm_status	Operational Status
contact_num	Contact ID
domain	Data Partition
first_name	First Name
global_queue_id	Global Queue
last_name	Group Name
last_name	Last Name
middle_name	Middle Name
position	Job Title
schedule	Work Schedule
service_type	Service Type
status	Configured Status
timezone	Time Zone
type	Contact Type
userid	User ID

Contract Family

Contents

The Contract family identifies a legally binding business document signed between two parties.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Contract	License Agreement	conx	ci_contract	License Agreement Contract
Contract	Other Contract	conx	ci_contract	Miscellaneous Contract
Contract	Warranty /Maintenance Contract	conx	ci_contract	Warranty /Maintenance Contract

Contract Attributes

The Contract family includes the following attributes that correspond to the conx extension table:

Object Name	Label	Description
con_comments	Comments	Free-form text to more fully describe the particular CI.
con_num	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
con_end_date	End Date	The date on which a contract, warranty, or other legal agreement expires.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
con_ref	Contract Reference	The name or number of another document that is related to a specified contract.
con_renewal_date	Renewal Date	The date on which an existing contract, warranty, or other legal agreement is put into effect for an additional period of time.
con_start_date	Start Date	The date on which a contract, document, service, or SLA becomes active.
con_status	Status	An indication of the status of an Application, Contract, Document, Service, or SLA CI (development, review, active, retired, and so on).
con_type	Type	A description of the kind of Application, Contract, Document, Service, or SLA CI.

Document Family

Contents

The Document family identifies printed or electronically stored text which is human-readable.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Document	Admin Guide	docx	ci_document	Administration Guide
Document	Application Test Plan	docx	ci_document	Application Test Plan Document
Document	Business Continuity Plan	docx	ci_document	Business Continuity Plan Document
Document	Other Document	docx	ci_document	Miscellaneous Document
Document	Policies and Standards	docx	ci_document	Policies and Standards Document
Document	Training Class Collateral	docx	ci_document	Training Class Collateral Document
Document	User Guide	docx	ci_document	User Guide Document

Document Attributes

The Document family includes the following attributes that correspond to the docx extension table:

Object Name	Label	Description
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
doc_category	Category	The high-level type designation for an application, service, SLA, or document.
doc_end_date	End Date	The date on which a document expires or is no longer valid.
doc_id	Document ID	The name or number that identifies a particular document.
doc_start_date	Start Date	The date on which a contract, document, service, or SLA becomes active.
doc_status	Status	An indication of the status of an Application, Contract, Document, Service, or SLA CI (development, review, active, retired, and so on).
doc_type	Type	A description of the kind of Application, Contract, Document, Service, or SLA CI.
doc_version	Version	A number or other identifier that indicates the current level (version) of an Application, Document, Service, or SLA CI.
priority	Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.

Enterprise Families

Contents

The Enterprise families include the following:

- **Enterprise.Service**
  Identifies a combination of people, processes, and information technology that directly or indirectly supports enterprise business processes.

- **Enterprise.Transaction**
  Identifies a single transaction in a transactional application.

- **Enterprise Transaction Context**
  Identifies an entity describing the flow of information for a specific application or the details of a complex transaction.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name
Enterprise.Service	Business Service	entsrvx	ci_enterprise_service
Enterprise.Service	Infrastructure Service	entsrvx	ci_enterprise_service
Enterprise.Service	Other Service	entsrvx	ci_enterprise_service
Enterprise.Transaction	Business Transactions	enttx	ci_enterprise_transaction
Enterprise Transaction Context	TransactionContext	trn_ctx	ci_transaction_ctx

Enterprise.Service Attributes

The Enterprise.Service family includes the following classes:

- Business Service
- Infrastructure Service
- Other Service

The Enterprise.Service family includes the following attributes that correspond to the entsrvx extension table:

Note: (R) indicates that the attribute can be stored as a relationship to other CIs.

Object Name	Label	Description
availability_end	Availability End	End of next anticipated service availability period for an intermittent service
availability_start	Availability Start	Start of next anticipated service availability period for an intermittent service
business_contacts (R)	Business Contacts	Business persons to contact with questions about service
business_impact	Business Impact	Magnitude of the effect on business if service is stopped or impaired
business_owner (R)	Business Owner	Person or persons who own the service
business_priority	Business Priority	Importance of the service to business
business_risk	Business Risk	Risk to business implied by the service

business_unit (R)	Business Unit	Business unit or units that receive the service
cancel_date	Cancel Date	Date service cancelled or terminated
category	Service Category	Service category
charge_code	Charge Code	Accounting code used to track service expenses
cobit_objective	Cobit Objective	Applicable COBIT control objective
description	Service Description	Service description
design_end_date	Design End Date	End date of design life cycle phase
design_start_date	Design Start Date	Start date of design life cycle phase
escalation_contacts (R)	Escalation Contacts	Persons to contact when escalating service issues
lifecycle_state	Service Lifecycle State	Conforms to ITIL v3. For example: design, transition, production, terminated.
lifecycle_status	Service Lifecycle Status	Status within lifecycle_state: Pending approval, Pending funding
operation_end_date	Operation End Date	End date of operations life cycle phase
operation_start_date	Operation Start Date	Start date of operations life cycle phase
portfolio (R)	Portfolio	Service portfolio holding service
service_alignment	Service Alignment	How well is service aligned to corporate goal? HIGH-MEDIUM-LOW
service_goal	Service Goal	Describe corporate strategy supported by the service
service_hours	Service Hours	Hours when service is normally available
service_manager (R)	Service Manager	Person or persons who manage the service
site (R)	Site	Primary location where service is maintained
SLA (R)	SLA	Brief description of applicable SLAs
transition_end_date	Transition End Date	End date of transition life cycle phase
transition_start_date	Transition Start Date	Start date of transition life cycle phase
unavailability_end	Unavailability End	End of next anticipated service blackout for an intermittent service
unavailability_start	Unavailability Start	Start of next anticipated service blackout for an intermittent service
version	Service Version	Current release of the service

Enterprise.Transaction Attributes

The Enterprise.Transaction family includes the following attributes that correspond to the enttx extension table:

Note: (R) indicates that the attribute can be stored as a relationship to other CIs.

Object Name	Label	Description
availability_end	Availability End	End of next anticipated service availability period for an intermittent service
availability_start	Availability Start	Start of next anticipated service availability period for an intermittent service
business_contacts (R)	Business Contacts	Business persons to contact with questions about service
business_impact	Business Impact	Magnitude of the effect on business if service is stopped or impaired
business_owner (R)	Business Owner	Person or persons who own the service
business_priority	Business Priority	Importance of the service to business
business_unit (R)	Business Unit	Business unit or units that receive the service
cancel_date	Cancel Date	Date service cancelled or terminated
category	Transaction Category	Service category
description	Transaction Description	Service description
design_end_date	Design End Date	End date of design life cycle phase
design_start_date	Design Start Date	Start date of design life cycle phase
escalation_contacts (R)	Escalation Contacts	Persons to contact when escalating service issues
lifecycle_state	Transaction Lifecycle State	DESIGN-TRANSITION-PRODUCTION-TERMINATED
lifecycle_status	Transaction Lifecycle Status	Status within lifecycle_state: Pending approval, Pending funding
operation_end_date	Operation End Date	End date of operations life cycle phase
operation_start_date	Operation Start Date	Start date of operations life cycle phase
site (R)	Site	Primary location where service is maintained
transaction_alignment	Transaction Alignment	Transaction Alignment
transaction_goal	Transaction Goal	Transaction Goal

Object Name	Label	Description
transaction_manager	Transaction Manager	Transaction Manager
transition_end_date	Transition End Date	End date of transition life cycle phase
transition_start_date	Transition Start Date	Start date of transition life cycle phase
unavailability_end	Unavailability End	End of next anticipated service blackout for an intermittent service
unavailability_start	Unavailability Start	Start of next anticipated service blackout for an intermittent service
version	Transaction Version	Current release of the service

Enterprise TransactionContext Attributes

The Enterprise.Transaction Context family includes the following attribute that corresponds to trn_ctx extension table:

Object Name	Label	Description
ContextType	Context Type	Type of context, whether a kind of application or a business context.

Facilities Family

Contents

The Facilities families include the following:

- **Facilities.Air Conditioning**
  Identifies air conditioning, heating, ventilation, humidity control, or general environment management systems.

- **Facilities.Fire Control**
  Identifies equipment for fire suppression.

- **Facilities.Furnishings**
  Identifies furnishings used to store important IT items.

- **Facilities.Other**
  Identifies miscellaneous facilities equipment or supplies.

- **Facilities.Uninterruptible Power Supply**
  Identifies uninterruptible power supplies, and other power conditioning and regulation systems.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Facilities.Air Conditioning	Air Conditioning	fac_acx	ci_fac_ac	Air Conditioning Facilities
Facilities.Fire Control	Fire Control	fac_firex	ci_fac_fire_control	Fire Control
Facilities.Furnishings	Equipment Rack	fac_furx	ci_fac_furnishings	Equipment Rack
Facilities.Furnishings	File Cabinet	fac_furx	ci_fac_furnishings	File Cabinet
Facilities.Other	Other Facilities	fac_othx	ci_fac_other	Miscellaneous Facilities
Facilities. Uninterruptible Power Supply	Uninterruptible Power Supply	fac_upsx	fac_upsx	Uninterruptible Power Supply

Facilities.Air Conditioning Attributes

The Facilities.Air Conditioning family includes the following attributes that correspond to the fac_acx extension table:

Object Name	Label	Description
active_date	Activation Date	The date on which the CI was put into active status.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_end_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_start_date	Lease Effective Date	The date on which a lease begins.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.

Object Name	Label	Description
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.

Facilities.Fire Control Attributes

The Facilities.Fire Control family includes the following attributes that correspond to the fac_firex extension table:

Object Name	Label	Description
active_date	Activation Date	The date on which the CI was put into active status.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_end_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.

Object Name	Label	Description
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_start_date	Lease Effective Date	The date on which a lease begins.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.

Facilities.Furnishings Attributes

The Facilities.Furnishings family includes the following attributes that correspond to the fac_furx extension table:

Object Name	Label	Description
active_date	Activation Date	The date on which the CI was put into active status.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.

Object Name	Label	Description
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_end_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_start_date	Lease Effective Date	The date on which a lease begins.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
warehouse_loc	Warehouse Location	The physical location of a warehouse or other storage facility where a CI resides after it has been received and is in "in stock" status.

Facilities.Other Attributes

The Facilities.Other family includes the following attributes that correspond to the fac_othx extension table:

Object Name	Label	Description
active_date	Activation Date	The date on which the CI was put into active status.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_end_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_start_date	Lease Effective Date	The date on which a lease begins.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
ci_priority	CI Priority	

Object Name	Label	Description
		The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
warehouse_loc	Warehouse Location	The physical location of a warehouse or other storage facility where a CI resides after it has been received and is in "in stock" status.

Facilities.Uninterruptible Power Supply Attributes

The Facilities.Uninterruptible Power Supply family includes the following attributes that correspond to the fac_upsx extension table:

Object Name	Label	Description
active_date	Activation Date	The date on which the CI was put into active status.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_end_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_start_date	Lease Effective Date	The date on which a lease begins.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.

Object Name	Label	Description
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
warehouse_loc	Warehouse Location	The physical location of a warehouse or other storage facility where a CI resides after it has been received and is in "in stock" status.

Hardware Families

Contents

- Hardware.File Attributes (see page 4217)
- Hardware.DiskPartition Attributes (see page 4218)
- Hardware.Memory Attributes (see page 4219)
- Hardware.Processor Attributes (see page 4220)
- Hardware.StoragePool Attributes (see page 4221)
- Hardware.StorageVolume Attributes (see page 4223)
- Hardware.VMDataStore Attributes (see page 4224)

The Hardware families include the following:

- **Hardware.Logical Partition**
  Identifies Logical Partitions (LPAR) that are a mainframe architecture that segments a single system into several independent logical systems.

- **Hardware.Mainframe**
  Identifies large central computing devices, traditionally manufactured by IBM and running z/OS, OS/390, and so on.

- **Hardware.Monitor**
  Identifies computer, video, and surveillance displays. Includes CRT's, LCD's, and plasma monitors.

- **Hardware.Other**
  Identifies miscellaneous IT hardware.

- **Hardware.Printer**
  Identifies a device typically connected to a computing system which converts electronic documents to visual physical media, usually paper.

- **Hardware.Server**
  Identifies computers on a network whose main function is to respond to requests from other computers rather than provide a display and keyboard to an individual user.

- **Hardware.Storage**
  Identifies units designed to store electronic data. Tape drives, optical disks, and SANs are all included.

- **Hardware.Virtual Machine**
  Identifies servers running on a system simulated in software, for example, VMWare, MSVM.

- **Hardware.Workstation**
  Identifies computers primarily used by end-users rather than serving other computers.

- **Hardware.EnvironmentalSensor**
  Identifies environmental sensor, measures physical quantity and converts it to a numeric value.

- **Hardware.File**
  Identified a file, directory or volume/filesystem that is being watched, on an executing hardware device, or that holds relevant management data.

- **Hardware.DiskPartition**
  Identifies the logical division of a physical hard drive to treat the drive as though it were multiple, independent disks.

- **Hardware.Memory**
  Identifies the physical or paging memory in an executing hardware device.

- **Hardware.PowerSupply**
  Identifies the hardware providing the current/voltages needed to operate a device.

- **Hardware.Processor**
  Identifies a processor (such as a CPU or math processor) in an executing hardware device.

- **Hardware.StoragePool**
  Identifies the grouping of storage capacity based on various criteria, such as location, cost or hardware ownership. Pools may consist of other pools or be assembled across MediaDrives.

- **Hardware.StorageVolume**
  Identifies the storage on an array backed by a StoragePool, MediaDrive or built on other lower-level volumes. A StorageVolume is published for use outside of its hosting system/array.

- **Hardware.VMDataStore**
  Identifies storage location for virtual machine files.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Hardware.Logical Partition	Logical Partition	har_lparx	ci_hardware_lpar	Mainframe Logical Partition
Hardware. Mainframe	Cray	har_maix	ci_hardware_mainframe	Cray Mainframe
Hardware. Mainframe	Group 80	har_maix	ci_hardware_mainframe	Group 80 Mainframe
Hardware. Mainframe	MVS	har_maix	ci_hardware_mainframe	MVS Mainframe
Hardware. Mainframe	OS/390	har_maix	ci_hardware_mainframe	OS/390 Mainframe
Hardware. Mainframe	Other Hardware Mainframe	har_maix	ci_hardware_mainframe	Miscellaneous Mainframe Hardware
Hardware. Mainframe	System 390	har_maix	ci_hardware_mainframe	System 390 Hardware
Hardware. Mainframe	System Z	har_maix	ci_hardware_mainframe	System Z Hardware
Hardware. Mainframe	Tandem - Mainframe	har_maix	ci_hardware_mainframe	Tandem Hardware
Hardware. Mainframe	Unisys.Mainframe	har_maix	ci_hardware_mainframe	Unisys Mainframe Hardware
Hardware. Mainframe	VAX - Mainframe	har_maix	ci_hardware_mainframe	VAX Hardware
Hardware. Mainframe	Virtual Storage Array	har_maix	ci_hardware_mainframe	Virtual Storage Array Hardware
	z/OS	har_maix		z/OS Hardware

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Hardware. Mainframe			ci_hardware_mainframe	
Hardware. Monitor	CRT	har_monx	ci_hardware_monitor	Cathode Ray Tube Monitor
Hardware. Monitor	Flat Screen	har_monx	ci_hardware_monitor	Flat Screen Monitor
Hardware. Monitor	Other Monitor	har_monx	ci_hardware_monitor	Miscellaneous Display Hardware
Hardware. Monitor	Terminal	har_monx	ci_hardware_monitor	Terminal Hardware
Hardware.Other	Barcode Reader	har_othx	ci_hardware_other	Barcode Reader Hardware
Hardware.Other	Copier	har_othx	ci_hardware_other	Copier Hardware
Hardware.Other	Digital Camera	har_othx	ci_hardware_other	Digital Camera
Hardware.Other	Electronic Whiteboard	har_othx	ci_hardware_other	Electronic Whiteboard
Hardware.Other	Other Hardware	har_othx	ci_hardware_other	Miscellaneous Hardware
Hardware.Other	Projector	har_othx	ci_hardware_other	Projector Hardware
Hardware.Other	Shredder	har_othx	ci_hardware_other	Shredder Hardware
Hardware.Other	Television	har_othx	ci_hardware_other	Television Hardware
Hardware.Other	VCR/DVD	har_othx	ci_hardware_other	VCR/DVD Hardware
Hardware.Other	Video Camera	har_othx	ci_hardware_other	Video Camera Hardware
Hardware.Printer	Bubble Jet	har_prix	ci_hardware_printer	Bubble Jet
Hardware.Printer	Ink Jet	har_prix	ci_hardware_printer	Ink Jet
Hardware.Printer	Laser	har_prix	ci_hardware_printer	Laser Printer
Hardware.Printer	Microfiche	har_prix	ci_hardware_printer	Microfiche Printer
Hardware.Printer	Other Printer	har_prix	ci_hardware_printer	Miscellaneous Printer Hardware
Hardware.Printer	Plotter	har_prix	ci_hardware_printer	Plotter Printer
Hardware.Server	AIX	har_serx	ci_hardware_server	Server using AIX
Hardware.Server	HP UX	har_serx	ci_hardware_server	Server using HP-UX
Hardware.Server	Linux	har_serx		Server using Linux

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
			ci_hardware_server	
Hardware.Server	Other Operating System	har_serx	ci_hardware_server	Server using miscellaneous OS
Hardware.Server	Server	har_serx	ci_hardware_server	Server Hardware
Hardware.Server	Sun	har_serx	ci_hardware_server	Server using Sun
Hardware.Server	Tandem	har_serx	ci_hardware_server	Server using Tandem
Hardware.Server	Unisys	har_serx	ci_hardware_server	Server using Unisys
Hardware.Server	UNIX	har_serx	ci_hardware_server	Server using UNIX
Hardware.Server	VAX	har_serx	ci_hardware_server	Server using VAX
Hardware.Server	VM	har_serx	ci_hardware_server	Server using VM
Hardware.Server	Windows	har_serx	ci_hardware_server	Server using Windows
Hardware.Storage	CD-Rom Drive	har_stox	ci_hardware_storage	CD-Rom Drive
Hardware.Storage	Disk Array	har_stox	ci_hardware_storage	Disk Array
Hardware.Storage	DVD	har_stox	ci_hardware_storage	DVD Storage
Hardware.Storage	File System	har_stox	ci_hardware_storage	File System Storage
Hardware.Storage	Hard Drive	har_stox	ci_hardware_storage	Hard Drive
Hardware.Storage	Network Attached Storage	har_stox	ci_hardware_storage	Network Attached Storage
Hardware.Storage	Optical	har_stox	ci_hardware_storage	Optical Hardware
Hardware.Storage	Other Hardware Storage	har_stox	ci_hardware_storage	Miscellaneous Storage Hardware
Hardware.Storage	Silo	har_stox	ci_hardware_storage	Storage Silo Hardware
Hardware.Storage	Storage Area Network	har_stox	ci_hardware_storage	Storage Area Network (SAN) Hardware
Hardware.Storage	Tape Array	har_stox	ci_hardware_storage	Tape Storage Array

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Hardware.Storage	Tape Library	har_stox	ci_hardware_storage	Tape Storage Library
Hardware.Storage	Virtual Tape System	har_stox	ci_hardware_storage	Virtual Tape System
Hardware.Storage	Zip Drive	har_stox	ci_hardware_storage	Zip Drive Hardware
Hardware.Virtual Machine	ESX Server	har_virx	ci_hardware_virtual	ESX Server
Hardware.Virtual Machine	GSX Server	har_virx	ci_hardware_virtual	GSX Server
Hardware.Virtual Machine	Microsoft Virtual Server	har_virx	ci_hardware_virtual	Microsoft Virtual Server
Hardware.Virtual Machine	Other Hardware Virtual Machine	har_virx	ci_hardware_virtual	Miscellaneous Virtual Machines
Hardware. Workstation	Workstation	har_worx	ci_hardware_workstation	Workstation Hardware
Hardware. EnvironmentalSensor	Temperature	har_comp	ci_hardware_component	Environmental Sensor
Hardware.File	File	har_file	ci_hardware_file	File, Directory or Volume/ Filesystem
Hardware. DiskPartition	BFS	har_dpar	ci_hardware_dpar	Logical division of a physical hard drive
Hardware. Memory	Physical	har_mem	ci_hardware_memory	Memory (physical or paging)
Hardware. PowerSupply	PowerSupply	har_comp	ci_hardware_component	
Hardware. Processor	x86	har_prcr	ci_hardware_processor	Processor
Hardware. StoragePool	StoragePool	har_stgpl	ci_hardware_storagepool	Storage Capacity
Hardware. StorageVolume	StorageVolume	har_stgvol	ci_hardware_storagevolume	Storage on an Array
Hardware. VMDataStore	NetworkFileSystem	har_vmds	ci_hardware_vmdatastore	Storage location for virtual machine files

Hardware.Logical Partition Attributes

The Hardware.Logical Partition family includes the following attributes that correspond to the har_lparx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
current_memory	Current Memory Used	An indication of how much memory is used, as opposed to the total amount available.
current_processors	Current Processors Used	An indication of how many of the processors are in use compared to the number available.
desired_memory	Desired Amount of Memory	The amount of memory to be allocated to a logical partition as long as the memory on the managed resource is not overcommitted.
desired_processors	Desired Number of Processors	The number of processors to be allocated to a logical partition as long as the processors on the managed resource are not overcommitted.
disk_type	Disk Type	The type of disk drive that resides on a workstation or server.
hard_drive_capacity	Disk Capacity	The amount of hard drive capacity that is available for use on a Hardware CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_start_date	Lease Effective Date	The date on which a lease becomes effective (also known as the lease start date).
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_end_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
max_memory	Maximum Memory Size	The maximum amount of memory available in an LPAR.

Object Name	Label	Description
max_processors	Maximum Number of Processors	The maximum number of processors available in an LPAR.
mem_capacity	Memory Capacity	The total amount of memory that can be installed and made available.
min_memory	Minimum Amount of Memory	The minimum amount of memory required for an LPAR.
min_processors	Minimum Number of Processors	The minimum number of processors required for an LPAR.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
number_mips	MIPS	An indication of the processing speed and capacity of a hardware or network device.
panel_display	Panel Display	The operator console used to manage logical partition configurations and booting, starting, and stopping of system or individual partitions.
phys_mem	Memory Installed	The physical amount of memory installed on a hardware device.
priority	Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proc_speed	Processor Speed	A measurement of the rate at which a computer performs its operations.
proc_type	Processor Type	The kind of CPU in a hardware device.
profile	Profile	The configuration name for a logical partition which indicates the desired system resource allocations.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.

Hardware.Mainframe Attributes

The Hardware.Mainframe family includes the following attributes that correspond to the har_maix extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
disk_type	Disk Type	The type of disk drive that resides on a workstation or server.
hard_drive_capacity	Disk Capacity	The amount of hard drive capacity that is available for use on a Hardware CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease becomes effective (also known as the lease start date).
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_end_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mem_capacity	Memory Capacity	The total amount of memory that can be installed and made available.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
number_mips	MIPS	An indication of the processing speed and capacity of a hardware or network device.
phys_mem	Memory Installed	The physical amount of memory installed on a hardware device.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proc_speed	Processor Speed	A measurement of the rate at which a computer performs its operations.

Object Name	Label	Description
proc_type	Processor Type	The kind of CPU in a hardware device.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.

Hardware.Monitor Attributes

The Hardware.Monitor family includes the following attributes that correspond to the har_monx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease becomes effective (also known as the lease start date).
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
		The number that uniquely identifies a maintenance contract.

Object Name	Label	Description
mtce_contract_number	Maintenance Contract Number	
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.

Hardware.Other Attributes

The Hardware.Other family includes the following attributes that correspond to the har_othx extension table:

Object Name	Label	Description
active_date	Activation Date	The date on which the CI was put into active status.
array_name	Storage Array Name	The identifier for an enterprise storage system that contains multiple disk drives and performs functions like RAID and virtualization.
array_serial_num	Storage Array Serial Number	The manufacturer's serial number for an enterprise storage system that contains multiple disk drives and performs functions like RAID and virtualization.
bios_ver	BIOS Version	The version number of the BIOS - the code that's run when a personal computer starts up.
cd_rom_type	CD ROM Type	The type of CD ROM drive that resides on a workstation or server.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
disk_type	Disk Type	The type of disk drive that resides on a workstation or server.
graphics_card	Graphics Card Model	The model designation for an expansion card that is installed in an available slot in a device for enhanced graphics capabilities.
hard_drive_capacity	Disk Capacity	The amount of hard drive capacity that is available for use on a Hardware CI.

Object Name	Label	Description
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease becomes effective (also known as the lease start date).
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_end_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
media_drive_num	Media Drive Capacity	The capacity of the hardware device that consolidates multiple memory cards into one unit.
media_type	Media Type	The kind of storage media on a hardware device, for example, disk, CD ROM.
mem_cache_proc	Processor Cache	The identifier of the hardware device that processes the high-speed memory storage between memory and the CPU.
mem_capacity	Memory Capacity	The total amount of memory that can be installed and made available.
memory_shares	Number of Memory Shares	The specified memory share granted to this virtual machine.
modem_card	Modem Card	The identifier of a card in a workstation or network device that enables a faster connection to a network or the Internet.
modem_type	Modem Type	The classification/speed of a modem used by a workstation for a faster connection to a network or the Internet.
monitor	Monitor Model	The type of display unit connected to a hardware, network, or telecom device.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
net_card	Network Card	

Object Name	Label	Description
		The designation for an expansion card that is installed in an available slot in a computer or network device so that it can connect and communicate to another networked component.
number_mips	MIPS	An indication of the processing speed and capacity of a hardware or network device.
number_net_card	Number of Network Cards	The number of expansion cards that have been installed in the available slots in a computer.
number_net_port	Number of Network Ports	The total number of ports in use on a device.
number_net_port_conn	Number of Network Port Connections	The total number of ports on a server.
number_proc_inst	Number of Processors Installed	The total number of processors installed on a hardware or network device.
number_slot_proc	Processor Capacity	The total number of processor slots on a hardware device.
phys_mem	Memory Installed	The physical amount of memory installed on a hardware device.
printer	Printer	The type or model of printer attached to a hardware or network device.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proc_speed	Processor Speed	A measurement of the rate at which a computer performs its operations.
proc_type	Processor Type	The kind of CPU in a hardware device.
processor_count	Processor Capacity	The number of CPU's or microprocessors available on a Hardware CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
role	Role	The business function supported by a hardware or network device, for example, production, test.
security_patch_level	Security Patch Level	An indication of the current security patch version for this CI.
server_type	Server Type	The kind of server, for example, application, mail, web, proxy, FTP.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.

slot_mem_used	Number of Memory Slots Used	The amount of memory in use from the available memory cards in a hardware or network device.
slot_total_mem	Number of Memory Slots	The total amount of memory available on memory cards in a hardware or network device.
swap_size	Swap Size	The size of the disk space allocated on a hardware or network device to store the state of a process that has been swapped out.
technology	Technology	The technology, TCP/IP, Ethernet, FDDI, and so on, employed by a hardware or network device.
total_capacity	Total Disk Capacity	The total amount of storage available on a hardware device.
type_net_conn	Type of Network Connection	An indication of the kind of network connection used by a hardware or network device.
used_space	Total Disk Used	The amount of available disk storage space that is in use by a CI.

Hardware.Printer Attributes

The Hardware.Printer family includes the following attributes that correspond to the har_prix extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease becomes effective (also known as the lease start date).
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_end_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.

Object Name	Label	Description
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.

Hardware.Server Attributes

The Hardware.Server family includes the following attributes that correspond to the har_serx extension table:

Object Name	Label	Description
active_date	Activation Date	The date on which the CI was put into active status.
bios_ver	BIOS Version	The version number of the BIOS - the code that's run when a personal computer starts up.
cd_rom_type	CD ROM Type	The type of CD ROM drive that resides on a workstation or server.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
hard_drive_capacity	Disk Capacity	The amount of hard drive capacity that is available for use on a Hardware CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.

Object Name	Label	Description
lease_effective_date	Lease Effective Date	The date on which a lease becomes effective (also known as the lease start date).
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mem_capacity	Memory Capacity	The total amount of memory that can be installed and made available.
monitor	Monitor Model	The type of display unit connected to a hardware, network, or telecom device.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
net_card	Network Card	The designation for an expansion card that is installed in an available slot in a computer or network device so that it may connect and communicate to another networked component.
number_mips	MIPS	An indication of the processing speed and capacity of a hardware or network device.
number_net_card	Number of Network Cards	The number of expansion cards that have been installed in the available slots in a computer.
number_net_port	Number of Network Ports	The total number of ports in use on a device.
number_net_port_conn	Number of Network Port Connections	The total number of ports on a server.
number_proc_inst	Number of Processors Installed	The total number of processors installed on a hardware or network device.
number_slot_proc	Processor Capacity	The total number of processor slots on a hardware device.

Object Name	Label	Description
panel_display	Panel Display	The operator console used to manage logical partition configurations and booting, starting, and stopping of system or individual partitions.
phys_mem	Memory Installed	The physical amount of memory installed on a hardware device.
printer	Printer	The type or model of printer attached to a hardware or network device.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proc_speed	Processor Speed	A measurement of the rate at which a computer performs its operations.
proc_type	Processor Type	The kind of CPU in a hardware device.
profile	Profile	The configuration name for a logical partition which indicates the desired system resource allocations.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
role	Role	The business function supported by a hardware or network device, for example, production, test.
security_patch_level	Security Patch Level	An indication of the current security patch version for this CI.
server_type	Server Type	The kind of server, for example, application, mail, web, proxy, FTP.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
slot_mem_used	Number of Memory Slots Used	The amount of memory in use from the available memory cards in a hardware or network device.
slot_total_mem	Number of Memory Slots	The total amount of memory available on memory cards in a hardware or network device.
swap_size	Swap Size	The size of the disk space allocated on a hardware or network device to store the state of a process that has been swapped out.
technology	Technology	The technology, TCP/IP, Ethernet, FDDI, and so on, employed by a hardware or network device.
type_net_conn	Type of Network Connection	An indication of the kind of network connection used by a hardware or network device.

Hardware.Storage Attributes

The Hardware.Storage family includes the following attributes that correspond to the har_stox extension table:

Object Name	Label	Description
active_date	Activation Date	The date on which the CI was put into active status.
array_name	Storage Array Name	The identifier for an enterprise storage system that contains multiple disk drives and performs functions like RAID and virtualization.
array_serial_num	Storage Array Serial Number	The manufacturer's serial number for an enterprise storage system that contains multiple disk drives and performs functions like RAID and virtualization.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
disk_type	Disk Type	The type of disk drive that resides on a workstation or server.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease becomes effective (also known as the lease start date).
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
media_drive_num	Media Drive Capacity	The capacity of the hardware device that consolidates multiple memory cards into one unit.
media_type	Media Type	The kind of storage media on a hardware device, for example, disk, CD ROM.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.

Object Name	Label	Description
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
total_capacity	Total Disk Capacity	The total amount of storage available on a hardware device.
used_space	Total Disk Used	The amount of available disk storage space that is in use by a CI.

Hardware.Virtual Machine Attributes

The Hardware.Virtual Machine family includes the following attributes that correspond to the har_virx extension table:

Object Name	Label	Description
active_date	Activation Date	The date on which the CI was put into active status.
bios_ver	BIOS Version	The version number of the BIOS - the code that's run when a personal computer starts up.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
cpu_shares	Number of CPU Shares	The specified CPU shares granted to this virtual machine.
disk_type	Disk Type	The type of disk drive that resides on a workstation or server.
hard_drive_capacity	Disk Capacity	The amount of hard drive capacity that is available for use on a Hardware CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease becomes effective (also known as the lease start date).

Object Name	Label	Description
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
media_type	Media Type	The kind of storage media on a hardware device, for example, disk, CD ROM.
mem_capacity	Memory Capacity	The total amount of memory that can be installed and made available.
memory_shares	Number of Memory Shares	The specified memory share granted to this virtual machine.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
number_mips	MIPS	An indication of the processing speed and capacity of a hardware or network device.
phys_mem	Memory Installed	The physical amount of memory installed on a hardware device.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proc_speed	Processor Speed	A measurement of the rate at which a computer performs its operations.
proc_type	Processor Type	The kind of CPU in a hardware device.
processor_affinity	Processor Affinity	An indicator of the preferred processor on which a task should be scheduled to run.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
	Retire Date	The date on which a CI is no longer active.

Object Name	Label	Description
retire_date		
security_patch_level	Security Patch Level	An indication of the current security patch version for this CI.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
virtual_processors	Number of Virtual Processors	The number of virtual processors, the representations of physical processors to the operating system of a logical partition that uses the shared processor pool.

Hardware.Workstation Attributes

The Hardware.Workstation family includes the following attributes that correspond to the har_worx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
bios_ver	BIOS Version	The version number of the BIOS - the code that's run when a personal computer starts up.
cd_rom_type	CD ROM Type	The type of CD ROM drive that resides on a workstation or server.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
disk_type	Disk Type	The type of disk drive that resides on a workstation or server.
graphics_card	Graphics Card Model	The model designation for an expansion card that is installed in an available slot in a device for enhanced graphics capabilities.
hard_drive_capacity	Disk Capacity	The amount of hard drive capacity that is available for use on a Hardware CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease becomes effective (also known as the lease start date).
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.

Object Name	Label	Description
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
max_memory	Maximum Memory Size	The maximum amount of memory available in an LPAR.
max_processors	Maximum Number of Processors	The maximum number of processors available in an LPAR.
media_drive_num	Media Drive Capacity	The capacity of the hardware device that consolidates multiple memory cards into one unit.
media_type	Media Type	The kind of storage media on a hardware device, for example, disk, CD ROM.
mem_cache_proc	Processor Cache	The identifier of the hardware device that processes the high-speed memory storage between memory and the CPU.
mem_capacity	Memory Capacity	The total amount of memory that can be installed and made available.
modem_card	Modem Card	The identifier of a card in a workstation or network device that enables a faster connection to a network or the Internet.
modem_type	Modem Type	The classification/speed of a modem used by a workstation for a faster connection to a network or the Internet.
monitor	Monitor Model	The type of display unit connected to a hardware, network, or telecom device.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
net_card	Network Card	The designation for an expansion card that is installed in an available slot in a computer or network device so that it may connect and communicate to another networked component.
number_proc_inst	Number of Processors Installed	The total number of processors installed on a hardware or network device.
number_slot_proc	Processor Capacity	The total number of processor slots on a hardware device.
phys_mem	Memory Installed	The physical amount of memory installed on a hardware device.
printer	Printer	The type or model of printer attached to a hardware or network device.

Object Name	Label	Description
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proc_speed	Processor Speed	A measurement of the rate at which a computer performs its operations.
proc_type	Processor Type	The kind of CPU in a hardware device.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retired Date	The date on which a CI is no longer active.
scsi_card	SCSI Card Model	The model identifier for a card that provides a standard interface and command set for transferring data between internal and external peripheral devices.
security_patch_level	Security Patch Level	An indication of the current security patch version for this CI.
svclvl	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for the IT component.
slot_mem_used	Number of Memory Slots Used	The amount of memory in use from the available memory cards in a hardware or network device.
slot_total_mem	Number of Memory Slots	The total amount of memory available on memory cards in a hardware or network device.

Hardware.EnvironmentalSensor Attributes

The Hardware.EnvironmentalSensor family includes the following attributes that corresponds to the har_comp extension table:

Object Name	Label	Description
DeviceAssetNumber	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
DeviceBiosSystemID	Device BIOS System ID	The identifier reported from the BIOS for the device.
DeviceDnsName	Device DNS Name	The fully qualified DNS name of the device.
DeviceSysName	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.

Object Name	Label	Description
DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.
DeviceMacAddress	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
DeviceIPV4Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4AddressWithDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
DeviceIPV6Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).
DeviceIPV6AddressWithDomain	Device IPV6 Address With Domain	An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
OSNumeric	OS Numeric	A numeric value either assigned by or calculated from the operating system.
ContainingIndex	Containing Index	A numeric value defining the index of the containing entity, as specified by the value of entPhysicalContainedIn in the Entity MIB.
IsPhysical	Is Physical	A boolean indicating whether the hardware is physical (if true) or logical /simulated (if false).
ContextID	Context ID	The ContextID element is used for identification.

Hardware.File Attributes

The Hardware.File family includes the following attributes that corresponds to the har_file extension table:

Object Name	Label	Description
DeviceAssetNumber	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
DeviceBiosSystemID	Device BIOS System ID	The identifier reported from the BIOS for the device.
DeviceDnsName	Device DNS Name	The fully qualified DNS name of the device.
DeviceSysName	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.

DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.
DeviceMacAddress	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
DeviceIPV4Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4AddressWithDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
DeviceIPV6Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).
DeviceIPV6AddressWithDomain	Device IPV6 Address With Domain	An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
FilePathUrl	File Path URL	A fully qualified path and file name (if applicable). Wild card characters are not allowed.

Hardware.DiskPartition Attributes

The Hardware.DiskPartition family includes the following attributes that corresponds to the har_dpar extension table:

Object Name	Label	Description
DeviceAssetNumber	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
DeviceBiosSystemID	Device BIOS System ID	The identifier reported from the BIOS for the device.
DeviceDnsName	Device DNS Name	The fully qualified DNS name of the device.
DeviceSysName	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.
DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.

Object Name	Label	Description
DeviceMac Address	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
DeviceIPV4 Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4 AddressWit hDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
DeviceIPV6 Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).
DeviceIPV6 AddressWit hDomain	Device IPV6 Address With Domain	An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
OSNumeric	OS Numeric	A numeric value either assigned by or calculated from the operating system.
ContainingI ndex	Containing Index	A numeric value defining the index of the containing entity, as specified by the value of entPhysicalContainedIn in the Entity MIB.
IsPhysical	Is Physical	A boolean indicating whether the hardware is physical (if true) or logical /simulated (if false).
CapacityIn MB	Capacity In MB	Maximum capacity of this Partition (in binary mebi-bytes).
ContextID	Context ID	The ContextID element is used for identification.

Hardware.Memory Attributes

The Hardware.Memory family includes the following attributes that corresponds to the har_mem extension table:

Object Name	Label	Description
DeviceAsset Number	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
DeviceBiosS ystemID	Device BIOS System ID	The identifier reported from the BIOS for the device.
DeviceDnsN ame	Device DNS Name	The fully qualified DNS name of the device.
DeviceSysN ame	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.

Object Name	Label	Description
DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.
DeviceMacAddress	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
DeviceIPV4Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4AddressWithDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
DeviceIPV6Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).
DeviceIPV6AddressWithDomain	Device IPV6 Address With Domain	An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
OSNumeric	OS Numeric	A numeric value either assigned by or calculated from the operating system.
ContainingIndex	Containing Index	A numeric value defining the index of the containing entity, as specified by the value of entPhysicalContainedIn in the Entity MIB.
IsPhysical	Is Physical	A boolean indicating whether the hardware is physical (if true) or logical /simulated (if false).
ContextID	Context ID	The ContextID element is used for identification.
SizeInMB	Size In MB	Maximum size of this File (file system, directory or individual file).

Hardware.Processor Attributes

The Hardware.Processor family includes the following attributes that corresponds to the har_prcr extension table:

Object Name	Label	Description
DeviceAssetNumber	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
DeviceBiosSystemID	Device BIOS System ID	The identifier reported from the BIOS for the device.
DeviceDnsName	Device DNS Name	The fully qualified DNS name of the device.

Object Name	Label	Description
DeviceSysName	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.
DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.
DeviceMacAddress	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
DeviceIPV4Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4AddressWithDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
DeviceIPV6Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).
DeviceIPV6AddressWithDomain	Device IPV6 Address With Domain	An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
OSNumeric	OS Numeric	A numeric value either assigned by or calculated from the operating system.
ContainingIndex	Containing Index	A numeric value defining the index of the containing entity, as specified by the value of entPhysicalContainedIn in the Entity MIB.
IsPhysical	Is Physical	A boolean indicating whether the hardware is physical (if true) or logical /simulated (if false).
ContextID	Context ID	The ContextID element is used for identification.
SpeedInGHz	Speed In GHz	The speed (in giga-hertz) of the Processor.

Hardware.StoragePool Attributes

The Hardware.StoragePool family includes the following attributes that corresponds to the har_stgpl extension table:

Object Name	Label	Description
DeviceAssetNumber	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
		The identifier reported from the BIOS for the device.

Object Name	Label	Description
DeviceBiosSystemID	Device BIOS System ID	
DeviceDnsName	Device DNS Name	The fully qualified DNS name of the device.
DeviceSysName	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.
DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.
DeviceMacAddress	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
DeviceIPV4Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4AddressWithDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
DeviceIPV6Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).
DeviceIPV6AddressWithDomain	Device IPV6 Address With Domain	An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
IsHAEnabled	Is HA Enabled	A numeric value either assigned by or calculated from the operating system. Boolean indicating whether the group (typically a Cluster instance or a GroupType="ResourceCluster") supports high availability/failover (if true) or not (if false).
IsMonitoringMembers	Is Monitoring Members	Boolean indicating whether the group (typically a Cluster instance or a GroupType="ResourceCluster") currently is using a heartbeat or other individual monitoring technique to determine if availability is lost (if true) or whether this capability does not exist or is not currently enabled (if false).
MaxFailures	Max Failures	Number of failures that can be supported by the Group, by sparing or other load balancing means.
MemberCriteria	Member Criteria	

Object Name	Label	Description
		Defines a comma-separated list of QNames, representing the constraints on the constituency of the Group. Instances referenced as the Target element in the HasMember relationship semantic should have one of the types specified.
GroupType	Group Type	An enumerated value describing the primary type or category of the Group - such as an "authorization group", a "virtual resource pool" or a "data center".
HomePage	Home Page	The URL of the website home page.
BusinessRelevance	Business Relevance	Description of the relevance of the Entity, to the business.
CapacityInGB	Capacity In GB	The total capacity (in gibi-bytes) available for allocation to StorageVolumes or child StoragePools.
RaidLevel	Raid Level	The RAID level used for the Pool.

Hardware.StorageVolume Attributes

The Hardware.StorageVolume family includes the following attributes that corresponds to the har_stgvol extension table:

Object Name	Label	Description
DeviceAssetNumber	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
DeviceBiosSystemID	Device BIOS System ID	The identifier reported from the BIOS for the device.
DeviceDnsName	Device DNS Name	The fully qualified DNS name of the device.
DeviceSysName	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.
DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.
DeviceMacAddress	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
DeviceIPV4Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4AddressWithDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").

DeviceIPV6 Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).
DeviceIPV6 AddressWithDomain	Device IPV6 Address With Domain	An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
OSNumeric	OS Numeric	A numeric value either assigned by or calculated from the operating system.
ContainingIndex	Containing Index	A numeric value defining the index of the containing entity, as specified by the value of entPhysicalContainedIn in the Entity MIB.
IsPhysical	Is Physical	A boolean indicating whether the hardware is physical (if true) or logical /simulated (if false).
LogicalUnit Number	Logical Unit Number	The LUN (logical unit number) used to access the Volume.
PortID	Port ID	The system/array port through which the StorageVolume is accessed.
PortWWName	Port WW Name	The World-Wide Name of the system/array port through which the StorageVolume is accessed.
CapacityIn MB	Capacity In MB	Maximum capacity of this Volume (in binary mebi-bytes).
IsThinlyProvisioned	Is Thinly Provisioned	Boolean indicating if the Volume is allocated on-demand ("thinly provisioned"), if true, or strictly allocated, if false.
IsDeDupeEnabled	Is DeDuplication Enabled	Boolean indicating if the Volume is deduplication enabled, if true, or if redundant data is persisted, if false.
IsMasked	Is Masked	When this boolean is true, the system/array validates the World-Wide Names of ports accessing the Volume, to ensure they are masked for that volume (present in the list, MaskedWWNames).
MaskedWW Names	Masked WW Names	A comma-separated list of WWNames of the allowed ports, permitted access by the StorageVolume.
RaidLevel	Raid Level	The RAID level used for the Volume. Values (both standard and non-standard) are defined by the open enumeration, RaidLevelEnum.

Hardware.VMDataStore Attributes

The Hardware.VMDataStore family includes the following attributes that corresponds to the har_vmds extension table:

Object Name	Label	Description
DeviceAsset Number	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
		The identifier reported from the BIOS for the device.

Object Name	Label	Description
DeviceBiosSystemID	Device BIOS System ID	
DeviceDnsName	Device DNS Name	The fully qualified DNS name of the device.
DeviceSysName	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.
DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.
DeviceMacAddress	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
DeviceIPV4Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4AddressWithDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
DeviceIPV6Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).
DeviceIPV6AddressWithDomain	Device IPV6 Address With Domain	An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
FilePathUrl	File Path URL	A fully qualified path and file name (if applicable). Wild card characters are not allowed.
CapacityInMB	Capacity In MB	Maximum capacity of this datastore (in binary mebi-bytes).
IsMultiHost	Is Multi Host	Indicates whether (or not) more than one hosting system has been configured with access to the data store.

Investment Families

Contents

The Investment families include the following:

- **Investment.Idea**
  Identifies the initial stage of creating new opportunities for investment such as projects, assets, applications, products, services, and other work. Ideas are containers for pertinent information that become the foundation for specific investments.

- **Investment.Other**
  Identifies a broad category to include investments in Application, Asset, Product, Service, and Other Work.

- **Investment.Project**
  Identifies a set of activities designed to achieve a specific objective. Labor, time, and budget constraints guide the projects.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Investment. Idea	Portfolio Idea	invidex	ci_investment_idea	Ideas are the initial stage of creating new opportunities for investment such as projects, assets, applications, products, services, and other work. Ideas lay the foundation for a specific type of investment by serving as a container for pertinent information.
Investment. Other	Portfolio Application	invothx	ci_investment_other	Captures data specific to applications running or being implemented in an organization.
Investment. Other	Portfolio Asset	invothx	ci_investment_other	Captures data specific to assets which incur costs and benefits for an organization.
Investment. Other	Portfolio Product	invothx	ci_investment_other	Captures data specific to products produced or owned by an organization.
Investment. Other	Portfolio Service	invothx	ci_investment_other	Captures data specific to services provided by an organization.
Investment. Other	Portfolio Work	invothx	ci_investment_other	Captures data specific to steady-state work performed. Other work can represent overhead tasks such as management and maintenance.
Investment. Project	Portfolio Program	invprjx	ci_investment_project	A Program is a top-level project that serves as the parent or "umbrella" project to one or more child projects.
		invprjx	ci_investment_project	A Project is a set of activities designed to achieve a specific objective. Projects are guided by labor, time and budget constraints.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Investment.Project	Portfolio Project			

Investment.Idea Attributes

The Investment.Idea family includes the following class:

- Portfolio Idea

The Investment.Idea family includes the following attributes that correspond to the invidex extension table:

Object Name	Label
business_unit	Business Unit
dependencies	Dependencies
est_finish_date	Estimated Finish Date
est_start_date	Estimated Start Date
existing_initiative_impact	Existing Initiative Impact
general_notes	General Notes
idea_priority	Idea Priority
owner	Owner
risks	Risks
subject	Subject
target_manager	Target Manager

Investment.Other Attributes

The Investment.Other family includes the following classes:

- Portfolio Application
- Portfolio Asset
- Portfolio Product
- Portfolio Service
- Portfolio Work

The Investment.Other family includes the following attributes that correspond to the invothx extension table:

Object Name	Label
active	Investment Active?
alignment	Alignment
charge_code	Charge Code
currency	Currency
finish_date	Finish Date
goal	Goal
investment_priority	Investment Priority
investment_status	Investment Status
manager	Manager
progress	Progress
risk	Risk
stage	Stage
start_date	Start Date
status_comment	Investment Status Comment
status_indicator	Investment Status Indicator
total_cost	Total Cost
total_effort	Total Effort
type	Investment Type

Investment.Project Attributes

The Investment.Project family includes the following classes:

- Portfolio Program
- Portfolio Project

The Investment.Project family includes the following attributes that correspond to the invprjx extension table:

Object Name	Label
active	Project Active?
alignment	Alignment
charge_code	Charge Code
currency	Currency
finish_date	Finish Date
goal	Goal
manager	Manager
progress	Progress
project_priority	Project Priority

project_status	Project Status
risk	Risk
stage	Stage
start_date	Start Date
status_comment	Project Status Comment
status_indicator	Project Status Indicator
total_cost	Total Cost
total_effort	Total Effort

Location Family

Contents

The Location family includes the following:

- **Location**
  Identifies a physical position or site.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Location	Building	locx	ci_location	A site contained within a single physical structure
Location	Campus	locx	ci_location	A group of buildings
Location	City	locx	ci_location	A governmental designation of a relatively large and populous area
Location	Country	locx	ci_location	An area comprised of multiple cities, regions, or states
Location	Datacenter	locx	ci_location	A site dedicated to IT operations
Location	Floor	locx	ci_location	A segment of a site on a single floor

Location Attributes

The Location family includes the following class:

- base_location
  Specifies the location that the CI represents (SREL uuid to loc). Represents an exclusive relationship where only one CI represents a location in the Location family.

The Location family includes the following attributes that correspond to the locx extension table:

Object Name	Label
address1	Address

Object Name	Label
city	City
country	Country
description	Description
site	Site
state	State/Province
zip	ZIP/Postal Code

Network Families

Contents

The Network families include the following:

- **Network.Bridge**
  Identifies an abstract device that connects multiple network segments along the data link layer.

- **Network.Controller**
  Identifies miscellaneous devices that throttle or manage bandwidth use.

- **Network.Frontend**
  Identifies a network front-end device that handles communication with host computers such as mainframes.

- **Network.Hub**
  Identifies a network device that connects together network devices by repeating the signal received at one port to others.

- **Network.Network Interface Card**
  Identifies a Network Interface Card (NIC) using any network communications protocol. Ethernet LAN and FDDI Ring network cards are NICs.

- **Network.Other**
  Identifies unclassified network components.

- **Network.Peripheral**
  Identifies network peripherals that are appliances such as printers and FAX machines that contain their own NIC cards.

- **Network.Port**
  Identifies a port on a network hub or switch that is used to connect to other hubs and switches instead of an end station.

- **Network.Router**
  Identifies any device in a network that routes messages between computers.

- **Network.Switch**
  Identifies a network device that intelligently forwards packets received at one port to other ports.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Network. Bridge	Bridge	net_brix	ci_network_bridge	Network Bridge
Network. Controller	Controller	net_conx	ci_network_controller	Controller
Network. Frontend	3270 Terminal	net_frox	ci_network_frontend	3270 Terminal
Network. Frontend	Network Terminal	net_frox	ci_network_frontend	Network Terminal
Network. Frontend	X Terminal	net_frox	ci_network_frontend	X Terminal
Network.Hub	Network Hub	net_hubx	ci_network_hub	Hub on a network
Network. Network	Interface Card	net_nicx	ci_network_nic	Network Interface Card (NIC)
Network. Other	Other Network Device	net_othx	ci_network_other	Other Network Device
Network. Peripheral	Fax Machine	net_perx	ci_network_peripheral	Fax Machine
Network.Port	Port	net_porx	ci_network_port	Network Port
Network. Router	Router	net_roux	ci_network_router	Ethernet Router
Network. Switch	Network Switch	net_gatx	ci_network_gateway	Network Switch

Network.Bridge Attributes

The Network.Bridge family includes the following attributes that correspond to the net_brix extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
addr_class	Address Class	

Object Name	Label	Description
		IP address values are arranged in Address Classes (A, B, and C). The Address Classes determine how many workstations can possibly exist on the network.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
gateway_id	Gateway ID	The unique identifier for a network point that acts as an entrance (gateway) to another network
ip_mgmt_addr	Management IP Address	The IP address assigned to a station (PC or workstation) that is authorized for either manager- or operator-level access to a switch.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
number_net_card	Number of Network Cards	The number of expansion cards that have been installed in the available slots in a computer.
		The total number of ports in use on a server.

Object Name	Label	Description
number_net_port	Number of Network Ports	
number__net_port_conn	Number of Network Port Connections	The total number of network port connections.
number_ports	Number of Ports	The total number of ports on a network device.
number_ports_used	Number of Ports Used	The total number of ports in use on a network device.
os_version	OS Version	The version number of a CI's operating system.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
protocol	Protocol	The communication method employed by a network device.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
role	Role	The business function supported by a hardware or network device, for example, production, test.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
subnet_mask	Subnet Mask	The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address, for example, 255.128.0.0.
type_net_conn	Type of Network Connection	An indication of the kind of network connection used by a hardware or network device.

Network.Controller Attributes

The Network.Controller family includes the following attributes that correspond to the net_conx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
addr_class	Address Class	IP address values are arranged in Address Classes (A, B, and C). The Address Classes determine how many workstations can possibly exist on the network.

Object Name	Label	Description
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
ip_mgmt_addr	Management IP Address	The IP address assigned to a station (PC or workstation) that is authorized for either manager- or operator-level access to a switch.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
number_mips	MIPS	An indication of the processing speed and capacity of a hardware or network device.
number_net_card	Number of Network Cards	The number of expansion cards that have been installed in the available slots in a computer.
		The total number of ports in use on a server.

Object Name	Label	Description
number_net_port	Number of Network Ports	
number_net_port_conn	Number of Network Port Connections	The total number of network port connections.
number_ports	Number of Ports	The total number of ports on a network device.
number_ports_used	Number of Ports Used	The total number of ports in use on a network device.
number_proc_inst	Number of Processors Installed	The total number of processors installed on a hardware or network device.
number_smips	Number of SMIPS	The toal number of SMIPS.
os_version	OS Version	The version number of a CI's operating system.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
role	Role	The business function supported by a hardware or network device, for example, production, test.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
subnet_mask	Subnet Mask	The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address, for example, 255.128.0.0.
technology	Technology	The technology (TCP/IP, Ethernet, FDDI, and so on) employed by a hardware or network device.
type_net_conn	Type of Network Connection	An indication of the kind of network connection used by a hardware or network device.

Network.Frontend Attributes

The Network.Frontend family includes the following attributes that correspond to the net_frox extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
addr_class	Address Class	IP address values are arranged in Address Classes (A, B, and C). The Address Classes determine how many workstations can possibly exist on the network.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
ip_mgmt_addr	Management IP Address	The IP address assigned to a station (PC or workstation) that is authorized for either manager- or operator-level access to a switch.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.

Object Name	Label	Description
number_mips	MIPS	An indication of the processing speed and capacity of a hardware or network device.
number_net_card	Number of Network Cards	The number of expansion cards that have been installed in the available slots in a computer.
number_net_port	Number of Network Ports	The total number of ports in use on a server.
number_net_port_conn	Number of Network Port Connections	The total number of network port connections.
number_ports	Number of Ports	The total number of ports on a network device.
number_ports_used	Number of Ports Used	The total number of ports in use on a network device.
number_proc_inst	Number of Processors Installed	The total number of processors installed on a hardware or network device.
number_smips	Number of SMIPS	The total number of SMIPS.
os_version	OS Version	The version number of a CI's operating system.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
role	Role	The business function supported by a hardware or network device, for example, production, test.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
subnet_mask	Subnet Mask	The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address, for example, 255.128.0.0.
technology	Technology	The technology (TCP/IP, Ethernet, FDDI, and so on) employed by a hardware or network device.
type_net_conn	Type of Network Connection	An indication of the kind of network connection used by a hardware or network device.

Network.Hub Attributes

The Network.Hub family includes the following attributes that correspond to the net_hubx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
addr_class	Address Class	IP address values are arranged in Address Classes (A, B, and C). The Address Classes determine how many workstations can possibly exist on the network.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
gateway_id	Gateway ID	The unique identifier for a network point that acts as an entrance (gateway) to another network
ip_mgmt_addr	Management IP Address	The IP address assigned to a station (PC or workstation) that is authorized for either manager- or operator-level access to a switch.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.

Object Name	Label	Description
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
net_card	Network Card	The designation for an expansion card that is installed in an available slot in a computer or network device so that it may connect and communicate to another networked component.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
number_net_card	Number of Network Cards	The number of expansion cards that have been installed in the available slots in a computer.
number_net_port	Number of Network Ports	The total number of ports in use on a server.
number_net_port_conn	Number of Network Port Connections	The total number of network port connections.
number_ports	Number of Ports	The total number of ports on a network device.
number_ports_used	Number of Ports Used	The total number of ports in use on a network device.
os_version	OS Version	The version number of a CI's operating system.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
role	Role	The business function supported by a hardware or network device, for example, production, test.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
subnet_mask	Subnet Mask	The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address, for example, 255.128.0.0.
technology	Technology	The technology (TCP/IP, Ethernet, FDDI, and so on) employed by a hardware or network device.
type_net_conn	Type of Network Connection	An indication of the kind of network connection used by a hardware or network device.

Network.Network Interface Card Attributes

The Network.Network Interface Card family includes the following attributes that correspond to the net_nicx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
addr_class	Address Class	IP address values are arranged in Address Classes (A, B, and C). The Address Classes determine how many workstations can possibly exist on the network.
gateway_id	Gateway ID	The unique identifier for a network point that acts as an entrance (gateway) to another network
ip_mgmt_addr	Management IP Address	The IP address assigned to a station (PC or workstation) that is authorized for either manager- or operator-level access to a switch.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
line_speed	Line Speed	The rate at which information is transmitted on a network connection.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
number_net_card	Number of Network Cards	The number of expansion cards that have been installed in the available slots in a computer.
number_net_port	Number of Network Ports	The total number of ports in use on a server.
number_net_port_conn	Number of Network Port Connections	The total number of network port connections.
number_ports	Number of Ports	The total number of ports on a network device.
number_ports_used	Number of Ports Used	The total number of ports in use on a network device.
os_version	OS Version	The version number of a CI's operating system.
protocol	Protocol	The communication method employed by a network device.
retire_date	Retire Date	The date on which a CI is no longer active.
role	Role	The business function supported by a hardware or network device, for example, production, test.
	Subnet Mask	

Object Name	Label	Description
subnet_mask		The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address, for example, 255.128.0.0.
technology	Technology	The technology (TCP/IP, Ethernet, FDDI, and so on) employed by a hardware or network device.
type_net_conn	Type of Network Connection	An indication of the kind of network connection used by a hardware or network device.

Network.Other Attributes

The Network.Other family includes the following attributes that correspond to the net_othx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
bios_ver	BIOS Version	The version number of the BIOS - the code that is run when a personal computer starts up.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
gateway_id	Gateway ID	The unique identifier for a network point that acts as an entrance (gateway) to another network
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
	Maintenance Period	The time frame for which a maintenance contract is active.

Object Name	Label	Description
maintenance_period		
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
os_version	OS Version	The version number of a CI's operating system.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
subnet_mask	Subnet Mask	The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address, for example, 255.128.0.0.

Network.Peripheral Attributes

The Network.Peripheral family includes the following attributes that correspond to the net_perx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
addr_class	Address Class	IP address values are arranged in Address Classes (A, B, and C). The Address Classes determine how many workstations can possibly exist on the network.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.

Object Name	Label	Description
gateway_id	Gateway ID	The unique identifier for a network point that acts as an entrance (gateway) to another network.
ip_mgmt_addr	Management IP Address	The IP address assigned to a station (PC or workstation) that is authorized for either manager- or operator-level access to a switch.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
number_net_card	Number of Network Cards	The number of expansion cards that have been installed in the available slots in a computer.
number_net_port	Number of Network Ports	The total number of ports in use on a server.
		The total number of network port connections.

Object Name	Label	Description
number_net_port_conn	Number of Network Port Connections	
number_ports	Number of Ports	The total number of ports on a network device.
number_ports_used	Number of Ports Used	The total number of ports in use on a network device.
os_version	OS Version	The version number of a CI's operating system.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
role	Role	The business function supported by a hardware or network device, for example, production, test.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
subnet_mask	Subnet Mask	The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address, for example, 255.128.0.0.
technology	Technology	The technology (TCP/IP, Ethernet, FDDI, and so on) employed by a hardware or network device.
type_net_conn	Type of Network Connection	An indication of the kind of network connection used by a hardware or network device.

Network.Port Attributes

The Network.Port family includes the following attributes that correspond to the net_porx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
addr_class	Address Class	IP address values are arranged in Address Classes (A, B, and C). The Address Classes determine how many workstations can possibly exist on the network.
channel_address	Channel Address	The tag used to identify a channel on a port.

Object Name	Label	Description
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
domain	Domain	The identifier of the logical grouping (domain) to which a network or telecom device is assigned.
gateway_id	Gateway ID	The unique identifier for a network point that acts as an entrance (gateway) to another network.
ip_mgmt_addr	Management IP Address	The IP address assigned to a station (PC or workstation) that is authorized for either manager- or operator-level access to a switch.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
line_speed	Line Speed	The rate at which information is transmitted on a network connection.
line_type	Line Type	The categorization of a network communication line, for example, ISDN.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.

Object Name	Label	Description
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
number_net_card	Number of Network Cards	The number of expansion cards that have been installed in the available slots in a computer.
number_net_port	Number of Network Ports	The total number of ports in use on a server.
number_net_port_conn	Number of Network Port Connections	The total number of network port connections.
number_ports	Number of Ports	The total number of ports on a network device.
number_ports_used	Number of Ports Used	The total number of ports in use on a network device.
os_version	OS Version	The version number of a CI's operating system.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
protocol	Protocol	The communication method employed by a network device.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
role	Role	The business function supported by a hardware or network device, for example, production, test.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
subnet_mask	Subnet Mask	The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address, for example, 255.128.0.0.
technology	Technology	The technology (TCP/IP, Ethernet, FDDI, and so on) employed by a hardware or network device.
type_net_conn	Type of Network Connection	An indication of the kind of network connection used by a hardware or network device.

Network.Router Attributes

The Network.Router family includes the following attributes that correspond to the net_roux extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
addr_class	Address Class	IP address values are arranged in Address Classes (A, B, and C). The Address Classes determine how many workstations can possibly exist on the network.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
flow	Flow	The amount of network traffic that can be handled by a router.
ip_mgmt_addr	Management IP Address	The IP address assigned to a station (PC or workstation) that is authorized for either manager- or operator-level access to a switch.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mem_cache_proc	Processor Memory Cache	The identifier of the hardware device that processes the high-speed memory storage between memory and the CPU.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
		The IP address at which this CI resides, for example, 192.168.0.4.

Object Name	Label	Description
network_address	Network Address	
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
number_net_card	Number of Network Cards	The number of expansion cards that have been installed in the available slots in a computer.
number_net_port	Number of Network Ports	The total number of ports in use on a server.
number_net_port_conn	Number of Network Port Connections	The total number of network port connections.
number_ports	Number of Ports	The total number of ports on a network device.
number_ports_used	Number of Ports Used	The total number of ports in use on a network device.
number_proc_inst	Number of Ports Installed	The total number of processors installed on a hardware or network device.
os_version	OS Version	The version number of a CI's operating system.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
protocol	Protocol	The communication method employed by a network device.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
role	Role	The business function supported by a hardware or network device, for example, production, test.
rout_prot	Router Protocol	The communication method employed by a network router.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
slot_mem_used	Number of Memory Slots Used	The amount of memory in use from the available memory cards in a hardware or network device.
slot_total_mem	Number of Memory Slots	The total amount of memory available on memory cards in a hardware or network device.
subnet_mask	Subnet Mask	The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address, for example, 255.128.0.0.

Object Name	Label	Description
technology	Technology	The technology (TCP/IP, Ethernet, FDDI, and so on) employed by a hardware or network device.
type_net_conn	Type of Network Connection	An indication of the kind of network connection used by a hardware or network device.

Network.Switch Attributes

The Network.Switch family includes the following attributes that correspond to the net_gatx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
addr_class	Address Class	IP address values are arranged in Address Classes (A, B, and C). The Address Classes determine how many workstations can possibly exist on the network.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
gateway_id	Gateway ID	The unique identifier for a network point that acts as an entrance (gateway) to another network
graphics_card	Graphics Card Model	The model designation for an expansion card that is installed in an available slot in a device for enhanced graphics capabilities.
ip_mgmt_addr	Management IP Address	The IP address assigned to a station (PC or workstation) that is authorized for either manager- or operator-level access to a switch.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.

Object Name	Label	Description
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
number_net_card	Number of Network Cards	The number of expansion cards that have been installed in the available slots in a computer.
number_net_port	Number of Network Ports	The total number of ports in use on a server.
number_net_port_conn	Number of Network Port Connections	The total number of network port connections.
number_ports	Number of Ports	The total number of ports on a network device.
number_ports_used	Number of Ports Used	The total number of ports in use on a network device.
os_version	OS Version	The version number of a CI's operating system.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
role	Role	The business function supported by a hardware or network device, for example, production, test.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
	Subnet Mask	

Object Name	Label	Description
subnet_mask		The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address, for example, 255.128.0.0.
technology	Technology	The technology (TCP/IP, Ethernet, FDDI, and so on) employed by a hardware or network device.
type_net_conn	Type of Network Connection	An indication of the kind of network connection used by a hardware or network device.

Organization Family

Contents

The Organization family includes the following:

- **Organization**
  Identifies an entity representing a structured group of persons.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Organization	External	orgx	ci_organization	An organization not part of the company
Organization	Internal	orgx	ci_organization	An organizational segment of the company

Organization Attributes

The Organization family contains the following class:

- **base_organization**
  Specifies the organization that the CI represents (SREL uuid to org). Represents an exclusive relationship where only one CI represents an organization in the Organization family.

The Organization family includes the following attributes that correspond to the net_orgx extension table:

Object Name	Label
alt_phone	Alternate Phone Number
billing_code	Billing Code
contact	Organization Contact
description	Description
email_addr	Email Address
fax_phone	Fax Number
location	Location

Object Name	Label
org_num	Organization Code
owning_contract	Service Contract
pemail_addr	Pager Email Address
phone_number	Primary Phone Number
service_type	Service Type
status	Configured Status

Security Family

Contents

The Security family includes the following:

- **Security**
  Identifies security systems that protect data, software, and hardware against unauthorized access or manipulation. These systems include digital certificates, directory services, and biomechanical or key-based systems.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Security	Application Security	secx	ci_security	Application Security
Security	Building Security	secx	ci_security	Building Security
Security	Data Security	secx	ci_security	Data Security
Security	Other Security	secx	ci_security	Miscellaneous Security

Security Attributes

The Security family includes the following attributes that correspond to the secx extension table:

Object Name	Label	Description
appl	Applies To	The designation of the domain of this security CI.
avail	Availability	An indication of when access to a security-related CI is offered.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
confidentiality_level	Confidentiality Level	The level of confidentiality (for example, view-only, high, medium, low) for a security-related CI.

Object Name	Label	Description
integrity_level	Integrity Level	The level of integrity (for example, high, medium, low) for a particular security-related CI.
priority	Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
security_id	SecurityID	Number or other identifier for a security-related CI.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.

Service Family

Contents

Important: The Service family has been deprecated in CA CMDB Release 12.9. Use the Enterprise Service family instead.

The Service family comprises:

- **Service**
  Identifies an entity that delivers or performs a consistent set of tasks to a consumer. Services can be high-level business services or lower level IT technical services. Support, email, accounting are often delivered as services.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
Service	Component	serx	ci_service	CA NSM Business Process View (BPV) Component
Service	Document	serx	ci_service	CA NSM BPV Document
Service	Person	serx	ci_service	CA NSM BPV Person
Service	Practice	serx	ci_service	CA NSM BPV Practice
Service	Process	serx	ci_service	CA NSM BPV Process
Service	Role	serx	ci_service	CA NSM BPV Role
Service	Service	serx	ci_service	CA NSM BPV Service

Service Attributes

The Service family includes the following attributes that correspond to the serx extension table:

Object Name	Label	Description
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
end_date	End Date	The date on which a service expires or is no longer valid.
portfolio	Service Portfolio	The name or identifier for a grouping of related services.
priority	Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
service_id	Service ID	The name or other unique identifier for a Service CI.
site	Site	A designation to describe the location of a CI.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
start_date	Start Date	The date on which a contract, document, service, or SLA becomes active.
type	Type	A description of the kind of Application, Contract, Document, Service, or SLA CI.
version	Version	A number or other identifier that indicates the current level (version) of an Application, Document, Service, or SLA CI.

Service Level Agreement (SLA) Family

Contents

The Service Level Agreement family includes the following classes that identify agreements between a service provider and consumer:

- Operational Level Agreement
- Other Service Level Agreement
- Service Level Agreement
- Underpinning Contract

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name
Service Level Agreement	Operational Level Agreement	slax	ci_sla
		slax	ci_sla

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name
Service Level Agreement	Other Service Level Agreement		
Service Level Agreement	Service Level Agreement	slax	ci_sla
Service Level Agreement	Underpinning Contract	slax	ci_sla

Service Level Agreement Attributes

The Service Level Agreement family includes the following attributes that correspond to the slax extension table:

Object Name	Label	Description
sla_category	Service Level Agreement Category	The high-level type designation for an application, service, SLA, or document.
sla_date_active	Service Level Agreement Activation Date	The date on which the Configuration Item was made available to users.
sla_end_date	Service Level Agreement End Date	The date on which an SLA expires or is no longer valid.
sla_id	Service Level Agreement ID	The unique name or other identifier for a Service Level Agreement CI.
sla_start_date	Service Level Agreement Start Date	The date on which a contract, document, service, or SLA becomes active.
sla_status	Service Level Agreement Status	An indication of the status of an Application, Contract, Document, Service, or SLA CI (development, review, active, retired, and so on).
sla_type	Service Level Agreement Type	A description of the kind of Application, Contract, Document, Service, or SLA CI.
sla_version	Service Level Agreement Version	A number or other identifier that indicates the current level (version) of an Application, Document, Service, or SLA CI.

Software Families

Contents

The Software families include the following:

- **Software.Application System**
  Identifies a group of related applications that perform a high-level business function, such as an SAP Financials system.

- **Software.Application Component**
  Identifies an aspect of a software program, application or application system, that is managed as part of a business transaction, and is responsible for a specific operation. Examples include a database connection or a web service.

- **Software.Application**
  Identifies programmatic components of the IT infrastructure.

- **Software.Application Server**
  Identifies a software engine that delivers client applications to client computers, typically through the Internet and using HTTP (Hypertext Transfer Protocol).

- **Software.Bespoke**
  Identifies software customized or constructed to order.

- **Software.COTS**
  Identifies software that was purchased, or leased and is manufactured outside of the owning company.

- **Software.Database**
  Identifies database management systems (DBMS) such as Oracle, DB2, and MS SQL.

- **Software.In-House**
  Identifies software applications developed by the company using the application.

- **Software.Operating System**
  Identifies system Software installed on a computer or similar device that provides basic services and enables other software to run.

- **Software.MessageServer**
  Identifies the software that processes incoming and outgoing mail message sent to/from authorized users.

- **Software.ESXHypervisor**
  Identifies the VMware software running on the OS of a VM hosting machine.

- **Software.HyperVHypervisor**
  Identifies the hyper-V software running on the OS of a VM hosting machine.

- Software.NetworkServer
  Identifies a server that is solely focused on providing protocol-specific functionality.

- Software.ResourceServer
  Identifies a system/software providing storage and query of resources - such as media - accessed via HTTP requests/responses.

- **Software.Schema**
  Identifies a named collection of data tables, stored procedures, and so on, that are managed and manipulated in a database management system (server).

- **Software.Tablespace**
  Identifies the description of the logical storage of a Database. A Tablespace bridges between the structure of the database (tables, indices, etc.) and a system's file system.

- **Software.VirtualManager**
  Identifies an application that manages a virtualization environment, the VM definitions, host machines and VMs running on the hosts.

- **Software.Website**
  Identifies a specialization of Group, representing a collection of files, designed for access using the World Wide Web, with a starting location/URI (also known as a "home page").

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name
Software.Application System	Application System	app_extx	ci_app_ext
Software.Application Component	SoftwareComponent	app_extx	ci_app_ext
Software.Application	Application	app_extx	ci_app_ext
Software.Application	Application Instance	app_extx	ci_app_ext
Software.Application Server	Application Server	app_extx	ci_app_ext
Software.Application Server	Application Server Instance	app_extx	ci_app_ext
Software.Bespoke	Bespoke	app_extx	ci_app_ext
Software.COTS	Batch	app_extx	ci_app_ext
Software.COTS	CICS	app_extx	ci_app_ext
Software.COTS	COTS	app_extx	ci_app_ext
Software.COTS	Network Software	app_extx	ci_app_ext
Software.COTS	Security	app_extx	ci_app_ext
Software.COTS	STC	app_extx	ci_app_ext
Software.COTS	TSO	app_extx	ci_app_ext
Software.COTS	WebSphere MQ	app_extx	ci_app_ext
Software.COTS	BackgroundProcess	app_extx	ci_app_ext
Software.COTS	BusinessProcessServer	app_extx	ci_app_ext
Software.COTS	Bootsoftware	app_extx	ci_app_ext

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name
Software.COTS	ManagementAgent	app_extx	ci_app_ext
Software.Database	CA-Datacom	dat_basx	ci_database
Software.Database	CA-IDMS	dat_basx	ci_database
Software.Database	DB2	dat_basx	ci_database
Software.Database	IMS	dat_basx	ci_database
Software.Database	Ingres	dat_basx	ci_database
Software.Database	Oracle	dat_basx	ci_database
Software.Database	Other Software Database	dat_basx	ci_database
Software.Database	SQL	dat_basx	ci_database
Software.Database	Sybase	dat_basx	ci_database
Software.In-House	In-House	app_inhx	ci_app_inhouse
Software.Operating System	AIX OS	opsysx	ci_operating_system
Software.Operating System	HP UX OS	opsysx	ci_operating_system
Software.Operating System	Linux OS	opsysx	ci_operating_system
Software.Operating System	MVS OS	opsysx	ci_operating_system
Software.Operating System	OS/390 OS	opsysx	ci_operating_system
Software.Operating System	Other Software	opsysx	ci_operating_system
Software.Operating System	Sun OS	opsysx	ci_operating_system
Software.Operating System	Tandem OS	opsysx	ci_operating_system
Software.Operating System	Unisys OS	opsysx	ci_operating_system
Software.Operating System	UNIX OS	opsysx	ci_operating_system
Software.Operating System	Vax OS	opsysx	ci_operating_system
Software.Operating System	VM OS	opsysx	ci_operating_system
Software.Operating System	Windows OS	opsysx	ci_operating_system
Software.Operating System	z/OS OS	opsysx	ci_operating_system

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name
Software.Schema	DatabaseSchema	app_extx	ci_app_ext
Software.DirectoryServer	LDAP	app_extx	ci_app_ext
Software.MessageServer	CommunicationServer	app_extx	ci_app_ext
Software.MessageServer	MailServer	app_extx	ci_app_ext
Software.ESXHypervisor	ESXHypervisor	app_esx	ci_app_esxhypervisor
Software.HyperVHypervisor	HyperVHypervisor	app_hyp	ci_app_hypervhypervisor
Software.NetworkServer	NetworkServer	app_netsvr	ci_app_netsvr
Software.ResourceServer	ResourceServer	app_ressvr	ci_app_ressvr
Software.ResourceServer	SecurityServer	app_ressvr	ci_app_ressvr
Software.ResourceServer	TransactionServer	app_ressvr	ci_app_ressvr
Software.ResourceServer	MessageServer	app_ressvr	ci_app_ressvr
Software.Tablespace	Tablespace	app_extx	ci_app_ext
Software.VirtualManager	VirtualizationManager	app_virmgr	ci_app_virtualmgr
Software.Website	Website	app_website	ci_app_website

Software Attributes

The following attributes correspond to the app_extx extension table and apply to the following families:

- Software.Application
- Software.Application Server
- Software.Bespoke
- Software.COTS

Object Name	Label	Description
app_id	Application ID	Application name or other unique identifier.
category	Category	The high-level type designation for an application.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on of a CI or group of CIs.
date_installed	Date Installed	The date on which the physical installation of a Configuration Item was completed.

Object Name	Label	Description
environment	Environment	The application environment (for example, development, test, production) or project environment (for example, mainframe, distributed).
highavail_appl_resources	High Availability Resource	The name of the resource that provides high availability capability for an Application CI.
highly_avail	Under High Availability?	An indication (Yes/No) that an Application CI operates in a high availability production scenario.
inhouse_or_vendor	External Vendor	The internal department responsible for development/maintenance of this software.
install_dir	Installation Directory	The directory where an application stores its program files.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_end_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_start_date	Lease Effective Date	The date on which a lease begins.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific timeframe or was purchased.
main_process	Main Process	The designation of the main thread of an application process.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The timeframe for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
portfolio	Portfolio	A grouping of projects into a unit for management and tracking purposes.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.

Object Name	Label	Description
response_time	Response Time	The desired time measurement between the time a transaction is entered and the application returns a response.
server	Server	The name of the server on which an application runs.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
storage_used	Storage Used	The amount of available storage that is in use.
support_end_date	Support End Date	The date on which support for an application is no longer provided.
support_start_date	Support Start Date	The beginning date on which support for an application is provided.
support_type	Support Type	The kind of support that is provided for this CI, for example, gold/silver /bronze.
type	Type	A description of the kind of Application, Contract, Document, Service, or SLA CI.
uptime	Uptime	The desired "availability" that indicates the proportion of time a component is in a fully functioning condition.
version	Version	A number or other identifier that indicates the current level (version) of an Application, Document, Service, or SLA CI.

Software.Database Attributes

The Software.Database family includes the following attributes that correspond to the dat_basx extension table:

Object Name	Label	Description
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on of a CI or group of CIs.
db_id	Database ID	A name that uniquely identifies a database.
environment	Environment	The application environment (for example, development, test, production) or project environment (for example, mainframe, distributed).
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific timeframe or was purchased.
portfolio	Portfolio	A grouping of projects into a unit for management and tracking purposes.
priority	Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code		The ID or other unique identifier for the project to which a CI is assigned.

Object Name	Label	Description
	Project Code	
server	Server	The name of the server on which an application runs.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
support_end_date	Support End Date	The date on which support for an application is no longer provided.
support_start_date	Support Start Date	The beginning date on which support for an application is provided.
support_type	Support Type	The kind of support that is provided for this CI, for example, gold/silver /bronze.
type	Type	A description of the kind of Application, Contract, Document, Service, or SLA CI.
version	Version	A number or other identifier that indicates the current level (version) of an Application, Document, Service, or SLA CI.

Software.In-House Attributes

The Software.In-House family includes the following attributes that correspond to the app_inhx extension table:

Object Name	Label	Description
app_id	Application ID	Application name or other unique identifier.
category	Category	The high-level type designation for an application, service, SLA, or document.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
date_installed	Date Installed	The date on which the physical installation of a Configuration Item was completed.
environment	Environment	The application environment (for example, development, test, production) or project environment (for example, mainframe, distributed).
highavail_appl_resources	High Availability Resource	The name of the resource that provides high availability capability for an Application CI.
highly_avail	Under High Availability?	An indication (Yes/No) that an Application CI operates in a high availability production scenario.
inhouse_or_vendor	Inhouse Department	The internal department responsible for development/maintenance of this software.

Object Name	Label	Description
install_dir	Installation Directory	The directory where an application stores its program files.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific timeframe or was purchased.
main_process	Main Process	The designation of the main thread of an application process.
portfolio	Portfolio	A grouping of projects into a unit for management and tracking purposes.
priority	Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost of a CI.
response_time	Response Time	The desired time measurement between the time a transaction is entered and the application returns a response.
server	Server	The name of the server on which an application runs.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
storage_used	Storage Used	The amount of available storage that is in use.
support_end_date	Support End Date	The date on which support for an application is no longer provided.
support_start_date	Support Start Date	The beginning date on which support for an application is provided.
support_type	Support Type	The kind of support that is provided for this CI, for example, gold/silver /bronze.
type	Type	A description of the kind of Application, Contract, Document, Service, or SLA CI.
uptime	Uptime	The desired "availability", indicating the proportion of time a component is in a fully functioning condition.
version	Version	A number or other identifier that indicates the current level (version) of an Application, Document, Service, or SLA CI.

Software.Operating System Attributes

The Software.Operating System family includes the following attributes that correspond to the opsysx extension table:

Object Name	Label	Description
os_id		Operating system name or other unique identifier.

Object Name	Label	Description
	Operating System ID	
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on of a CI or group of CIs.
date_installed	Date Installed	The date on which the physical installation of a Configuration Item was completed.
environment	Environment	The application environment (for example, development, test, production) or project environment (for example, mainframe, distributed).
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_end_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_start_date	Lease Effective Date	The date on which a lease begins.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific timeframe or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The timeframe for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
server	Server	The name of the server on which an application runs.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.

Object Name	Label	Description
support_end_date	Support End Date	The date on which support for an application is no longer provided.
support_start_date	Support Start Date	The beginning date on which support for an application is provided.
support_type	Support Type	The kind of support that is provided for this CI, for example, gold/silver /bronze.
type	OS Type	A description of the kind of Application, Contract, Document, Service, or SLA CI.
version	Version	A number or other identifier that indicates the current level (version) of an Application, Document, Service, or SLA CI.

Software.ESXHypervisor Attributes

The Software.ESXHypervisor family includes the following attributes that corresponds to the app_esx extension table:

Object Name	Label	Description
DeviceAssetNumber	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
DeviceBiosSystemID	Device BIOS System ID	The identifier reported from the BIOS for the device.
DeviceDnsName	Device DNS Name	The fully qualified DNS name of the device.
DeviceSysName	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.
DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.
DeviceMacAddress	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
DeviceIPV4Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4AddressWithDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
DeviceIPV6Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).

Object Name	Label	Description
DeviceIPV6AddressWithDomain	Device IPV6 Address With Domain	An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
IsMigrationEnabled	Is Migration Enabled	Boolean indicating whether (or not) migration of VM's between hosts is enabled.
ComputeResourceIndex	Compute Resource Index	Identifier for a single host, acting as a "compute resource". Either a single system or a cluster can be a "compute resource".
HostIndex	Host Index	An index generated by VMware for the host, for example, host-6746.
DatacenterPath	Datacenter Path	Although hosts are managed by vCenter and its data centers, this element is provided for query purposes. It indicates the data center to which the host belongs.
FTVersion	FT Version	The version of Fault Tolerance running on the host. Only hosts with the same version of Fault Tolerance are compatible.
NumberOfPrimaryVMs	Number Of Primary VMs	The total number of primary VMs configured to this host, supported by fault tolerance.
NumberOfSecondaryVMs	Number Of Secondary VMs	The total number of secondary VMs configured to this host, to support fault tolerance.

Software.HyperVHypervisor Attributes

The Software.HyperVHypervisor family includes the following attributes that corresponds to the app_hyp extension table:

Object Name	Label	Description
DeviceAssetNumber	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
DeviceBiosSystemID	Device BIOS System ID	The identifier reported from the BIOS for the device.
DeviceDnsName	Device DNS Name	The fully qualified DNS name of the device.
DeviceSysName	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.
DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.
DeviceMacAddress	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.

DeviceIPV4Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4AddressWithDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
DeviceIPV6Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).
DeviceIPV6AddressWithDomain	Device IPV6 Address With Domain	An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
IsMigrationEnabled	Is Migration Enabled	Boolean indicating whether (or not) migration of VM's between hosts is enabled.
DefaultExternalDataRoot	Default External Data Root	The fully-qualified path to the default location for the Hyper-V files.
DefaultVhdPath	Default VHD Path	The fully-qualified path to the default location for the Hyper-V Virtual Hard Disk files.
MinimumMacAddress	Minimum MAC Address	The minimum MAC address for dynamically generated MAC addresses. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
MaximumMacAddress	Maximum MAC Address	The maximum MAC address for dynamically generated MAC addresses. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.

Software.NetworkServer Attributes

The Software.NetworkServer family includes the following attributes that corresponds to the app_netsvr extension table:

Object Name	Label	Description
DeviceAssetNumber	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
DeviceBiosSystemID	Device BIOS System ID	The identifier reported from the BIOS for the device.
DeviceDnsName	Device DNS Name	The fully qualified DNS name of the device.

Object Name	Label	Description
DeviceSysName	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.
DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.
DeviceMacAddress	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
DeviceIPV4Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4AddressWithDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
DeviceIPV6Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).
DeviceIPV6AddressWithDomain	Device IPV6 Address With Domain	An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
ProcessID	Process ID	The PID of the running software, as defined by the operating system. This value is important to distinguish between multiple running instances of the same ProvisionedSoftware.
AccessedViaTcpPort	Accessed Via TCP Port	The TCP port number to use when communicating with the software.
ProcessDistinguishingID	Process Distinguishing ID	A string providing an additional identifier/distinguisher for RunningSoftware when the ProcessID and TCP port data are not available or are not sufficient to distinguish the instances (for example, for an Application where little information can be discovered via the current access mechanisms).
Protocol	Protocol	Defines the protocol supported by the NetworkServer - such as DHCP and DNS.
ContextID	Context ID	The ContextID element is used for identification.

Software.ResourceServer Attributes

The Software.ResourceServer family includes the following attributes that corresponds to the app_ressvr extension table:

Object Name	Label	Description
DeviceAssetNumber	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
DeviceBiosSystemID	Device BIOS System ID	The identifier reported from the BIOS for the device.
DeviceDnsName	Device DNS Name	The fully qualified DNS name of the device.
DeviceSysName	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.
DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.
DeviceMacAddress	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
DeviceIPV4Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4AddressWithDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
DeviceIPV6Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).
DeviceIPV6AddressWithDomain	Device IPV6 Address With Domain	An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
ProcessID	Process ID	The PID of the running software, as defined by the operating system. This value is important to distinguish between multiple running instances of the same ProvisionedSoftware.
AccessedViaTcpPort	Accessed Via TCP Port	The TCP port number to use when communicating with the software.
ProcessDistinguishingID	Process Distinguishing ID	A string providing an additional identifier/distinguisher for RunningSoftware when the ProcessID and TCP port data are not available or are not sufficient to distinguish the instances (for example, for an Application where little information can be discovered via the current access mechanisms).

capabilities	capabilities	A comma-separated list of the capabilities of the Server.
ContextID	Context ID	The ContextID element is used for identification.

Software.VirtualManager Attributes

The Software.VirtualManager family includes the following attributes that corresponds to the app_virmgr extension table:

Object Name	Label	Description
DeviceAssetNumber	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
DeviceBiosSystemID	Device BIOS System ID	The identifier reported from the BIOS for the device.
DeviceDnsName	Device DNS Name	The fully qualified DNS name of the device.
DeviceSysName	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.
DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.
DeviceMacAddress	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
DeviceIPV4Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4AddressWithDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
DeviceIPV6Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).
		An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").

Object Name	Label	Description
DeviceIPV6AddressWithDomain	Device IPV6 Address With Domain	
ProcessID	Process ID	The PID of the running software, as defined by the operating system. This value is important to distinguish between multiple running instances of the same ProvisionedSoftware.
AccessedViaTcpPort	Accessed Via TCP Port	The TCP port number to use when communicating with the software.
ProcessDistinguishingID	Process Distinguishing ID	A string providing an additional identifier/distinguisher for RunningSoftware when the ProcessID and TCP port data are not available or are not sufficient to distinguish the instances (for example, for an Application where little information can be discovered via the current access mechanisms).
ApiVersion	API Version	The version identifier for the APIs applicable to the Manager.
ContextID	Context ID	The ContextID element is used for identification.

Software.Website Attributes

The Software.Website family includes the following attributes that corresponds to the app_website extension table:

Object Name	Label	Description
DeviceAssetNumber	Device Asset Number	Number or other designator assigned to hardware by asset management, often the finance department, that is used for tracking ownership of the resource.
DeviceBiosSystemID	Device BIOS System ID	The identifier reported from the BIOS for the device.
DeviceDnsName	Device DNS Name	The fully qualified DNS name of the device.
DeviceSysName	Device System Name	The system name of the device, as defined in the system block of SNMP's MIB-II. Other information (than the MIB-II sysName) should NOT be used for this element.
DevicePhysSerialNumber	Device Physical Serial Number	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component.

Object Name	Label	Description
DeviceMacAddress	Device MAC Address	A MAC address for the entity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
DeviceIPV4Address	Device IPV4 Address	An IPv4 address for the device. The address is expressed using typical dotted decimal notation (4 groups of up to 3 decimal digits, separated by periods).
DeviceIPV4AddressWithDomain	Device IPV4 Address With Domain	An IPv4 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
DeviceIPV6Address	Device IPV6 Address	An IPv6 address for the device. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons).
DeviceIPV6AddressWithDomain	Device IPV6 Address With Domain	An IPv6 address for the device, prefixed by a contextual domain name, where the domain name is separated from the address by a dash ("-").
IsHAEnabled	Is HA Enabled	Boolean indicating whether the group (typically a Cluster instance or a GroupType="ResourceCluster") supports high availability/failover (if true) or not (if false).
IsMonitoringMembers	Is Monitoring Members	Boolean indicating whether the group (typically a Cluster instance or a GroupType="ResourceCluster") currently is using a heartbeat or other individual monitoring technique to determine if availability is lost (if true) or whether this capability does not exist or is not currently enabled (if false).
MaxFailures	Max Failures	Number of failures that can be supported by the Group, by sparing or other load balancing means.
MemberCriteria	Member Criteria	Defines a comma-separated list of QNames, representing the constraints on the constituency of the Group. Instances referenced as the Target element in the HasMember relationship semantic should have one of the types specified.
GroupType	Group Type	An enumerated value describing the primary type or category of the Group, such as an "authorization group", a "virtual resource pool" or a "data center".
HomePage	Home Page	The URL of the web site's home page.
BusinessRelevance	Business Relevance	Description of the relevance of the Entity, to the business.

J2EE Conventions

CA CMDB includes the following families of Software CIs:

- Software.COTS extension: ci_app_ext

- Software.Application extension: ci_app_ext
- Software.Application Server extension: ci_app_ext
- Software.Bespoke extension: ci_app_ext
- Software.In-House extension: ci_app_inhouse
- Software.Database extension: ci_database
- Software.Operating System extension: ci_operating_system

The existing CA CMDB/CA Cohesion ACM integration uses the family Software.COTS for all software CIs including both J2EE applications and J2EE application servers. Software CIs are reconciled by their system_name attribute which is composed in the following format:

HostName|AppName|Version|Qualifier

In addition, these CIs are named using a similar format:

AppName|Version|Qualifier

Families, Classes, and Reconciliation for J2EE

The following reconciliation considerations apply if you use J2EE Application or J2EE Application Server CIs:

- If you have J2EE Application and Application Server CIs, and you do *not* have CA Wily products or other MDR sources for J2EE CIs, you can use your existing reconciliation strategy. CA Cohesion ACM provides an export capability that you can customize to behave in its original mode.
- If you intend to use CA Wily products, and you already have CIs discovered by CA Cohesion ACM, you can write a script to mark your existing J2EE CIs as Inactive. Then the CIs can be rediscovered using the new CA CMDB integrations.

For future integrations with CA CMDB, use the following Families, Classes, and reconciliation key for J2EE Application CIs:

Objects	Values
Family	Software.Application
Extension	ci_app_ext
Class	Application
Attributes	Category and Type **Note:** These attributes distinguish J2EE applications from other kinds of applications.
Reconciliation attributes /key	Name: AppName|Port system_name: HostName|AppName|Port

For future integrations with CA CMDB, use the following Families, Classes, and reconciliation key for J2EE Application Server CIs:

Objects	Values
Family	Software.Application Server
Extension	ci_app_ext
Class	Application Server
Attributes	Category and Type **Note:** These attributes distinguish J2EE applications from other kinds of applications.
Reconciliation attributes /key	Name: *Host*Name|Port system_name: HostName|Port

Storage Area Network (SAN) Families

Contents

The Storage Area Network (SAN) families include the following:

- **SAN.Interface**
  Identifies a fiber channel interface, similar to a network interface card, used in a SAN fabric.
- **SAN.Switch**
  Identifies a fiber channel switch, similar to a network switch, used in a SAN fabric.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name	Description
SAN. Interface	Interface	net_nicx	ci_network_nic	Interface to a SAN
SAN.Switch	Hub	net_hubx	ci_network_hub	Hub on a SAN
SAN.Switch	Switch	net_hubx	ci_network_hub	Switch on a SAN

SAN.Interface Attributes

The SAN.Interface family includes the following attributes that correspond to the net_nicx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
addr_class	Address Class	IP address values are arranged in Address Classes (A, B, and C). The Address Classes determine how many workstations can exist on the network.
gateway_id	Gateway ID	The unique identifier for a network point that acts as an entrance (gateway) to another network

Object Name	Label	Description
ip_mgmt_addr	Management IP Address	The IP address assigned to a station (PC or workstation) that is authorized for either manager- or operator-level access to a switch.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
line_speed	Line Speed	The rate at which information is transmitted on a network connection.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
number_net_card	Number of Network Cards	The number of expansion cards that have been installed in the available slots in a computer.
number_net_port	Number of Network Ports	The total number of ports in use on a server.
number_net_port_conn	Number of Network Port Connections	The total number of ports on a server.
number_ports	Number of Ports	The total number of ports on a network device.
number_ports_used	Number of Ports Used	The total number of ports in use on a network device.
os_version	OS Version	The version number of a CI's operating system.
protocol	Protocol	The communication method employed by a network device.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
role	Role	The business function supported by a hardware or network device, for example, production, test.
subnet_mask	Subnet Mask	The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address, for example, 255.128.0.0.
technology	Technology	The technology (TCP/IP, Ethernet, FDDI, and so on) employed by a hardware or network device.
type_net_conn	Type of Network Connection	An indication of the kind of network connection used by a hardware or network device.

SAN.Switch Attributes

The SAN.Switch family includes the following attributes that correspond to the net_hubx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
addr_class	Address Class	IP address values are arranged in Address Classes (A, B, and C). The Address Classes determine how many workstations can exist on the network.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and son on, of a CI or group of CIs.
gateway_id	Gateway ID	The unique identifier for a network point that acts as an entrance (gateway) to another network
ip_mgmt_addr	Management IP Address	The IP address assigned to a station (PC or workstation) that is authorized for either manager- or operator-level access to a switch.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_effective_date	Lease Effective Date	The date on which a lease begins.
leased_or_owned_status	Leased or Owned	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.

Object Name	Label	Description
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
number_net_card	Number of Network Cards	The number of expansion cards that have been installed in the available slots in a computer.
number_net_port	Number of Network Ports	The total number of ports in use on a server.
number_net_port_conn	Number of Network Port Connections	The total number of ports on a server.
number_ports	Number of Ports	The total number of ports on a network device.
number_ports_used	Number of Ports Used	The total number of ports in use on a network device.
os_version	OS Version	The version number of a CI's operating system.
priority	Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
project code	Project Code	
protocol	Protocol	The communication method employed by a network device.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
role	Role	The business function supported by a hardware or network device, for example, production, test.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
subnet_mask	Subnet Mask	The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address, for example, 255.128.0.0.
technology	Technology	The technology (TCP/IP, Ethernet, FDDI, and so on) employed by a hardware or network device.
type_net_conn	Type of Network Connection	An indication of the kind of network connection used by a hardware or network device.

Telecom Families

Contents

- Telecom.Wireless Attributes (see page 4283)
- Telecom.Radio Attributes (see page 4285)
- Telecom.Voice Attributes (see page 4287)

The Telecom families include the following:

- **Telecom.Circuit**
  Identifies a dedicated connection between two nodes of a telecommunications network.

- **Telecom.Other**
  Identifies miscellaneous telecom components.

- **Telecom.Radio**
  Identifies an RF receiver or transmitter.

- **Telecom.Voice**
  Identifies a multiplexed connection supporting multiple voice lines on the same circuit.

- **Telecom.Wireless**
  Identifies telecom devices that do not rely on land lines, such as mobile or cellular phones, or wireless handsets or headsets.

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name
Telecom.Circuit	Communication Circuit	tel_cirx	ci_telcom_circuit
Telecom.Circuit	Other Telecom Circuit	tel_cirx	ci_telcom_circuit
Telecom.Circuit	Satellite Link	tel_cirx	ci_telcom_circuit
Telecom.Other	ACD	tel_othx	ci_telcom_other
Telecom.Other	IVR	tel_othx	ci_telcom_other
Telecom.Other	Other Telecom	tel_othx	ci_telcom_other
Telecom.Other	PDA	tel_othx	ci_telcom_other
Telecom.Other	Video Conferencing Unit	tel_othx	ci_telcom_other
Telecom.Radio	Other Telecom Radio	tel_radx	ci_telcom_radio
Telecom.Radio	Radio Data Modem	tel_radx	ci_telcom_radio
Telecom.Radio	Radio Handsets	tel_radx	ci_telcom_radio
Telecom.Voice	Centrex	tel_voix	ci_telcom_voice
Telecom.Voice	Conference Bridge Line	tel_voix	ci_telcom_voice
Telecom.Voice	Desk Phone	tel_voix	ci_telcom_voice
Telecom.Voice	Other Telecom Voice	tel_voix	ci_telcom_voice
Telecom.Voice	PBX	tel_voix	ci_telcom_voice
Telecom.Voice	Phone Card	tel_voix	ci_telcom_voice
	Mobile Phone	tel_wirx	ci_telcom_wireless

Family	Class	Extension Table / Logical Name	Extension Table / Physical Name
Telecom. Wireless			
Telecom. Wireless	Other Telecom Wireless	tel_wirx	ci_telcom_wireless
Telecom. Wireless	Pager	tel_wirx	ci_telcom_wireless

Telecom.Circuit Attributes

The Telecom.Circuit family includes the following attributes that correspond to the tel_cirx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
bandwidth	Bandwidth	The amount of data that can be carried in a given time period over a wired or wireless communications link. Usually specified as bits per second, KB per second, MB per second, and so on.
carrier	Carrier	A company that provides telecommunication services, such as AT&T, Cingular, Sprint, Verizon, and so on.
circuit_number	Circuit Number	The number issued by the phone company that uniquely identifies a circuit.
circuit_type	Circuit Type	The high-level type designation for a telecommunication circuit.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins.
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
	Leased or Ownedv	An indication of whether a particular CI has been leased for a specific time frame or was purchased.

Object Name	Label	Description
leased_or_owned_status		
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
server_id	Server ID	The name or other unique identifier for a server.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.

Telecom.Other Attributes

The Telecom.Other family includes the following attributes that correspond to the tel_othx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
bandwidth	Bandwidth	The amount of data that can be carried in a given time period over a wired or wireless communications link. Usually specified as bits per second, KB per second, MB per second, and so on.

Object Name	Label	Description
bios_ver	BIOS Version	The version number of the BIOS - the code that's run when a personal computer starts up.
carrier	Carrier	A company that provides telecommunication services, such as AT&T, Cingular, Sprint, Verizon, and so on.
circuit_number	Circuit Number	The number issued by the phone company that uniquely identifies a circuit.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
cpu_type	CPU Type	The type (and speed) of the central processor in a telecom device.
domain	Domain	The identifier of the logical grouping (domain) to which a network or telecom device is assigned.
frequency	Frequency	The wavelength at which a telecom signal is transmitted to a wireless or radio device.
gateway_id	Gateway ID	The unique identifier for a network point that acts as an entrance (gateway) to another network
harddrive_capacity	Hard Drive Capacity	The amount of hard drive capacity that is available for use on a Telecom CI.
harddrive_used	Hard Drive Space Used	The amount of hard drive capacity that is being used.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins.
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Ownedv	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
license_expiration_date	License Expiration Date	The date on which a hardware or software license expires.

Object Name	Label	Description
ci_license_number	CI License Number	The valid license number for a hardware or software CI.
line_id	Line ID	The designation that uniquely identifies a telecommunication line.
main_extension	Main Extension	The primary telephone number for a business.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
memory_available	Memory Available	The amount of memory that is still available for use.
memory_used	Memory Used	The amount of the available memory that is in use.
monitor	Monitor Model	The type of display unit connected to a hardware, network, or telecom device.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
nic_card	NIC Card	Each device (Node) on a network has a Network Interface Card (NIC). The NIC can be Ethernet, Token Ring, RF, or other. The NIC is installed inside the device and provides a real-time dedicated connection to the network.
phone_number	Phone Number	The number issued by the phone company that uniquely identifies a land line or cellular telephone connection.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.

Object Name	Label	Description
retire_date	Retire Date	The date on which a CI is no longer active.
server_id	Server ID	The name or other unique identifier for a server.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
subnet_mask	Subnet Mask	The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address for example, 255.128.0.0.

Telecom.Wireless Attributes

The Telecom.Wireless family includes the following attributes that correspond to the tel_wirx extension table:

Object Name	Label	Description
active_date	Activation Date	The date on which the CI was put into active status.
bandwidth	Bandwidth	The amount of data that can be carried in a given time period over a wired or wireless communications link. Usually specified as bits per second, KB per second, MB per second, and so on.
bios_ver	BIOS Version	The version number of the BIOS - the code that's run when a personal computer starts up.
carrier	Carrier	A company that provides telecommunication services, such as AT&T, Cingular, Sprint, Verizon, and so on.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
cpu_type	CPU Type	The type (and speed) of the central processor in a telecom device.
domain	Domain	The identifier of the logical grouping (domain) to which a network or telecom device is assigned.
frequency	Frequency	The wavelength at which a telecom signal is transmitted to a wireless or radio device.
gateway_id	Gateway ID	The unique identifier for a network point that acts as an entrance (gateway) to another network
harddrive_capacity	Hard Drive Capacity	The amount of hard drive capacity that is available for use on a Telecom CI.
harddrive_used	Hard Drive Space Used	The amount of hard drive capacity that is being used.
		The latest date on which maintenance was performed on a CI.

Object Name	Label	Description
last_mtce_date	Last Maintenance Date	
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins.
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Ownedv	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
license_expiration_date	License Expiration Date	The date on which a hardware or software license expires.
ci_license_number	CI License Number	The valid license number for a hardware or software CI.
line_id	Line ID	The designation that uniquely identifies a telecommunication line.
main_extension	Main Extension	The primary telephone number for a business.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
memory_available	Memory Available	The amount of memory that is still available for use.
memory_used	Memory Used	The amount of the available memory that is in use.
monitor	Monitor Model	The type of display unit connected to a hardware, network, or telecom device.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.

Object Name	Label	Description
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
nic_card	NIC Card	Each device (Node) on a network has a Network Interface Card (NIC). The NIC can be Ethernet, Token Ring, RF, or other. The NIC is installed inside the device and provides a real-time dedicated connection to the network.
phone_number	Phone Number	The number issued by the phone company that uniquely identifies a land line or cellular telephone connection.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
subnet_mask	Subnet Mask	The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address for example, 255.128.0.0.

Telecom.Radio Attributes

The Telecom.Radio family includes the following attributes that correspond to the tel_radx extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
bandwidth	Bandwidth	The amount of data that can be carried in a given time period over a wired or wireless communications link. Usually specified as bits per second, KB per second, MB per second, and so on.
bios_ver	BIOS Version	The version number of the BIOS - the code that's run when a personal computer starts up.
	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.

Object Name	Label	Description
contract_number		
cpu_type	CPU Type	The type (and speed) of the central processor in a telecom device.
domain	Domain	The identifier of the logical grouping (domain) to which a network or telecom device is assigned.
frequency	Frequency	The wavelength at which a telecom signal is transmitted to a wireless or radio device.
gateway_id	Gateway ID	The unique identifier for a network point that acts as an entrance (gateway) to another network
harddrive_capacity	Hard Drive Capacity	The amount of hard drive capacity that is available for use on a Telecom CI.
harddrive_used	Hard Drive Space Used	The amount of hard drive capacity that is being used.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins.
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Ownedv	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
license_expiration_date	License Expiration Date	The date on which a hardware or software license expires.
ci_license_number	CI License Number	The valid license number for a hardware or software CI.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.

Object Name	Label	Description
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.
memory_available	Memory Available	The amount of memory that is still available for use.
memory_used	Memory Used	The amount of the available memory that is in use.
monitor	Monitor Model	The type of display unit connected to a hardware, network, or telecom device.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
nic_card	NIC Card	Each device (Node) on a network has a Network Interface Card (NIC). The NIC can be Ethernet, Token Ring, RF, or other. The NIC is installed inside the device and provides a real-time dedicated connection to the network.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.
subnet_mask	Subnet Mask	The identifier of the subnet into which a CI falls. Expressed in the same format as an IP address for example, 255.128.0.0.

Telecom.Voice Attributes

The Telecom.Voice family includes the following attributes that correspond to the tel_voix extension table:

Object Name	Label	Description
active_date	Active Date	The date on which the CI was put into active status.
carrier	Carrier	A company that provides telecommunication services, such as AT&T, Cingular, Sprint, Verizon, and so on.
circuit_number	Circuit Number	The number issued by the phone company that uniquely identifies a circuit.
contract_number	Contract Number	The unique identifier for a legal contract covering the purchase, lease, warranty, maintenance, and so on, of a CI or group of CIs.
cpu_type	CPU Type	The type (and speed) of the central processor in a telecom device.
harddrive_capacity	Hard Drive Capacity	The amount of hard drive capacity that is available for use on a Telecom CI.
harddrive_used	Hard Drive Space Used	The amount of hard drive capacity that is being used.
last_mtce_date	Last Maintenance Date	The latest date on which maintenance was performed on a CI.
lease_cost_per_month	Monthly Lease Cost	The dollar amount owed to the vendor each month for a lease.
lease_effective_date	Lease Effective Date	The date on which a lease begins.
lease_renewal_date	Lease Renewal Date	The date on which a lease must be renewed for the next time period, or the affected CIs must be returned to the vendor.
lease_termination_date	Lease Termination Date	The date on which a lease ends and the affected CIs must be returned to the vendor.
leased_or_owned_status	Leased or Ownedv	An indication of whether a particular CI has been leased for a specific time frame or was purchased.
main_extension	Main Extension	The primary telephone number for a business.
maintenance_fee	Maintenance Fee	The amount of money paid to cover the cost of maintenance services over a specified time period.
maintenance_period	Maintenance Period	The time frame for which a maintenance contract is active.

Object Name	Label	Description
memory_available	Memory Available	The amount of memory that is still available for use.
memory_used	Memory Used	The amount of the available memory that is in use.
monitor	Monitor Model	The type of display unit connected to a hardware, network, or telecom device.
mtce_contract_number	Maintenance Contract Number	The number that uniquely identifies a maintenance contract.
mtce_level	Maintenance Level	An indication of the current patch version for this CI.
mtce_type	Maintenance Type	The kind of maintenance that is provided for this CI, for example, vendor or in-house.
network_address	Network Address	The IP address at which this CI resides, for example, 192.168.0.4.
network_name	Network Name	The unique name or identifier for a communications system that connects two or more computers and their peripheral devices.
nic_card	NIC Card	Each device (Node) on a network has a Network Interface Card (NIC). The NIC can be Ethernet, Token Ring, RF, or other. The NIC is installed inside the device and provides a real-time dedicated connection to the network.
phone_number	Phone Number	The number issued by the phone company that uniquely identifies a land line or cellular telephone connection.
ci_priority	CI Priority	The service level designation that is assigned to indicate the priority for restoration of this CI.
proj_code	Project Code	The ID or other unique identifier for the project to which a CI is assigned.
purchase_amountc	Purchase Amount	The cost incurred to buy a CI.
retire_date	Retire Date	The date on which a CI is no longer active.
SLA	Service Level Agreement	The name or identifier of the contract between IT and the customer that governs the level of service and support options that are expected and acceptable for this IT component.

General Resource Loader - GRLoader

Contents

GRLoader Considerations

Review the following considerations before you use GRLoader:

- GRLoader Release 12.9 is compatible with earlier releases of CA CMDB, but early releases of GRLoader are incompatible with CA CMDB Release 12.9. For example, a site has an existing CA CMDB r11.2 installation and later installs CA CMDB Release 12.9, so the site has two installations. GRLoader Release 12.9 works with both installed systems, but GRLoader r11.2 only works with the r11.2 installation. You can use the - s parameter to specify which one of the multiple installations for GRLoader to use.

- We recommend that you migrate all your MDR scripts to use the latest version of GRLoader. If you want to insert new CIs, migration requires altering existing scripts to specify -n.

  Note: If you do not specify -n or -a, GRLoader does not insert or update CIs and relationships.

- You can specify GRLoader options in a configuration file.

- Whenever you update a CI with the -a option, Last Change Date and user displayed in the Configuration Item List are updated even if no attributes were changed. This update occurs whether a CI was edited in the user interface (and saved without changes) or updated by using GRLoader.

- If GRLoader generates a warning, the error log records the CI information, an error, or a skip. For example, when GRLoader loads CIs, but -a is not specified to allow updates, the information appears in the error log with an appropriate message.

- When you run GRLoader from a batch file, specify the *-ad attr=value* as *-ad attr{value}* to get past the Windows command parser which may remove the equal "=" symbols.

- Do *not* use curly brackets "{ }" as work area delimiter characters when you want GRLoader to insert CIs into the CMDB. TWA delimiters work properly when inserting CIs from general notes, CSV and Excel files, and JDBC/ODBC databases.

- GRLoader does not support smart quotes. Use double quote characters, or any other single character delimiter instead.

- GRLoader does not let you create NULL or empty relationships between CIs. The CA SDM web interface lets you create these relationships, but GRLoader displays the *ERROR:Relationship type is required* message in the generated error XML file.

- GRLoader does not let you create duplicate relationships between the same two CIs. Instead, GRLoader tries to update the existing relationship between the same two CIs that have the same relationship type.
  For example, the CMDB contains a relationship such as *ci_1 manages ci_2*. When you try to insert the same relationship through GRLoader, the utility tries to update the existing relationship, instead of creating a new relationship. The CA SDM web interface lets you create a duplicate relationship between the same two CIs, or update the existing relationship.

- You cannot use the *SELECT ** syntax on UNIX systems.

Use Database Queries to Verify Correct Data

We recommend that you use database queries before executing GRLoader. These queries help you debug imports to SQL Server. For example, you want to specify Server as the class in your SQL statement.

Follow these steps:

1. Create a configuration file named sqlServer.cfg with the following code:

```
grloader.jdbc.driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
grloader.jdbc.url=jdbc:sqlserver://sqlserverhostname:1433;databaseName=mdb;
grloader.jdbc.user=userid
grloader.jdbc.password=password
```

2. Save the file.

3. Execute the following query in SQL Server:

```
select ca_owned_resource.resource_name as name,
       ca_resource_class.name as class
       from ca_owned_resource, ca_resource_class
       where ca_owned_resource.resource_class = ca_resource_class.id
```

   The query executes successfully because you specified the correct class name.

4. Open GRLoader.

5. Execute the following command:

```
GRLoader -cfg sqlserverdb.cfg -u userid -p password -E -s http://sdmhostname:
8080 -E -dbstmt "select ca_owned_resource.resource_name as name,
ca_resource_class.name as class from ca_owned_resource, ca_resource_class where
ca_owned_resource.resource_class = ca_resource_class.id" -a -e "c:\errorjdbc1.
xml"
```

   The data is imported.

The GRLoader Command

The General Resource Loader (GRLoader) imports CI information into CA SDM. GRLoader uses XML documents as input, which lets you import data that originates in different data sources. Run GRLoader from a command prompt or by using a .bat or .cmd file. The CA SDM installation adds the GRLoader to the path during installation, so it runs from any directory.

Results from an import show counts for all processed CIs and Relationships, including the amount of Read, Skipped, Inserts, Updates, Errors, and Warnings. GRLoader logs all processing details and errors in the *nx_root*/log/grloader.log file, where *nx_root* specifies the CA SDM installation directory.

Syntax

```
C:\WINDOWS>GRLoader -?
```

The GRLoader command uses the following parameters:

- **-u *userid***
  (Required) Specifies the user ID that runs the GRLoader process.

- **-p *password***
  (Required) Specifies the password for the user ID. If you run GRLoader without the -p parameter, the utility prompts the console for the password.

- **-s http[s]://*cmdb_servername*:*port***
  (Required) Specifies the server URL including the port number that runs the web services. For running GRLoader on the primary server or application server in a default installation, you can use the following command:

  ```
  -s http://localhost:8080
  ```

  Note: If you specify the optional -C parameter, GRLoader ignores the -s parameter.

- **-i *input_file***
  (Required) Specifies a full path name or a relative path name. If the filename contains a .xls or .xlsx suffix, GRLoader considers the file as a spreadsheet, otherwise it considers it as an XML file.

- **-n**
  (Optional) Allows new CI insertion into the CMDB. Without -n, CIs write to the XML error file (see the -e parameter). Relationships are only added if either -n or -a is specified. If neither is specified, no updates are performed. Updating CIs also require the -a parameter.

- **-a**
  (Optional) Allows updates to configuration items (by default, updates are not allowed if the CI exists in the CMDB). The -n flag also is required to add new CIs.

- **-D**
  (Optional) Specifies a name prefix for relations (defaults to "GRLoader"). Use the prefix for the sym field in new relationships. The sym file must be unique, so a datetime field and a number is appended to this prefix to make it unique.
  Default Prefix: GRLoader.

- **-e *XML_err_file***
  (Optional) Produces an XML error file when GRLoader detects errors or warnings. By default, the error file name uses the name of the input file, appended with _err.xml. For example, using the input file as abc.xml creates the error file as abc_err.xml. Use the -e parameter to override this default name.

- **-E**
  (Optional) Lets you overwrite the XML error file. By default, the error file is not overwritten.

- **-l**
  (Optional) Ignores case. When you use this parameter, GRLoader is not case-sensitive when comparing the input value of a lookup field with the actual value stored in the database. By default, lookups are case-sensitive.

- **-ua**
  Always updates the CMDB.

- **-lftwa [-chg *nnnn*]**
  (Optional) Loads TWA transactions into the CMDB. If used with -chg, the load selects only those transactions associated with change order *nnnn*.

  
  Note: The Change Order string is not validated when loaded into the CMDB.

- **-lftwai [-chg *nnnn*]**
  (Optional) Runs TWA transactions to update the CMDB. Transactions that run successfully are set to Inactive so that they do not appear in lists. If you use -chg, the load selects only those transactions associated with change order *nnnn*.

- **-lttwa**
  (Optional) Loads XML into the transaction work area (TWA) instead of directly into the CMDB. After data has been loaded into the TWA, it can be edited, changed and verified. After the data modification process completes, individual transactions can load into the CMDB (see - lftwa).

- **-lttwar**
  (Optional) Loads XML into the initial state in the transaction work area (TWA) instead of directly into the CMDB. Transaction data in the TWA can be edited, changed, and verified (see -simci and -simrel). After the data modification process completes, individual transactions can load into the CMDB (see - lftwai).

- **-nospinner (-spinner)**
  (Optional) Turns off the spinner that displays CI and relationship progress. Use -spinner to enable the progress display.

- **-P**
  (Optional) Specifies preload data to improve performance for large processing. For large input files, supplying the - P parameter preloads a few tables into memory so that they can be processed more quickly. For smaller inputs (< 50 entries), preload is not necessary.

- **-rs**
  (Optional) Replaces symbolic values that CA SDM includes in the XML input file. If you enable this parameter, corresponding values replace the following symbolic values:

  - *now* -- Replaced by a unique date/time string appended with a sequence number to help ensure uniqueness.
  - *userid* -- Indicates the userid specified in the -u parameter.
  - *inputfile* -- Indicates the filename specified in the -I parameter.
  - *relationcount* -- Specifies the number of relationships processed so far in this GRLoader run.
  - *lastciuuid* -- Specifies the UUID of the most recently processed CI.
  - *cicount* -- Specifies the number of CIs processed so far in this GRLoader run.

Examples: Use the -rs Parameter

With -rs enabled, the following example creates 100 CIs named ci1, ci2, …, ci100

```
<GRLoader>
<ci><name>ci*cicount*</name><class>Server</class></ci>
[...repeated 100 times...]
</GRLoader>
```

With -rs enabled, the following example updates the CI description with information about the most recent update.

```
<GRLoader>
<ci>
<name>server1</name>
<description>updated by *userid* on *now* using input file *inputfile*</description>
</ci>
</GRLoader>
```

- **-simci**
  (Optional) Simulates CI operations to predetermine whether a set of transactions creates CIs, and therefore possible ambiguities for other CIs.

- **-simrel**
  (Optional) Simulates relationship operations to predetermine whether a relationship transaction creates a relationship or updates a relationship.

- **-T *trace_level***
  (Optional) Specifies the tracing level. Known tracing levels are 0 (off, the default), 1 (low), 5 (medium) and 10 (verbose). We recommend only using this setting when necessary because much output can result.

- **-tf *filename***
  (Optional) Runs GRLoader using translation rules. *filename* specifies the name of the file that contains the translation rule set.

- **-slump**
  (Optional) Specifies the slump.jar file. This parameter can provide better performance than web services. **Important:** -slump only can be used with the -s parameter to target the following server:

  - Conventional: Primary server
  - Advanced Availability: Application server.

  Note: If another CA product is installed, for example, CA Coheshion ACM or CMDB service pack is installed, verify that the slump.jar file is identical to the one that is installed on the target CA SDM system.

- **-C**
  (Optional) Validates the XML input file without any additional processing. This argument only validates the XML tags, not field values.

- **-h (or -?)**
  (Optional) Displays online help.

- **-v**
  (Optional) Displays the GRLoader product version and build date.

- **-maxerror *number***
  (Optional) Specifies the maximum number of errors that can occur before remaining CIs or relationships are skipped.

- **-maxwarn *number***
  (Optional) Specifies the maximum number of warnings that can occur before remaining CIs or relationships are skipped.

- **-chg *nnnn***
  Used with - lftwa and -lftwar. Loads only those transactions associated with change order *nnnn*.

  Note: The Change Order string is not validated when loaded into the CMDB.

- **-cfg *myconfigfile*.cfg**
  (Optional) Specifies the name of the input configuration file.

- **-dt t*enant***
  (Optional) Specifies the tenant assignment for the CI/relationship. You must enable multi-tenancy to use this parameter. You can use PUBLIC to indicate that the object is public. If the tenant access of the user does not authorize creating public objects, the object is created using the default tenant.

- **-sc classname**

  Lists the attributes of CIs in the class you specify.

- **-scx classname**

  Lists the attributes of CIs in the class you specify in XML format. The XML is stored in a file named classname.xml. Any special characters are removed from the class name.

Example: Load CI and Relationship Data

The following example loads the CI and relationship data contained in the filehardware_servers.xml (in the current directory) into the CMDB that resides on the server located on the local computer on port 8080.

```
grloader -u CMDBAdmin -p password -s http://localhost:8080 -i hardware_servers.xml -n
```

Input Options

Contents

JDBC Database Input Options

The following table lists the options that you use in the configuration file and the corresponding command line options when you input JDBC databases.

Note: If you use SQL Server or Oracle databases, CA SDM includes the required JAR files. If you use other database types, you must use the -addjar option to add support for those databases to GRLoader dynamically. Consult your database vendor documentation for the name and location of the necessary JAR files to use JDBC. You can also consult your database vendor or database administrator for specific values and credentials.

GRLoader Option	Command Line Option	Description
grloader.jdbc.driver=*name*	-dbdriver *name*	Specifies the JDBC driver name. **Note:** This driver must be available on the classpath, similar to -addjar. Consult the database vendor for specific values.
grloader.jdbc.url=*URL*	-dburl *URL*	Specifies the JDBC database URL that describes the location of the database which contains the table you want to load.
grloader.jdbc.user=*name*	-dbuser *name*	Specifies the user ID for the JDBC database.
grloader.jdbc.password=*password*	-dbpswd *password*	Specifies the password for the user ID for the JDBC database.
grloader.jdbc.statement=*statement*	-dbstmt *statement*	Specifies the JDBC statement that describes the columns and selection criteria for the data you want to import. **Note:** The column names used in the query statement must match CMDB attribute names. If these names differ, use the SQL *AS* keyword to map database column names to CMDB attributes.

Spreadsheet Input Options

The following table lists the options that you use in the configuration file and the corresponding command line options when you input spreadsheets. You can also usethe {} symbols as delimiters surrounding the lookup field as well as using the keyword EMPTY.

- **boolean**
  Specifies a value from one the following pairs: 1/0, YES/NO, or TRUE/FALSE.

Note: If the input file name ends in .xls or .xlsx when you use the *grloader.inputfile=name* GRLoader option or the *-i* command line argument, GRLoader assumes that it is a spreadsheet.

GRLoader Option	Command Line Option	Description
grloader.spreadsheet.filename=*name*	-ssf	Specifies the Excel spreadsheet file name when it does not contain the .XLS or .XLSX file extension.
grloader.spreadsheet.sheetname=*name*	-sss	Specifies the sheet name. **Default:** The first sheet in the spreadsheet.
grloader.spreadsheet.firstrow=*n*	-ssfr	Set this value to skip over the first *n-1* rows in the spreadsheet.
grloader.spreadsheet.lastrow=*n*	-sslr	Ignores *rows> n (greater than)* in the spreadsheet.
grloader.spreadsheet.firstcol=*x*	-ssfc	Specifies to start processing on this column. You can express this column as a letter or number, depending on your spreadsheet options.
grloader.spreadsheet.lastcol=*x*	-sslc	Ignores *columns > x (greater than)* in the spreadsheet. You can express this column as a letter or number, depending on your spreadsheet options.
grloader.spreadsheet.embeddedseparator	-sses	Specifies a character to separate multiple values contained in a single cell. This option only applies to the relationship type column in a row with multiple embedded relationships. **Default:** semi-colon ":"
grloader.attributedefault.atrname=*value*	-ad attrname=*value*	Provides a default value if you did not specify one in the input source. **Note:** These values do not undergo attribute name or data value translation. **Note:** When you run GRLoader from a batch file, specify the *-ad attr=value* as *-ad attr{value}* to get past the Windows command parser which may remove the equal "=" symbols.

GRLoader Option	Command Line Option	Description
	-dt	Deprecated. Instead, use the -ad tenant=*name* option.
grloader.maxci=*n*	-maxci	Specifies the maximum number of CIs to import before skipping further CI imports.
grloader.maxrel=*n*	-maxrel	Specifies the maximum number of relationships to import before skipping further relationship imports.
N/A	-sc *classname*	Lists the attirbutes of CIs in the class you specify.
N/A	-scx *classname*	Lists the attributes of CIs in the class you specify in XML format.
grloader.workarea.changeorderrequired=*boolean*	-cor	If set to yes, TWA transactions that do not contain a non-blank change order number are ignored.
grloader.ignoreinvalidattributes=*boolean*	-iia	Specifies if you want to ignore invalid attributes. This command suppresses all warning messages about invalid attribute names.

CSV Input Options

The following table lists the options that you use in the configuration file and the corresponding command line options when you input CSV files.

Note: If required, consult your database vendor or database administrator for specific values and credentials.

GRLoader Option	Command Line Option	Description
-i		GRLoader assumes that a file ending in .csv is a CSV file.
grloader.csv.filename=*n* *ame*	-csvf *name*	Specifies the filename when it does not end in .csv.
grloader.csv.separator=*x*	-csvsep *x*	Specifies when the CSV file uses other than comma delimiters. You can specify a single character, such as a Tab (\t) or a semicolon.
grloader.csv.escape=*x*	-csvesc *x*	Specifies when the CSV file uses an escape character (\).
grloader.csv.comment=*x*	-csvcom *x*	Specifies when the CSV file uses the comment character (#).
grloader.csv.quote=*x*	-csvquote *x*	Specifies when the CSV file uses the quote character (").

TWA Input Options

The following table lists the options that you use in the configuration file and the corresponding command line options when you input from the TWA.

GRLoader Option	Command Line Option	Description
grloader.workarea.changeorderrequired=yes/no	-cor	GRLoader ignores TWA transactions that do not contain a non-blank Change Order number.

General Options

The following table lists the options that you use in the configuration file and the corresponding command line options when you input from all inputs.

Note: If necessary, consult your database vendor or database administrator for specific values and credentials.

GRLoader Option	Command Line Option	Description
grloader.system.addjar=*xx;yy;zz*	-addjar *xx*	Adds JAR files to the GRLoader classpath. You can use this option with -jdbcdriver. **Note:** The grloader.system.addjar option can only appear once in the configuration file. You can add multiple jars through grloader.system.addjar by separating the filenames with a semi-colon. This option only specifies a single jar file, and you can specify it as many times as required.
grloader.attributedefault.attrname=*value*	-ad attrname=*value*	Provides a default value if you did not specify a value in the input source. **Note:** These values do not undergo attribute name or data value translation. When you run GRLoaderfrom from a batch file, specify -ad attr=value as *-ad attr{value}.* The Windows command parser can delete the equals symbol.
N/A	-ad tenant=*name*	Specifies the tenant name.
grloader.maxci=*n*	-maxci *n*	Specifies the maximum number of CIs to import before skipping further CI imports.
grloader.maxrel=*n*	-maxrel *n*	Specifies the maximum number of relationships to import before skipping further relationship imports.
N/A	-sc *xx*	Lists attributes of CIs in the class *xx*.
N/A	-scx *xx*	Lists attributes of CIs in class *xx* in XML format.
	-aer	

GRLoader Option	Command Line Option	Description
grloader.reader.allowembeddedrelationships=yes/no		Allows embedded relationships. **Default:** Yes For backward compatibility only
grloader.ignoreinvalidattributes=yes/no	-iia	Ignores invalid attributes by suppressing all warning messages about invalid attribute names.
grloader.updatealways=yes/no		

Example Display CI Class Attributes

When you create input for GRLoader, list the attributes associated with a specific class.

To list the attributes, execute the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080 -sc [class name]
```

- **sc**
  Lists attributes of CIs in a class that you specify.
- **class name**
  Specifies any valid CA CMDB class name.

Example: List Attributes for Class Server

```
grloader  - u username  - p password  - s http://sdm-host:8080 -sc Server

10:33:01.997 CI and Relationship Loader for CA Service Desk Manager

List of attributes in class(Server) extension(har_serx)

ATTRIBUTE NAME                    DATA TYPE
acquire_date                      Date
active_date                       Date
alarm_id                          STRING(64)
ambiguity                         Integer
asset_count                       Integer
asset_num                         STRING(64)
audit_userid                      SREL(cnt.combo_name)
```

Example Display CI Class Attributes in XML Format

When you create input for GRLoader, list the attributes associated with a specific class in XML format. The command creates the file [class name].xml with the result.

To list the attributes in XML format, execute the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080 -scx [class name]
```

- **scx**
  Lists attributes of CIs in XML format in a class that you specify.

- **class name**
  Specifies any valid CA CMDB class name.

Example: List Attributes for Class Server

```
grloader  - u username  - p password  - s http://sdm-host:8080 -scx Server

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<GRLoader>
 <ci>
    <acquire_date></acquire_date>                      <!-- Date -->
    <active_date></active_date>                        <!-- Date -->
    <alarm_id></alarm_id>                              <!-- String(64) -->
    <ambiguity></ambiguity>                            <!-- Integer -->
    <asset_count></asset_count>                        <!-- Integer -->
    <asset_num></asset_num>                            <!-- String(64) -->
    <audit_userid lookup="combo_name"></audit_userid>  <!-- SREL cnt -->
```

Note: If the class name contains special characters, they are removed.

Data Error Handling

If GRLoader finds errors, the failing CI or Relation node writes to an error file. We recommend that you edit the XML file to correct the problem, and then run GRLoader against the edited file. The -e parameter lets you name the error file. The -maxerror and -maxwarn parameters let you specify the maximum number of errors or warnings that can occur until GRLoader skips the remaining CIs or relationships.

Consider the following information about error destinations:

- If you use the TWA as the input source, the TWA also becomes the error destination.

- If you use the JDBC database as the input source, $NX_ROOT\log\grloader_err.xml becomes the error destination.

- If you use filename.xls, filename.xlsx, filename.xml, or filename.csv as the input source, filename_err.xml becomes the error destination.

Note: When you troubleshoot errors or you perform simulations, review these files and the standard CA SDM logs.

GRLoader Configuration File

Contents

You can specify GRLoader options in a configuration file. This approach provides the following advantages:

- You no longer enter passwords in the command line.
- The command prompt window (Windows) does not display the password, or in the results of the -ps command (UNIX).
- Standardized commands reduce errors.

Important! We recommend that you keep configuration files in a secure location. Avoid specifying passwords in command lines and use configuration files, especially in Linux and UNIX environments.

The following input specifies the format of the configuration file parameter:

- **-cfg *myconfigfile*.cfg**
  Specifies the name of the input configuration file. You can specify the -cfg parameter at any location in the GRLoader parameter string.

If the command line and the configuration file conflict, GRLoader uses the last value you entered.

Example: Specify a Configuration File

A configuration file command uses the following syntax:

```
GRLoader -cfg myconfigfile.cfg -i myinputfile.xml
```

Instead of specifying the more complex command:

```
GRLoader -u userid -p password -i myinputfile.xml -a -n -E -maxerror 10 -maxwarn 10 -
dt IBM -nomn
```

Example: Last Password Value is Used

The configuration file GRLoader.cfg specifies the following passwords:

```
GRLoader.password=password1
GRLoader.password=password2
```

The command line specifies the following password:

```
GRLoader -p password3 -cfg GRLoader.cfg
```

The password that is used is password2.

If the command line was changed to specify:

```
GRLoader -cfg GRLoader.cfg -p password3
```

The password that is used is password3 because it was the last one specified.

Configuration File Options

The following table lists the GRLoader options that you can use in the configuration file and the corresponding command line options.

- **boolean**
  Specifies a value from one the following pairs: 1/0, YES/NO, or TRUE/FALSE.

GRLoader Option	Command Line Option	Description
grloader.userid=*userid*	-u	Specifies the user name of the administrator.
grloader.password=*password*	-p	Specifies the administrator password.
grloader.server=*server*	-s	Specifies the URL of the CA SDM server.
grloader.inputfile=*name*	-i **Note:** If the input file name ends in .XLS or .XLSX, GRLoader assumes it is a spreadsheet.	Specifies the file you want to import with GRLoader.
grloader.errorfile=*name*	-e	
grloader.nxroot=*name*	-N	
grloader.casesensitive=boolean	-I	
grloader.loadfromtwa=yes	-lftwa [-chg *nnnn*]	
grloader.loadfromtwa.inactivatesuccessful=yes	-lftwai [-chg *nnnn*]	
	-lttwa	

GRLoader Option	Command Line Option	Description
grloader.loadtotwa=yes		
grloader.loadtotwa.ready=yes	-lttwar	
grloader.simulateloadci=boolean	-simci	
grloader.simulateloadrelation=boolean	-simrel	
grloader.emptyvalue=EMPTY		
grloader.workarea.delimiters={ }		Provides alternate lookups for the dependent CI.
grloader.workarea.ignore_transaction_dates=yes		
grloader.normalizemac=boolean	-nm/nonm	
grloader.maxerror=*number*	-maxerror	
grloader.maxwarn=*number*	-maxwarn	
grloader.defaulttenant=*tenant* | PUBLIC	-dt *tenant* | PUBLIC **Note:** The multi-tenancy option must be *setup* or *on* to use these options.	
grloader.allowupdate=boolean	-a	
grloader.allowinsert=boolean	-n	
grloader.overwriteerrorxml=boolean	-E	

GRLoader Option	Command Line Option	Description
grloader.slump=boolean	-slump (primary or application server only)	
grloader.preload=boolean	-P	
grloader.replacesymbols=boolean	-rs	
grloader.translationfile=*filename*	-tf	
grloader.tracelevel=number	-T	
grloader.spinner=boolean	-spinner/-no (equivalent to -nospinner)	
grloader.cmdbversion=11.0	(no equivalent)* *Required for CA CMDB r11.0 only. GRLoader is compatible with all later releases.	
grloader.spreadsheet.filename=*name*	-ssf	Specifies the Excel spreadsheet file name when it does not contain the .XLS or .XLSX file extension.
grloader.spreadsheet.sheetname=*name*	-sss	Specifies the sheet name. **Default:** The first sheet in the spreadsheet.
grloader.spreadsheet.firstrow=*n*	-ssfr	Set this value to skip over the first *n-1* rows in the spreadsheet.
grloader.spreadsheet.lastrow=*n*	-sslr	Ignores *rows> n (greater than)* in the spreadsheet.
grloader.spreadsheet.firstcol=*x*	-ssfc	Specifies to start processing on this column. You can express this column as a letter or number, depending on your spreadsheet options.
grloader.spreadsheet.lastcol=*x*	-sslc	Ignores *columns > x (greater than)* in the spreadsheet. You can express this column as a letter or number, depending on your spreadsheet options.
	-sses	

GRLoader Option	Command Line Option	Description
grloader.spreadsheet.embeddedseparator		Separates multiple values contained in a single cell. This option only applies to the relationship type column in a row with multiple embedded relationships. **Default:** semi-colon ":"
grloader.attributedefault.atrname=*value*	-ad attrname=*value*	Provides a default value if you did not specify one in the input source. **Note:** These values do not undergo attribute name or data value translation. **Note:** When you run GRLoader from a batch file, specify the *-ad attr=value* as *-ad attr{value}* to get past the Windows command parser which may remove the equal "=" symbols.
	-dt	Deprecated. Instead, use the -ad tenant=*name* option.
grloader.maxci=*n*	-maxci	Specifies the maximum number of CIs to import before skipping further CI imports.
grloader.maxrel=*n*	-maxrel	Specifies the maximum number of relationships to import before skipping further relationship imports.
N/A	-sc *classname*	Lists the attributes of CIs in the class you specify.
N/A	-scx *classname*	Lists the attributes of CIs in the class you specify in XML format.
grloader.workarea.changeorderrequired=*boolean*	-cor	If set to yes, TWA transactions that do not contain a non-blank change order number are ignored.
grloader.ignoreinvalidattributes=*boolean*	-iia	Specifies if you want to ignore invalid attributes. This command suppresses all warning messages about invalid attribute names.

Note: If the input file name ends in .xls or .xlsx when you use the grloader.inputfile=name GRLoader option or the -i command line argument, GRLoader assumes that it is a spreadsheet.

GRLoader XML

This article contains the following topics:

GRLoader requires XML document input that consists of a document header followed by enclosing <GRLoader> XML elements tags with one or more <ci> tags (for CI definitions) or <relation> tags (for relationships).

Specify the XML document header as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
```

Update the encoding attribute as needed to handle the appropriate character encoding requirements. For example, specify “ISO-8859-1” to handle special Norwegian characters.

Example: Format a GRLoader XML File

The following template presents the format for a GRLoader XML file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<GRLoader>

<ci>
[define a CI: common and family-specific attributes, versioning, reconciliation, MDR]
</ci>
[repeat as necessary for each CI]

<relation>
        <type>relationship_type</type>
        <delete_flag>active_state</delete_flag>
        <provider>
                <name>resource name</name>
                <serial_number>serial number</serial_number>
                <system_name>host name</system_name>
                <asset_num>resource tag</asset_num>
                <mac_address>mac address</mac_address>
                <dns_name>dns name</dns_name>
                <id>ci_uuid</id>
        </provider>
        <dependent>
                <name>resource name</name>
                <serial_number>serial number</serial_number>
                <system_name>host name</system_name>
```

```
                <asset_num>resource tag</asset_num>
                <mac_address>mac address</mac_address>
                <dns_name>dns name</dns_name>
                <id>ci_uuid</id>
        </dependent>
</relation>
[repeat as necessary for each relationship]
</GRLoader>
```

XML Content The CI Tag

GRLoader uses the CI XML definition to load a CIs attribute values and relationships. The CI definition must include a minimum set of required attributes to be created or updated by using *<ci>* XML element tags.

You define the XML for a CI by specifying values for the following attributes:

- Class identification (required)
- Reconciliation attributes (required)
- Common attributes
- Family-specific attributes
- MDR identification attributes
- Versioning attributes

The CI Tag Family and Class Identification

Class identification must be specified for each CI to associate the proper family and class with the CI.

Specify the family and class attributes using the following XML tags:

- **<family>**
  (Optional) Specifies a collection of CIs that have similar attributes.
- **<class>**
  (Required) Specifies a subset of CIs within a family.

> **Note:** If GRLoader cannot find family or class, the CI is not created or updated.

Example: Identify a CI by Family and Class

The following example shows a CI named ServerCI that is identified by the family Hardware.Server and class Windows.

```
<ci>
        <name>ServerCI</name>
```

```
        <family>Hardware.Server</family>
        <class>Windows</class>
...
</ci>
```

The CI Tag Reconciliation Attributes (Required)

One or more reconciliation attributes are required when creating, updating, or referencing a CI. GRLoader uses these attributes to uniquely identify the CI to be created or updated. Reconciliation attributes are also used to identify a provider/dependent relationship between two CIs.

Specify the reconciliation attributes using the following XML element tags:

- <name> -- The name of the CI or resource (required when creating the CI for first time)
- <serial_number> -- The manufacture unique identifier
- <asset_num> -- Alternate resource identifier, for example, an alternate ID located on sticker placed on computer
- <system_name> -- Computer name (hardware only)
- <dns_name> -- The name by which this device is known in the domain name server
- <mac_address> -- MAC address. (hardware only)
- <id> -- UUID of the CI, used for direct updates when ID is known

The name attribute is required when creating a CI for the first time. If GRLoader cannot resolve the specified reconciliation attributes, an existing CI is not updated. Reconciliation attributes are special purpose Common Attributes that are used for identification purposes.

Example: Identify a CI When Creating or Updating It

In the following example, the CI definition uses name, serial_number, dns_name, mac_address and system_name to uniquely identify the CI when creating or updating it.

```
<ci>
    <name>ServerCI</name>
    <serial_number>HMVV081</serial_number>
    <dns_name>serverci.myco.com</dns_name>
    <mac_address>00:12:3F:48:F0:95</mac_address>
    <system_name>ServerCI</system_name>
...
</ci>
```

The CI Tag Common Attributes

In general, common attributes are attributes that can be used in any CMDB family or class. The XML element tag used for the attribute is the same as the attribute object name. The attribute value depends on its type, which can be a constant or an SREL value that indicates a foreign key reference to another table.

Example: Specify Common Attributes

In the following example, the CI definition named ServerCI specifies the following common attributes: manufacturer, model, and alarm_id (IP Address). The ServerCI name is also a common attribute.

```
<ci>
    <name>ServerCI</name>
...
    <manufacturer>Dell Inc.</manufacturer>
    <model>OptiPlex GX280</model>
    <alarm_id>130.200.19.220</alarm_id>
...
</ci>
```

The CI Tag Family-Specific Attributes

Class attributes are unique to a specific CI family or class. The XML element tag used for the class attribute is the same as the attribute object name found in the family/class specific tables.

Example: Specify Family-Specific Attributes

In the following example, the CI definition named ServerCI specifies the attributes specific to the Hardware.Server family that include bios_ver, cd_rom_type, hard_drive_capacity, and so on.

```
<ci>
    <name>ServerCI</name>
...
    <bios_ver>A04</bios_ver>
    <cd_rom_type>DVD+-RW DVD8701</cd_rom_type>
    <hard_drive_capacity>90 MB</hard_drive_capacity>
    <number_net_card>3</number_net_card>
    <number_proc_inst>1</number_proc_inst>
    <phys_mem>2048 MB</phys_mem>
    <proc_speed>2793 MHz</proc_speed>
   <swap_size>4959 MB</swap_size>
...
</ci>
```

The CI Tag MDR Identification

A management data repository (MDR) identifies the data provider for a CI and how the CIs maps back to the corresponding MDR.

CA SDM uses MDR information to perform the following tasks:

- Launch in context from the CI log directly to the MDR data provider.
- Tracks CI attribute changes back to the source MDR.
- Detects when more than one MDR updates a CI attribute. This situation occurs when multiple MDRs contribute data independently to a CI definition.
- Identifies which MDR acts as the authoritative source.

Note: For more information about MDRs, see this (see page 2538) topic.

Use the following XML element tags to specify MDR attributes:

- **<mdr_class>**
  Specifies the MDR class to group MDRs that CA SDM processed similarly.

- **<mdr_name>**
  Specifies the MDR name that an MDR uses to reference itself. Verify that the mdr_name and mdr_class value combination is unique within your enterprise.

- **<federated_asset_id>**
  Specifies the Federated asset ID that indicates the unique identifier of an MDR for a CI.

If GRLoader cannot resolve the specified mdr_class and mdr_name to an existing MDR, GRLoader does not import the CI. A CI with no associated federated_asset_id mapping is not federated.

Example: Identify a CI in the MDR

In the following example, the CI definition named ServerCI specifies mdr_class and mdr_name to uniquely identify the MDR and federated asset id, and thus identify the CI in the MDR.

Note: CA SDM uses the mdr_class string value *Cohesion* when federating data from the [assign the value for acm in your book] product.

```
<ci>
    <name>ServerCI</name>
...
    <federated_asset_id>1001118</federated_asset_id>
    <mdr_class>Cohesion</mdr_class>
    <mdr_name>CohesionServer</mdr_name>
...
</ci>
```

The CI Tag Versioning Attributes

You can use GRLoader to set versioning attributes for a CI.

Note: For more information about versioning, see the Versioning section.

Specify the Versioning attributes using the following XML element tags:

- **<milestone>**
  Specifies the label associated with that milestone that displays in the Versioning tab.

- **<standard_ci>**
  Specifies the name of the standard CI to use for baseline comparisons in the Versioning tab.

The CI that you specified for the standard_ci attribute must already exist in the CMDB or be specified before you specify the CI definition in the XML file. The milestone generated records the state of the CI at the time that GRLoader executes.

Example: Specify Baseline Comparisons

In the following example, the CI definition named ServerCI specifies the standard CI named standard server config for baseline comparisons with ServerCI (the focal CI). This example assumes that the standard CI already exists in CA SDM. In addition, a milestone named Fiscal year end 2008 is also created to preserve the state of the CI at the time that GRLoader imports the XML.

```
<ci>
     <name>ServerCI</name>
     <class>Server</class>
     <standard_ci>standard server config</standard_ci>
     <milestone>Fiscal year end 2008</milestone>
...
</ci>
```

XML Content The Relation Tag

GRLoader can create or update relationships between configuration items by using the <relation> XML element tag. Relationships are many-to-many, and the relationship type specifies how two provider/dependent configuration items relate to one another in CMDB.

Specify the relation attributes using the following XML element tags:

- **<type>**
  (Optional) Specifies the name of the relationship type.

- **<delete_flag>**
  Designates a relationship as inactive or active. Specify 1 (one), yes, or true to make the relationship inactive. Specify 0 (zero), no or false to make the relationship active again. Setting the delete_flag to true leaves the existing relationship intact but marks it as inactive.

- **<provider>**
  (Required) Identifies the provider CI for the relationship, which contains one or more of the CI reconciliation attributes.

- **<dependent>**
  (Required) Identifies the dependent CI for the relationship, which contains one or more of the CI reconciliation attributes.

Note: If GRLoader cannot find a specified type, provider CI, or dependent CI, the relationship is created or updated.

Example: Define a Relationship Between CIs

The following example defines a relationship between the CIs named ServerCI (provider) and ServerCI|NetworkAdaptor-0 (dependent). The relationship type is contains. The example assumes that both CIs have already been defined in the CMDB or are specified preceding the relationship definition in an XML file. In addition, both the provider and dependent CIs must match all reconciliation attributes for the relationship to be created.

```
<relation>
    <type>contains</type>

    <provider>
        <name>ServerCI</name>
        <serial_number>HMVV081</serial_number>
        <dns_name>serverci.myco.com</dns_name>
        <mac_address>00:12:3F:48:F0:95</mac_address>
        <system_name>ServerCi</system_name>
    </provider>
    <dependent>
        <name>ServerCI|NetworkAdaptor-0</name>
    </dependent>
</relation>
```

XML Content Special Values

Special-purpose XML attributes can modify how a CI value is set or updated when imported by GRLoader. You can use these attributes to perform special processing or formatting when setting the value; for example, to format a date value or use the result of a lookup.

Examples of special XML values include the following ones:

- **lookup**
  Specifies a CI by an attribute other than combo_name (lastname, firstname, middle). Examples include: userid,

- **update_if_null**
  Specifies the update_if_null option for GRLoader to use to distinguish between values that are blank and those which are not supplied in the XML. By default, update_if_null is set to "", which means that blank or missing values are ignored by GRLoader.
  The following attribute descriptions for serial number are equivalent:

  ```
  <serial_number></serial_number>

  <serial_number/>

  <serial_number update_if_null="">
  ```

  If you want to remove the serial number from a CI that has one, the previous XML does *not* work, because GRLoader ignores blank or missing values. Instead, code xml for the serial number as follows:

  ```
  <serial_number update_if_null="true"></serial_number>
  ```

  This syntax always updates the attribute, even if the value is blank or missing.

- **dateformat=[utc | localtime]**
  Sets the *dateformat* attribute for the date field to be either “utc” or “localtime”. Required when the format of the date is in UNIX Time Code (UTC) format. If dateformat is not set, the default is “localtime".

Date Formats

CMDB supports the following localtime date formats:

- yyyy.mm.dd
- yyyy.mm.dd hh:mm:ss

If the value does not match either of these formats, the parser tries to resolve the date as a UTC time. If the date format is not UTC, CMDB uses the system locale setting: for US English, the 12-hour format of “mm/dd/yyyy” or “mm/dd/yyyy hh:mm:ss *a*” where *a* specifies either AM or PM).

Contact and Other Lookup Fields

The Contact object combines first name, middle initial, and last name. The object has the following format:

```
<resource_contact>Lastname, Firstname MiddleInitial</resource_contact>
```

If you want to use a different field for a lookup field, you can supply a lookup attribute. For example, if you wanted to look up John Q. Doe by userid, use the following entry:

```
<resource_contact lookup="userid">doejo04</resource_contact>
```

Fields Validated Against Data in Existing Tables (SREL)

Common attributes accept only a specific set of values that must be defined in related tables in CMDB. These attributes can also have additional restrictions and exceptions that must be met for the assignment to occur. For example, a class attribute specified in XML must match one of the existing class names (CMDB default or user-defined). Otherwise, the CI is not created or updated. In addition, the value cannot be set to null, and the class must be Active for the assignment to occur.

The following fields validate data against data in existing tables:

- audit_userid
- bm_rep
- bm_status
- class
- company_bought_for_uuid
- contact_1
- contact_2

- contact_3
- delete_flag
- department
- expense_code
- family
- location
- manufacturer
- model
- operating_system
- org_bought_for_uuid
- priority
- repair_org
- resource_contact
- resource_owner_uuid
- service_org
- service_type
- status
- supplier
- vendor_repair
- vendor_restore

XML Input

When importing CI data, format the data in a supported format, such as XML or a spreadsheet (XLS or XLSX).

Consider the following XML format example:

XML Document	Notes
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?> <GRLoader>	These headers are required.

<ci>	Include zero or more <ci> nodes to define the CIs.
<name>value</name> <mac_address>value </mac_address> <dns_name>value </dns_name> <asset_num>value </asset_num> <serial_number>value </serial_number> <system_name>value </system_name>	These six characteristics uniquely identify a CI in a CI or Relations definition. At least one must be specified.
<class>value</class> <family>value</family> <manufacturer>value </manufacturer> <model>value</model>	These four values determine the class and family of a CI. You specify either (class) or (manufacturer/model).
<mem_capacity>value </mem_capacity> <number_net_card>value </number_net_card> <phys_mem>value </phys_mem_update> <proc_speed>value </proc_speed> <proc_type>value </proc_type> <server_type>value </server_type> </ci>	Family-specific values. Zero or more family-specific values can be provided when defining a CI.
<relation> <type>relation_type </type>	Include zero or more <relation> nodes to define relationships. Specify the relationship type.
<provider> <name>value</name> <mac_address>value </mac_address> <dns_name>value </dns_name> <asset_num>value </asset_num> <serial_number>value </serial_number> </provider>	Identify the provider CI with at least one attribute.
<dependent>	Identify the dependent CI with at least one attribute.

```
<name>value</name>
<mac_address>value<
/mac_address>
<dns_name>value<
/dns_name>
<asset_num>value<
/asset_num>
<serial_number>value<
/serial_number>
</dependent>
</relation>

</GRLoader>
```

Example: XML Input

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<GRLoader>
    <ci>
        <name>Host1</name>
        <class>Server</class>
    </ci>
    <ci>
        <name>Host2</name>
        <class>Server</class>
    </ci>
    <relation>
        <type>connects to</type>
        <provider>
            <name>host1</name>
        </provider>
        <dependent>
            <name>host2</name>
        </dependent>
    </relation>
</GRLoader>
```

MAC Address Normalization

Previous releases of GRLoader normalized the MAC address of CIs by removing the ":" and "-" delimiters from the MAC address. This normalization resulted in a MAC address of: aa:bb:cc:dd:ee storing as aabbccddee.

Consider the following MAC address behavior:

- The default is no MAC address normalization.
- CIs created with no normalization in CMDB reconcile with CIs that were created without normalization in CMDB r11.x.
- Invalid MAC addresses are treated as simple strings and are stored unmodified.

The following GRLoader parameters let you enable or disable MAC normalization:

- **-mn**
  Removes the ":" and "-" delimiters from MAC addresses (MAC normalization).

- **-nomn**
  Does not remove the ":" and "-" delimiters from MAC addresses.

  Important! Installing an earlier version if CMDB enables MAC address normalization automatically. You can override normalization by using the *-nomn* parameter

Because options are processed sequentially on the command line, the order of the options is important in the syntax.

How to Prepare for Loading JDBC Data

Contents

Complete the following steps when preparing to load data from a JDBC database table into CA SDM:

1. Identify the database, database type, userid, password and the JDBC drivers used to access the database.
2. Identify the table and columns that you want to load.
3. If necessary, map column names using the SQL *AS* keyword to CMDB attribute names.
4. If necessary, map data values using a translation file or a SQL join.
5. Identify portions of the table that you want GRLoader to ignore or skip.

Example JDBC Attribute Mapping

The following example shows how to use the SQL AS clause for JDBC attribute mapping:

```
GRLoader  - dbdriver sun.jdbc.odbc.JdbcOdbcDriver
-dburl "jdbc:odbc:Driver={Microsoft Access Driver (*.mdb, *.accdb)};DBQ=filename"
-dbuser administrator
-dbpswd adminpassword
-s http://hostname:8080
-n  - a -E
```

```
 - dbstmt "SELECT 'ci'    AS objecttype, resource_name AS name , ip_address AS
alarm_id     FROM   my_table"
```

Consider the following information about the previous example:

- The objecttype column is required when you import CIs without specifying a class column in the SELECT statement.
  Note: Use the SQL “AS” keyword when you use input from database tables to create views.

- You use the *ci* value in the obecttype column as a constant value that does not require a physical presence in the database.

Example Load Data from a Microsoft Access Database Using ODBC

CA SDM includes the generic JDBC-ODBC driver named sun.jdbc.odbc.JdbcOdbcDriver in the rt.jar file. If you want to use a database-specific driver, specify additional JDBC JAR files, as required by your database vendor. Use the -addjar facility to add any necessary JARs to the classpath dynamically. In this example, you load data from a Microsoft Access database.

Follow these steps:

1. Open GRLoader.

2. Execute the following command:

```
GRLoader
 - dbdriver sun.jdbc.odbc.JdbcOdbcDriver
-dburl "jdbc:odbc:Driver={Microsoft Access Driver (*.mdb, *.accdb)};
DBQ=filename"
-dbuser administrator
-dbpswd adminpassword
-s http://hostname:8080
-n  - a -E
-u userid -p password
-dbstmt "SELECT ciname AS name, ciclass AS class,
 FROM table1"
-e jdbc_err.xml
```

> **Important!** When you use values that contain spaces, enclose the values in double quotations, such as with dbdriver and dbstmt.

Example Load Data from a Microsoft Access Database Using ODBC and a Configuration File

In this example, you include the database connection information in a separate configuration file. Using this file reduces the command line length in GRLoader.

Note: You do not have to include quotes in the configuration file. Input statements on single lines and do not continue the input across multiple lines.

Follow these steps:

1. Create a file named table1.cfg and add the following code:

```
grloader.jdbc.driver=sun.jdbc.odbc.JdbcOdbcDriver
grloader.jdbc.url=jdbc:odbc:Driver={Microsoft Access Driver (*.mdb, *.accdb)};
DBQ=filename
grloader.jdbc.user=administrator
grloader.jdbc.password=adminpassword
```

   Note: In this example file, the grloader.jdbc.url appears on one line, as each option in the configuration file also appear.

2. Save the file.

3. Open GRLoader.

4. Execute the following command:

```
GRLoader
 - cfg table1.cfg
-s http://hostname:8080
-n  - a -E
-u userid -p password
-dbstmt "SELECT ciname AS name, ciclass AS class FROM table1"
```

Example Load Data from a SQL Server Database Table

In this example, you load data from a SQL Server database using drivers supplied by the database vendor.

Follow these steps:

1. Open GRLoader.

2. Execute the following command:

```
GRLoader
-dbdriver com.microsoft.sqlserver.jdbc.SQLServerDriver
-dburl jdbc:sqlserver://localhost:1433;databaseName=mdb;
-dbuser servicedesk -dbpswd password
-s http://hostname:8080  -a -n -E
-u userid -p password
-dbstmt "SELECT name, 'Server' AS class
         FROM ca_owned_resource"
-e jdbc_err.xml
```

Example Load Data from an Unsupported MySQL Database

In this example, you load data from an unsupported MySQL Server database to the TWA using drivers supplied by the database vendor. You specify the database user and password in the dburl option.

Follow these steps:

1. Open GRLoader.
2. Execute the following command:

```
GRLoader
-dbdriver com,mysql.jdbc.Driver
-dburl jdbc:mysql://hostname/test?user=abed&password=pwd
-s http://hostname:8080  -a -n -E
-lttwa
-u userid -p password
-dbstmt "SELECT name, class from mytable3"
-e jdbc_err.xml
```

Example Import Relationships from a Database Table

In this example, you load relationships from a database table. The provider and dependent attribute names are prefixed with *provider_* and *dependent_*, as in the TWA.

Follow these steps:

1. Open GRLoader.
2. Execute the following command:

```
GRLoader
-dbdriver com.microsoft.sqlserver.jdbc.SQLServerDriver
-dburl jdbc:sqlserver://localhost:1433;databaseName=mdb;
-dbuser servicedesk -dbpswd password
-s http://hostname:8080  -a -n -E
-u userid -p password
-dbstmt "SELECT provider_name, type, dependent_name,
 FROM mytable4"
```

Example Display the WHERE Clause in the SELECT Statement

In this example, you display the WHERE clause in the SELECT statement to filter input data by location.

Follow these steps:

1. Open GRLoader.
2. Execute the following command:

```
GRLoader
-dbdriver com.microsoft.sqlserver.jdbc.SQLServerDriver
-dburl jdbc:sqlserver://localhost:1433;databaseName=mdb;
-dbuser servicedesk -dbpswd password
-s http://hostname:8080  -a -n -E
-u userid -p password
-dbstmt "SELECT name, class,
 FROM mytable5 WHERE location='Brooklyn' "
```

Example Set Default Values for Attributes that Do Not Appear in the Input Table

In this example, you can specify any attribute with the -ad option. You can apply this example to spreadsheets and XML files.

Important! We recommend that you do not specify the tenant with the -ad option. Instead, GRLoader should inherit the tenant from the user ID that runs GRLoader. The Service Provider assigns each tenant a tenant-specific user ID, and then each tenant uses that user ID when creating objects that belong to that tenant.

Follow these steps:

1. Open GRLoader.
2. Execute the following command to set a default IP address:

   ```
   grloader  - i myspreadsheet.xlsx  - ad alarm_id="Unknown"
   ```

   Note: If a row in the spreadsheet contains a value for alarm_id, then GRLoader does not use the default value.
3. Use the -iia option to ignore an invalid attribute name to hide the warning message.
   For example, the spreadsheet contains both CIs and relationships, and the relationships would receive a warming message because alarm_id is not a valid relationship attribute.

How to Prepare for Loading CSV File Data

Contents

GRLoader can read CSV files to load CIs and relationships, similar to how it processes JDBC database tables and spreadsheets. GRLoader treats any rows that begin with # as comments.

Note: The first row in the CSV file must contain column headings so that GRLoader translates the CI and relationship attribute names correctly.

Complete the following steps when preparing to load data from a CSV file:

1. Identify the CSV file that you want to load.
2. If necessary, add a header row.
3. If necessary, map attribute names and data values using a translation (see page 4326) file.
4. Identify parts of the CSV file that GRLoader *must* ignore or skip. If necessary, write corresponding translation rules.

Example Load Data from a CSV File

In this example, you load data from a file named sample.csv and the example.rul translation file.

Follow these steps:

1. Open the CSV file that contains the following information:

```
"name","class","alarm_id","disk space","carrier","phys_mem"
"server 1","Server","1","5","","7"
"server2","Server","2","6","",""
"acd1","ACD","3","","Vendor1",""
"server3","Discovered Hardware","4","","","",""
```

2. Open the translation file that contains the following information:

```
<ruleset>
<rule><attribute>attributename</attribute>
      <from>disk space</from><to>hard_drive_capacity</to>
      <rulename>rule12</rulename></rule>
</ruleset>
```

3. Execute the following GRLoader command:

```
grloader  - u username -p password  - s  http://sdmhost:8080  - i example13.
csv  - tf example13.rul -lttwa.
```

GRLoader loads 4 CIs to the TWA.

How to Prepare for Loading Spreadsheet Data

This article contains the following topics:

- Example Load a CI with Multiple Embedded Relationships (see page 4333)
- Example Create a CI and a Relationship by Specifying the UUID (see page 4334)
- Example Load a Spreadsheet that Contains Change Specifications (see page 4334)

If the spreadsheet includes instructions, comments, and data that you do *not* want load into CA SDM, specify the exact area you want to import into GRLoader. To specify the area of the spreadsheet to use as input, use GRLoader to provide the spreadsheet file name, the spreadsheet sheet name, the first and last rows, and the first and last columns, as set by the - i (or -ssf), -sss, -ssfr, -sslr, -ssfc, and -sslc options.

Perform the following tasks before loading CI data from a spreadsheet with GRLoader.

1. Identify the general area of the spreadsheet to use as an input to GRLoader.
2. If necessary, map attribute names and data values using a translation file (see page 4326).
3. Identify parts of the spreadsheet that GRLoader *must* ignore or skip.

The input examples in the following sections use a fictitious spreadsheet named *grloader_spreadsheet_example.xls*. This spreadsheet contains nine subsheets, named Sheet1, Sheet2, Sheet3, and so on.

Spreadsheet Data Loading Support

GRLoader supports loading CI and CI relationship (see page 4332) data from spreadsheets (see page 4323) in Microsoft® Excel XLS and XLSX format, but it does *not* support XLSB files. By default, GRLoader attempts to process the first sheet of the spreadsheet file. In general, GRLoader attempts to match the column names in the spreadsheet to attribute names in the CI or relationship. GRLoader uses rules similar to when importing data from the TWA.

For example, a spreadsheet contains the following cells:

name	class	phys_mem
server1	Server	1gb
server2	Server	2gb

The following XML matches the spreadsheet cells exactly:

```
<GRLoader>
<ci><name>server1</server><class>Server</class>
    <phys_mem>1gb</phys_mem></ci>
<ci><name>server2</server><class>Server</class>
    <phys_mem>2gb</phys_mem></ci>
</GRLoader>
```

Note: Like when loading data to the TWA, if the GRLoader import results in an error, a file ending in **_err.XML* appears in the input file directory with information about the error. For example, if your spreadsheet file name is cidata.xlsx, the error file is named cidata_err.xml. As usual, logging information is also directed to the GRLoader.log file in the nxroot\log directory.

Spreadsheet Column Rules

A single spreadsheet can contain both CIs and relationships. When you load spreadsheet data, the presence of specific columns implies the target object type, as described by the following rules:

- If a column *class* is present with a nonblank value, the object type is assumed as *CI*.
- If any column prefixed with *provider_* is present with a nonblank value, the object type is assumed as *relation*.
- If data exists in both the *class* and *provider_* columns in the spreadsheet, you can specify *objecttype*. Use *ci* or *relation* as the value of the objecttype.
- A default class specified on the command line with *-ad class=class name*.
- A default provider attribute is specified on the command line with *-ad provider_xxxx*=nonblank.

By applying these rules, you cannot determine if the following example input data represents a CI or a relationship, which can represent an update to a CI:

name	hard_drive_capacity
Server1	10 GB

If you did not specify class, set the *objecttype* on the command line, or set it explicitly in the spreadsheet table as shown in the following example:

objecttype	name	hard_drive_capacity
ci	Server1	10 GB

The objecttype attribute takes precedence over the existence of class or provider_ attribute names when GRLoader determines if the row represents a CI or a relationship.

When you load relationship data from spreadsheets or databases, prefix the CI-identifying attribute with either *provider_* or *dependent_*, to match how they were specified in the TWA. For example, specify the name of a relationship provider by naming a column as *provider_name* in the database table.

Spreadsheet Rows with Embedded Relationships

For convenience of entering data, a single row in a spreadsheet can contain embedded relationships. A row with an embedded relationship contains both a CI and its associated relationships. The following example shows a CI with an embedded relationship.

objecttype	name	hard_drive_capacity	is used by
ci	Server1	10 GB	Server2; Server3

How GRLoader Converts Spreadsheet Data Types

When you use spreadsheets to load data, GRLoader performs data type conversions automatically:

1. Converts *DATES* to standard CA SDM dates in the *yyyy.mm.dd hh:mm:ss* format.
   Note: Excel stores these dates as milliseconds past the epoch.

2. Converts *NUMERIC* values to strings.
3. Converts *BOOLEAN* values to 0 or 1.
4. *STRINGS* are not altered.
5. GRLoader ignores *BLANK* values.
6. Evaluates *FORMULAS* first and then applies the previously specified rules to the cell.

Translation Rule Spreadsheet Attribute Mapping

Column names typically define the same CI or CI relationship attribute names. If the names differ, use a translation file to convert a column heading to an attribute name.

Important! The first row of the selected input area is significant because it contains column headings.

You map attribute names by including a rule which specifies a rule for the new keyword attribute name named *attributename*. GRLoader processes rules for *attributename* before applying value maps. A rule which specifies *<attribute>attributename</attribute>* is an attribute map, not a value map, so it changes the attribute name of an attribute, not the value of the attribute data.

For example, CA SDM requires that you load the IP address of a CI into a field named *alarm_id*. If the spreadsheet column name is *ip address*, use a translation rule to map *ip address* to *alarm_id* by using the following translation rule:

```
<rule>
   <attribute>attributename</attribute>
   <from>ip address</from>
   <to>alarm_id</to>
</rule>
```

Mapping an attribute name to “” (blank) is equivalent to ignoring that attribute. In the following example, GRLoader ignores all *owner* data:

```
<rule>
   <attribute>attributename</attribute>
   <from>owner</from>
   <to></to>
</rule>
```

Setting Default Attribute Values

In a typical business environment, you use an existing spreadsheet as an input to GRLoader. We recommend that you do not change the content in the spreadsheet. If that spreadsheet is incomplete and does *not* contain information necessary to import the data, you *must* specify the - ad (attribute default) option on the command line, as shown in the following example:

```
grloader  - u username  - p password  - s http://sdm-host:8080  - i myspreadsheet.
xlsx  - ad tenant=tenanta -ad mdr_class=spreadsheet -ad mdr_name=mdr1 -n
```

You can specify any attribute with the - *ad* option. For example, set a default IP address with the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080  - i myspreadsheet.
xlsx  - ad alarm_id="Unknown" -n
```

If a row in the spreadsheet contains a value for alarm_id, then the default value is not used.

You can also specify attribute defaults for relationships. If myspreadsheet.xlsx contains both CIs and relationships, the relationships receive a warning message because alarm_id is not a valid relationship attribute. In this case, use the *-iia* parameter in GRLoader to ignore the invalid attribute name because this option suppresses the warning message.

Spreadsheet Considerations

The spreadsheet input area contains two areas, column headings and data. The GRLoader options bind the square input area for the start row, end row, start column, and end column. If you do not supply these options, then the bounds define the natural limits of the spreadsheet.

If you want to import CI data and CI relationships from spreadsheets (see page 4323), consider the following information:

- GRLoader considers the first populated row in the input area as column headings, and *must* contain CI attribute names or relationship attribute names, as XML attribute names appear for XML-based input.
- GRLoader does *not* process comments from Excel spreadsheets.
  Note: A red triangle in the upper right corner of the cell indicates a comment in Excel.
- GRLoader ignores the entire column when the heading row value is prefixed with the comment character (#).
- If a heading line consists entirely of comment, GRLoader considers it as a blank line and skips it.
- GRLoader can view hidden rows and columns in spreadsheets.
- GRLoader ignores embedded objects within spreadsheets.
- GRLoader identifies embedded relationships by an attribute name when it is an actual relationship type.
- GRLoader supports embedded relationships (see page 4332) with the following limitations:
  - The CI identified by name, serial number, mac address, and so on, represents the provider CI.
  - In the relationship column, specify the CI as the dependent, when you use a provider /dependent relationship type.
  - Using a dependent/provider relationship type reverses the roles of the two CIs.

- Multiple embedded relationships can occur in a single relationship cell. You separate each partner name from other partners by the *grloader.spreadsheet.embeddedseparator* character specified in the config file.

- If you *must* specify more than one identifying attributes for a dependent or provider in a relationship, then you *must* fall back to the fully qualified style of creating relationships. In this case, you specify provider_name, provider_mac_address, type, dependent_name, dependent_mac_address, and so on. If you want to specify more than one identifying attribute, you cannot use embedded relationships.

- GRLoader can evaluate most functions in a spreadsheet, but not all functions. The following functions are known to be incompatible with GRLoader:

  - edate()

  - text()

Important! Any cell that directly or indirectly references an incompatible function generates an error message and GRLoader ignores the cell.

Error Handling

When loading data into integer fields (such as hardware_server.purchase_amount) previous versions of GRLoader would attempt to load the data resulting in partial and incorrect data. The current GRLoader generates a warning message indicating the data is invalid. The only valid characters in an integer field are [0-9].

Because using the - *ad* option often results in an attribute warning message when both CI and relationships are imported in the same run, referring to an invalid attribute in a CI or Relationship definition results in a warning instead of an error. The Ignore Invalid Attribute - *iia* option can be used to suppress these warnings.

Example Load CI Data from a Simple Spreadsheet

Use GRLoader to load a simple spreadsheet with CI data. The column headings match CI attribute names in the following example in *Sheet1* of *grloader_sample_spreadsheet.xls*:

name	class
server1	Server
server2	Server
acd1	ACD

To load the data with GRLoader, execute the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080 -i
grloader_sample_spreadsheet. -n
```

GRLoader loads three CIs with no errors.

Example Load CI Data from the Extension Table

Use GRLoader to load a spreadsheet with CI data, including data from the extension table. The column headings match CI attribute names in the following example in *Sheet2* of *grloader_sample_spreadsheet*.xls:

name	class	alarm_id	hard_drive_capacity	carrier	phys_mem
server1	Server	1	5		7
server2	Server	2	6		
acd1	ACD	3		carrier1	
server3	Discovered Hardware	4			

To load the data with GRLoader, execute the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080 -i
grloader_sample_spreadsheet.xls -sss Sheet2 -n
```

GRLoader loads four CIs with no errors, including family-specific attributes.

If the data is offset from the A1 cell in *Sheet3* in the spreadsheet, and the data has blank rows and columns, load the data by executing the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080 -i
grloader_sample_spreadsheet.xls -sss Sheet3 -n
```

GRLoader ignores blank rows, columns, and cells, and loads four CIs with no errors.

If the data in *Sheet4* contains missing (or blank) column headings, such as E5, execute the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080 -i
grloader_sample_spreadsheet.xls -sss Sheet4 -n
```

GRLoader ignores the empty Column E (E5) and loads four CIs with no errors.

If the data in *Sheet5* contains four rows that you want to ignore, and the CI data begins on the C5, execute the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080 -i
grloader_sample_spreadsheet.xls -sss Sheet5 -ssfr 5 -n
```

GRLoader ignores the first four rows and loads four CIs with no errors.

Example Load a Spreadsheet with Column Names that Contain Invalid CI Attribute Names

Use GRLoader and translation file to load a spreadsheet with column names that contain invalid CI attribute names. The name column begins on row C5. The column headings match CI attribute names in the following example in *Sheet7* of *grloader_sample_spreadsheet.xls*:

name	class		hard_drive_capacity	carrier	phys_mem
server1	Server	ignore	ok		ok
server2	Server	ignore	ok		ok
acd1	ACD	ignore		ok	ok
server3	Discovered Hardware	ignore			ok

Before you run GRLoader, create a translation file named *Sheet7.rul* that contains the following XML:

```
<ruleset>
<rule>
   <attribute>attributename</attribute>
   <from>ip address</from>
   <to>alarm_id</to>
</rule>
</ruleset>
```

After you create this XML file, load the data with GRLoader by executing the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080  - i
grloader_sample_spreadsheet.xls  - sss Sheet7  - ssfr 5  - tf Sheet7.rul -n
```

GRLoader ignores the first four rows and column E because E5 is empty, and loads four CIs with no errors.

Load a Spreadsheet that Does Not Contain mdr_name or tenant

Use GRLoader to load a spreadsheet that does not contain mdr_name or tenant. You can set attributes from the command line. The name column begins on C5. The column headings match CI attribute names in the following example in *Sheet8* of *grloader_sample_spreadsheet.xls*:

name	class	tenant	federated_asset_id
server1	Server		f1
server2	Server		f2
acd1	ACD	tenantb	f3
server3	Discovered Hardware	tenantb	f4

To load the data with GRLoader, execute the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080  - i
grloader_sample_spreadsheet.xls  - sss Sheet8  - ssfr 5  - ad tenant=tenanta  - ad
mdr_name=ACMserver1  - ad mdr_class=ACM12 -n
```

GRLoader assigns server1 and server2 to tenanta, assigns all CIs with the mdr_name as ACMserver1, assigns all CIs with the mdr_class as ACM12, and loads the four CIs with no errors.

Example Load a Spreadsheet that Rejects Bad Data

Use GRLoader to load a spreadsheet that rejects bad data by using a translation rule. In the following example, the name column begins on row C5 in *Sheet9* of *grloader_sample_spreadsheet.xls*:

name	class	skip	ip address
server1	Server		
server2	Server	yes	
server3	ACD	1	
server4	ACD		bad
server5	ACD		bad
server6	ACD		

Before you run GRLoader, create a translation file named *Sheet9.rul* that contains the following XML:

```
<ruleset>
<rule><attribute>skip</attribute><from>1</from>
      <reject>yes</reject><rulename>rule1</rulename></rule>
<rule><attribute>skip</attribute><from>yes</from>
      <reject>yes</reject><rulename>rule2</rulename></rule>
<rule><attribute>alarm_id</attribute><from>bad</from>
      <reject>yes</reject><rulename>rule3</rulename></rule>
<rule><attribute>attributename</attribute>
      <from>ip address</from><to>alarm_id</to>
      <rulename>rule4</rulename></rule>
</ruleset>
```

After you create this XML file, load the data with GRLoader by executing the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080  - i
grloader_sample_spreadsheet.xls  - sss Sheet9  - ssfr 6  - tf Sheet9.rul -n
```

Based on the translation rule, GRLoader completes the following actions:

1. GRLoader loads two CIs: server1 and server6.
2. GRLoader rejects server2 because the skip column is set to yes (rulename rule2).
3. GRLoader rejects server3 because the skip column is set to 1 (rulename rule1).
4. GRLoader rejects server4 and server5 because of bad IP addresses for these CIs (rulename rule3).

Note: The attribute name translation (rule4) occurs before value translation, so the value translation rules *must* specify the translated attribute name. Even though the spreadsheet contained a column heading of *ip address*, the rule to reject the *bad* ip addresses (rule 3) *must* specify alarm_id.

Example Load a Spreadsheet Using Embedded Relationships

Use GRLoader to load a spreadsheet that contains CIs and relationships using embedded relationships. If you want to specify more than one identifying attribute, you cannot use embedded relationships.

In the following example, the name column begins on row A1 in *Sheet10* of *grloader_sample_spreadsheet.xls*:

name	class	connects to	hosts
accounting	Service		
server1	Server		accounting
server2	AIX	server1	accounting
server3	UNIX		GIS

Load the data with GRLoader by executing the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080  - i
grloader_sample_spreadsheet.xls -sss Sheet10 -aer yes -n
```

GRLoader creates the following CIs:

- accounting
- server1
- server2
- server3

GRLoader creates the following relationships:

- server1 hosts accounting
- server2 connects to server1
- server2 hosts accounting
- server3 hosts GIS

Loading Relationship Data from Spreadsheets

When you load relationship data from spreadsheets, specify the attributes for the provider and dependent CIs in the same way as they were in the TWA. As a result, you prefix the CI-identifying attribute with either *provider_* or *dependent_*.

For example, to specify the name of a relationship provider, specify *provider_name* in the spreadsheet column heading.

Example Load CI Relationships

Use GRLoader to load a spreadsheet that contains CI relationships. In the following example, the dependent_name column begins on row A5 in *Sheet6* of *grloader_sample_spreadsheet.xls*:

dependent_name	type	provider_name
service1	uses	server2
service1	uses	server3

To load the spreadsheet with CI relationships, execute the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080  - i
grloader_sample_spreadsheet.xls  - sss Sheet6  - ssfr 5 -n
```

After you execute the command, GRLoader ignores the first four rows and loads two relationships with no errors.

Example Load a CI with Multiple Embedded Relationships

Use GRLoader to load a spreadsheet that contains CIs and relationships using embedded relationships. If you want to specify more than one identifying attribute, you cannot use embedded relationships.

In the following example, the name column begins on row A1 in *Sheet11* of *grloader_sample_spreadsheet.xls*:

name	class	manages	is managed by
chief	manager		
agent99	agent		
agent86	agent		
chief	manager	agent86;agent99	CEO

Load the data with GRLoader by executing the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080  - i
grloader_sample_spreadsheet.xls -sss Sheet11 -aer yes -n
```

GRLoader creates the following CIs and relationships:

- The first three rows create three CIs.
- Row 4, processed after rows 1-3, creates the following CI relationships:
  - chief *manages* agent86
  - chief *manages* agent99
  - chief *is managed by* CEO

- As with XML input, the direction of the relationship is significant. In the *manages* column labeled, GRLoader creates two relationships, because chief is the *provider* for both dependents, agent86 and agent99.

- Because the *is managed by* attribute is a dependent/provider relationship type, the provider and dependents are switched in the *is managed by* column, because chief is a dependent and CEO is the provider.

Example Create a CI and a Relationship by Specifying the UUID

Use GRLoader to load a spreadsheet that contains CIs and relationships by specifying the UUID.

In the following example, the *# transaction* column begins on row A1 in *Sheet12* of *grloader_sample_spreadsheet.xls*:

# transaction	objecttype	name	class	provider_id	type	dependent_name
1	ci	server1	Server			
2	relation			12345678901234567890123456789012	uses	server2

Load the data with GRLoader by executing the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080  - i
grloader_sample_spreadsheet.xls -sss Sheet12 -n
```

GRLoader creates the following CIs and relationships:

- The transaction creates the server1 CI.

- The transaction creates a relationship between server1 and server2.

Example Load a Spreadsheet that Contains Change Specifications

Use GRLoader to load a Change Order with multiple change specifications.

In the following example, the *# transaction* column begins on row A1 in *Sheet13* of *grloader_sample_spreadsheet.xls*:

objecttype	chg	ci	attribute_name	attribute_value_planned
change specification	12345	server1	ip address	1.2.3.4
change specification	12345	server2	ip address	1.2.3.5
change specification	12345	server3	ip address	1.2.3.6
change specification	12345	server4	ip address	1.2.3.7

Load the data with GRLoader by executing the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080  - i
grloader_sample_spreadsheet.xls  - sss Sheet13
```

GRLoader creates four CIs and inserts the CIs into Change Order 12345.

Data Translation

This article contains the following topics:

Data values provided by an MDR may not meet the requirements of CMDB because of the following reasons:

- The country or language for an MDR can differ from the country or language selected for CMDB server installation. For example: A CA Cohesion MDR that uses American English transfers data to a CMDB in France. When CA Cohesion creates server CIs, it specifies the CI family as "Server". However, in France the CI family must be specified as "Serveur". An inbound "Server" value must be translated to the required "Serveur" value whenever the American-based MDR communicates with the French CMDB installation.

- Data inconsistencies can occur in lookup (SREL) fields. For example: An MDR contains CIs with a manufacturer of "Dell Inc", "Dell Corporation", or simply "Dell". If the CMDB manufacturer table requires "Dell Inc", other values are rejected with warning messages. The invalid inbound "Dell Corporation" and "Dell" values must be translated to the standard "Dell Inc" value for the manufacturer attribute.

- Data inconsistencies in non-SREL fields. For example, some MDRs report data in units, while others report data in bytes or gigabytes. You can standardize the format of the data stored in the CMDB.

To satisfy these requirements, GRLoader can translate any incoming value to another value, by using an XML-based lookup file when GRLoader is run.

Important: The pre-edit translation and validation step occurs when CI and relationship XML is read, before normal GRLoader processing occurs (for example, update_if_null, lookup, dateformat) and before data is transmitted to the CMDB server.

Because each MDR can have specific translation requirements, the data translation file is specified for each GRLoader invocation. For standardization purposes, we recommend that this file is located on a common file system and shared among the CMDB data providers.

Create Translation Rules

To use the GRLoader data translation and validation feature, create a set of rules to specify the data to be translated. Rules are required for each attribute and value being translated. Data translation rules are applied to the GRLoader input XML using the - tf *filename* parameter. The rules in *filename* are applied to all input submitted to GRLoader using the -i parameter. You can also use translation rules when importing CI data from spreadsheets.

Note: For information about creating translation rules for importing spreadsheet data, see this (see page 4323)topic.

To create translation rules, use a text editor to create and save rules in the GRLoader input XML like the following:

1. <ruleset>
2. <rule>
3. <attribute>class</attribute>
4. <from>Server</from>
5. <to>Serveur</to>
6. </rule>
7. <rule>
8. <attribute>manufacturer</attribute>
9. <from>Dell Corporation</from>
10. <to>Dell Inc</to>
11. </rule>
12. <rule>
13. <attribute>manufacturer</attribute>
14. <from>Dell</from>
15. <to>Dell Inc</to>

16. </rule>
17. </ruleset>

The translation rules are created.

Notes:

Lines 2-6 specify that whenever GRLoader encounters a line specifying <class>Server</class>: replace Server with Serveur (French) before sending the data to CMDB.

Lines 7-11 specify that a manufacturer of Dell Corporation should be replaced by Dell Inc. A single set of XML rules can be used to redefine several different attributes.

Lines 12-16 translate any input specifying Dell to the standard Dell Inc. The single set of XML contains multiple rules. When taken together, the rules specify multiple from/to values.

Data Transformation Example

This example shows a sample subset of the required rules for sharing data between MDRs using different languages. The GRLoader input XML example translates three classes from English to their French equivalents.

1. <?XML version="1.0" encoding="UTF-8"?>
2. <ruleset>
3. <rule>
4. <attribute>class</attribute>
5. <from>Server</from>
6. <to>Serveur</to>
7. </rule>
8. <rule>
9. <attribute>class</attribute>
10. <from>Printer</from>
11. <to>Imprimante</to>
12. </rule>
13. <rule>
14. <attribute>class</attribute>
15. <from>Contract</from>
16. <to>Contrat</to>

17. </rule>
18. </ruleset>

Data Validation

Often the values that are accepted into an attribute must be validated against a list of acceptable values before the CI is stored. The relationship between an attribute and its set of acceptable values (stored in a separate table) is named a *single relationship* (SREL).

When you want to validate data even when an SREL is not created for it, data translation rules can enforce standardization of data values.

Example: Convert Units of Data Storage

In the following GRLoader input XML, the MDR provides data in gigabytes (GB), but we want to store the total number of bytes in the CMDB.

1. <ruleset>
2. <rule>
3. <attribute>phys_mem</attribute>
4. <from>1 GB</from>
5. <to>1,073,741,824</to>
6. </rule>
7. <rule>
8. <attribute>phys_mem</attribute>
9. <from>2 GB</from>
10. <to>2,147,483,648</to>
11. </rule>
12. ...
13. </ruleset>

Unmatched or Non-Standard Input Values

When validating data, you can reject unacceptable values and replace them with new values. When input data does not match a rule, it proceeds unchanged to the next GRLoader phase.

Example: Validate Primary Colors

In the following example, if the GRLoader input specifies <color>hot pink</color>, the color data is unaffected by any translation.

```
1. <ruleset>
2. <rule>
3. <attribute>color</attribute>
4. <from>red</from>
5. <to>red</to>
6. </rule>
7. <rule>
8. <attribute>color</attribute>
9. <from>blue</from>
10. <to>blue</to>
11. </rule>
12. <rule>
13. <attribute>color</attribute>
14. <from>yellow</from>
15. <to>yellow</to>
16. </rule>
17. </ruleset>
```

In the previous example, the "from" and "to" values are the same. The following example shows a shortened form of the rule definition that does not include the "to" value:

```
1. <ruleset>
2. <rule>
3. <attribute>color</attribute>
4. <from>red</from>
5. </rule>
6. <rule>
```

7. <attribute>color</attribute>
8. <from>blue</from>
9. </rule>
10. <rule>
11. <attribute>color</attribute>
12. <from>yellow</from>
13. </rule>
14. </ruleset>

Using the shortened form of the rule definition, line 16 is more apparent. Line 16 specifies that if there is no matching "from" value for an attribute, that whatever value is specified, it is replaced by the "to" value.

1. <ruleset>
2. <rule>
3. <attribute>color</attribute>
4. <from>red</from>
5. </rule>
6. <rule>
7. <attribute>color</attribute>
8. <from>blue</from>
9. </rule>
10. <rule>
11. <attribute>color</attribute>
12. <from>yellow</from>
13. </rule>
14. <rule>
15. <attribute>color</attribute>
16. <to>unknown color</to>
17. <unmatched>yes</unmatched>

18. </rule>
19. </ruleset>

The GRLoader input includes a rule that matches "hot pink" (the "unmatched" rule on line 16). If color specifies an attribute other than red, blue or yellow (as indicated on lines 4, 8 and 12 respectively), that color is changed to the "to" value. For example, <color>hot pink</color> is recoded to <color>unknown color</color>.

If only lines 14-18 appear in the rule set (that is, no matches are possible), all colors in the GRLoader input XML file are set to "unknown color". This technique forces all values of a specific attribute to a single value.

Important!: The editing process cannot create new XML when none exists. If the input XML does not include information about <widgets>, all rules about <widgets> are ignored.

Example: Change All Unmatched "owner" Attributes to "Pete"

The following GRLoader input XML sets the value Pete for unmatched owners.

1. <ruleset>
2. <rule>
3. <attribute>owner</attribute>
4. <unmatched>yes</unmatched>
5. <to>Pete</to>
6. </rule>
7. </ruleset>

Consider how the following GRLoader input XML uses the previous ruleset:

1. <GRLoader>
2. <ci>
3. <name>server1</name>
4. <owner>John</owner>
5. </ci>
6. </GRLoader>

If the attribute "owner" has a rule, the rule attempts to match the value "John". Because no rule for the value "John" exists, GRLoader looks for an unmatched rule for the attribute "owner". If one exists, the translated input results in the following:

1. <GRLoader>
2. <ci>
3. <name>server1</name>
4. <owner>Pete</owner>
5. </ci>
6. </GRLoader>

Now consider the following GRLoader input XML file:

1. <GRLoader>
2. <ci>
3. <name>server2</name>
4. </ci>
5. </GRLoader>

The ruleset results in the following:

1. <GRLoader>
2. <ci>
3. <name>server2</name>
4. </ci>
5. </GRLoader>

The CI "server2" does not set the owner to Pete because no owner tag exists in the original XML.

Specify an Empty String

When an empty string must be specified as either the "from" value or the "to" value, always include the <from> or <to> value in the rule set.

Important!: Specifying <to></to> or not specifying <to> in the XML have very different XML meanings!

1. <ruleset>
2. <rule>
3. <attribute>size</attribute>
4. <from>XXL</from>
5. </rule>
6. <rule>
7. <attribute>manufacturer</attribute>
8. <from>General Motors</from>
9. <to></to>
10. </rule>
11. </ruleset>

Lines 2-5 specify that a size of XXL is possible. Because <to> is not specified, no recoding is performed on a size=XXL. This kind of rule is only useful when an unmatched rule appears later in the rule set for the same attribute.

Lines 6-10 examine all input data for a manufacturer="General Motors". Whenever this rule is found, because "<to></to>" is specified in the rule on line 9, the value of "General Motors" is replaced by "".

If you want to blank out the manufacturer, specify the update_if_null="YES" keyword in the GRLoader input XML.

Note: For more information about the use of the "update_if_null" option to blank out values in the database, see this (see page 4306) topic.

Alternative Comparison Methods

The default method uses "equals" for comparison. That is, when the <from> value is compared with the value in the GRLoader input, the two are considered to match when they are equal. The <comparetype> tag specifies alternative forms of comparison.

The comparetype tag accepts one of the following values:

- startswith
- endswith
- contains

- equals
- equalsignorecase

Example: Standardize a Company Name

In the following example, all manufacturer names beginning with "Dell" (such as "Dell Corp", "Dell Inc", "Dell Corporation") are reset to "Dell".

1. <ruleset>
2. <rule>
3. <attribute>manufacturer</attribute>
4. <from>Dell Corp</from>
5. <to>Dell</to>
6. </rule>
7. <rule>
8. <attribute>manufacturer</attribute>
9. <from>Dell Inc</from>
10. <to>Dell</to>
11. </rule>
12. <rule>
13. <attribute>manufacturer</attribute>
14. <from>Dell Corporation</from>
15. <to>Dell</to>
16. </rule>
17. </ruleset>

Alternatively, the following rule produces the same result:

1. <ruleset>
2. <rule>
3. <attribute>manufacturer</attribute>
4. <from>Dell</from>

5. <comparetype>startswith</comparetype>
6. <to>Dell</to>
7. </rule>
8. </ruleset>

Input Rejection

To reject input from an MDR before loading data into the CMDB, use the <reject> tag.

Example: Rejecting Input Data

The<reject tag> can be used with the <comparetype> tag, as shown in following example.

1. <ruleset>
2. <rule>
3. <attribute>name</attribute>
4. <from>test</from>
5. <comparetype>startswith</comparetype>
6. <reject>yes</reject>
7. </rule>
8. </ruleset>

When a reject rule is matched, the corresponding CI or relationship is rejected and the CMDB is not updated or created for that entire object. The transaction is skipped, and the XML is written to the _err file with an error message indicating that it was rejected.

Rule Syntax

The following table describes the XML tags that are used in a data translation rule set.

Tag	Description
<?XML version="1.0" encoding="codepage"?>	Enables different code pages for GRLoader.
<ruleset>	Begins a rule set. A ruleset can contain many rules.
<rule>	Begins a rule
<attribute>*attr_name*< /attribute>	Specifies an attribute that the rest of the rule applies to. *attribute* mus t be a valid CMDB attribute name.
<from>*value*</from>	Specifies a value to be changed. The <from> tag is modified by the <comparetype> tag.
<to>*value*</to>	Specifies the replacement value

<comparetype>*value*</comparetype>	(Optional) Specifies one of the following values: equals startswith endswith contains equalsignorecase If not specified, "equals" is the default.
<reject>yes</reject>	Specifies that GRLoader reject the CI or relationship. Yes can be specified as "yes" or one (1). No can be specified as "no" or zero (0). If not specified in a rule, the default is "no" (reject).
<rulename>*rule_name*</rulename>	(Optional) *name* assigned to identify this rule. This name appears in debugging messages.
</rule>	Ends a rule
</ruleset>	Ends a rule set

Running GRLoader with Translation Enabled

To run GRLoader using translation/transformation, run GRLoader with the **- tf** *filename* option. *filename* specifies the file which that contains the translation rule set.

Note: Alternatively, you can specify grloader.translationfile=*filename* in the configuration file.

Logging

Input modifications are logged in the stdlog.n and the GRLoader log messages, which reflect the data values after translation rules have run.

You can run GRLoader with the - T option set to five (5) or greater to display additional debugging information.

Localized CMDB Considerations

When implementing a localized CMDB, you can translate the class and family names from one language to another. Translation rules are provided in the $nxroot/java/lib/GRLoader directory. These rules are named xlate_*xx*_to_*yy*.RUL. *xx* and *yy* represent the language codes (en, fr, es, dm, and so on).

You can expand these rules to accommodate any additional SREL fields.

The XML Header

Following XML coding standards, if the XML content in the rule set contains non-UTF-8 characters, you may require a line at the beginning of the XML translation file that is similar to the following:

<?XML version="1.0" encoding="*codepage*"?>

codepage defines the code page.

Note: For more information about GRLoader XML, see the CMDB Technical Reference (see page 4168) .

Test the Rules

Before running the XML input file through GRLoader, test the rules and view the translation results.

To test the translation rules, run GRLoader without the " - a" or " - n" options.

Running without inserts and updates effectively writes the translated and validated XML to the _err. XML file, where the results of the rule translation can be reviewed.

Run GRLoader from a Remote MDR

You can use GRLoader to copy data from a remote MDR to the CMDB in either of two ways:

- Copy the XML data from the remote system that runs the MDR to the system running CMDB, and then execute GRLoader on the CMDB system.
- Execute GRLoader on the remote MDR system itself.

To prepare to execute GRLoader from a remote system that does not have CMDB installed

1. Verify that the Java Runtime Environment (JRE) version 6.0 or higher is installed and available.
2. Copy the contents of the %NX_ROOT%\java\lib directory from the CMDB system to a directory on the remote system where you want to run it. This remote directory is called % ROOT%.
3. Create a file called NX.ENV in the %ROOT% directory:
   @NX_LOG=path_which_will_contain log files
4. Create directory %ROOT%\site\cfg
5. Create directory %ROOT%\log

To run GRLoader from the remote system, execute the following command:

```
java -Xmx512M -cp %ROOT% -jar %ROOT%/GRLoader.jar -N %ROOT% -u [userid]  - s [server]
-i [other GRLoader options]
```

where %ROOT% is the fully qualified path containing the files that were copied in Step 2.

GRLoader and Multi-Tenancy

Multi-tenancy allows multiple independent tenants to share hardware and application support resources in a single implementation of CMDB. You can use the tenant attribute (<tenant>) in XML so that GRLoader assigns tenants for multi-tenancy use in CMDB. All changes that you make to the tenant attribute are reflected in the CMDB Versioning tab.

The tenant attribute is as follows:

- **<tenant>**
  Specifies the tenant assignment for the CI/Relationship. You can use PUBLIC to specify that the object is public. The Tenant may or may not be set in the object, depending on your default roles tenant access.

Consider the following tenant assignment behavior *before* you implement multi-tenancy using GRLoader:

- Tenants can only be assigned during the creation of a CI or relationship.
- All CIs that GRLoader loads are assigned either a default tenant or a specific one from the XML file.
- GRLoader XML lets you specify the <tenant> attribute or a default tenant for a CI or a relationship.
- If you do not specify <tenant> or a default tenant, the tenant is assumed to be blank and the tenant assignment is based on the logged on users default role. This default role assignment is used primarily for CA Cohesion and other MDRs that do not specify a tenant when creating CIs.
- GRLoader sets the tenant of a CI or relationship based on input from the following sources. When the default role lets you select the choice of tenant in the objects created, you can specifically set the tenant for an object. The multi-tenancy option must be set to setup or on to use <tenant>.
  - Including <tenant> in the xml.
  - Use of the - dt command line option when invoking GRLoader.
  - Use of the grloader.defaulttenant option in the configuration file.
  - The default tenant associated with the contact.

Example: Set the Tenant for an Object

Your default access allows you to create CIs for a specific tenant and for public use. You want to create several public CIs.

Run grloader with a default tenant of PUBLIC to indicate the tenant of the new objects specifically.

Bulk Loading Change Specifications with GRLoader

Contents

- Change Specification Example Spreadsheet (see page 4350)

After a user creates a Change Order, you can use GRLoader to bulk load change specifications, instead of using the web interface. Use the *object* node with the *objecttype* attribute.

You can use the following attributes with GRLoader:

- **objecttype**
  (Required) Identifies the Change Specification.
- **chg**
  (Required) Specifies the Change Order ticket number.
- **ci**
  Specifies the CI name.
- **attribute_name**
  (Required) Specifies the CI attribute that you want to change.
- **attribute_value_planned**
  Specifies the new value of the attribute_name you entered.
- **status**
  Specifies the initial verify status. By default, GRLoader uses the managed attribute initial verify status.
- **description**
  Specifies descriptive text of the change.

Note: Change specifications are not reconciled. If you run GRLoader multiple times with identical input, CACF creates duplicate change specifications. Use the web interface to edit and remove duplicates that CACF creates accidentally. Duplicates are independent of each other.

Change Specification Example XML

The following example XML adds change specifications for a Change Order numbered 24. The changeorder24.xml file specifies that alarm_id becomes server1, and location becomes 2.4.6.8.

```
<GRLoader>
     <object>
        <objecttype>ci_planned_change</objecttype>
        <description>created by grloader *now* </description>
        <attribute_name>alarm_id</attribute_name>
        <chg>24</chg>
        <ci>server1</ci>
        <attribute_value_planned>2.4.6.8</attribute_value_planned>
    </object>
    <object>
        <objecttype>ci_planned_change</objecttype>
     <description>created by grloader *now* </description>
        <attribute_name>location</attribute_name>
        <chg>24</chg>
        <ci>server1</ci>
```

```
        <attribute_value_planned>NY</attribute_value_planned>
    </object>
</GRLoader>
```

Execute the following command:

```
grloader -u ServiceDesk -p password -s http://hostname:8080 -i changeorder24.xml
```

Change Specification Example Spreadsheet

The following example spreadsheet adds Change Specification for a Change Order numbered 24, which assigns new IP addresses and locations to three CIs:

objecttype	chg	CI	attribute_name	attribute_value_planned	description
ci_planned_change	24	server 1	alarm_id	1.1.1.1	loaded by grloader at *now*
ci_planned_change	24	server 2	alarm_id	1.1.1.2	loaded by grloader at *now*
ci_planned_change	24	server 3	alarm_id	1.1.1.3	loaded by grloader at *now*
ci_planned_change	24	server 1	location	NY	loaded by grloader at *now*
ci_planned_change	24	server 2	location	NY	loaded by grloader at *now*
ci_planned_change	24	server 3	location	NY	loaded by grloader at *now*

The GRLoader Command

This article contains the following topics:

The General Resource Loader (GRLoader) imports CI information into CA SDM. GRLoader uses XML documents as input, which lets you import data that originates in different data sources. Run GRLoader from a command prompt or by using a .bat or .cmd file. The CA SDM installation adds the GRLoader to the path during installation, so it runs from any directory.

Results from an import show counts for all processed CIs and Relationships, including the amount of Read, Skipped, Inserts, Updates, Errors, and Warnings. GRLoader logs all processing details and errors in the *nx_root*/log/grloader.log file, where *nx_root* specifies the CA SDM installation directory.

Syntax

```
C:\WINDOWS>GRLoader -?
```

The GRLoader command uses the following parameters:

- **-u *userid***
  (Required) Specifies the user ID that runs the GRLoader process.

- **-p *password***
  (Required) Specifies the password for the user ID. If you run GRLoader without the -p parameter, the utility prompts the console for the password.

- **-s http[s]://*cmdb_servername*:*port***
  (Required) Specifies the server URL including the port number that runs the web services. For running GRLoader on the primary server or application server in a default installation, you can use the following command:

  ```
  -s http://localhost:8080
  ```

  Note: If you specify the optional -C parameter, GRLoader ignores the -s parameter.

- **-i *input_file***
  (Required) Specifies a full path name or a relative path name. If the filename contains a .xls or . xlsx suffix, GRLoader considers the file as a spreadsheet, otherwise it considers it as an XML file.

- **-n**
  (Optional) Allows new CI insertion into the CMDB. Without -n, CIs write to the XML error file (see the -e parameter). Relationships are only added if either -n or -a is specified. If neither is specified, no updates are performed. Updating CIs also require the -a parameter.

- **-a**
  (Optional) Allows updates to configuration items (by default, updates are not allowed if the CI exists in the CMDB). The -n flag also is required to add new CIs.

- **-D**
  (Optional) Specifies a name prefix for relations (defaults to "GRLoader"). Use the prefix for the sym field in new relationships. The sym file must be unique, so a datetime field and a number is appended to this prefix to make it unique.
  Default Prefix: GRLoader.

- **-e *XML_err_file***
  (Optional) Produces an XML error file when GRLoader detects errors or warnings. By default, the error file name uses the name of the input file, appended with _err.xml. For example, using the input file as abc.xml creates the error file as abc_err.xml. Use the -e parameter to override this default name.

- **-E**
  (Optional) Lets you overwrite the XML error file. By default, the error file is not overwritten.

- **-I**
  (Optional) Ignores case. When you use this parameter, GRLoader is not case-sensitive when comparing the input value of a lookup field with the actual value stored in the database. By default, lookups are case-sensitive.

- **-ua**
  Always updates the CMDB.

- **-lftwa [-chg *nnnn*]**
  (Optional) Loads TWA transactions into the CMDB. If used with -chg, the load selects only those transactions associated with change order *nnnn*.

  
  Note: The Change Order string is not validated when loaded into the CMDB.

- **-lftwai [-chg *nnnn*]**
  (Optional) Runs TWA transactions to update the CMDB. Transactions that run successfully are set to Inactive so that they do not appear in lists. If you use -chg, the load selects only those transactions associated with change order *nnnn*.

- **-lttwa**
  (Optional) Loads XML into the transaction work area (TWA) instead of directly into the CMDB. After data has been loaded into the TWA, it can be edited, changed and verified. After the data modification process completes, individual transactions can load into the CMDB (see - lftwa).

- **-lttwar**
  (Optional) Loads XML into the initial state in the transaction work area (TWA) instead of directly into the CMDB. Transaction data in the TWA can be edited, changed, and verified (see -simci and -simrel). After the data modification process completes, individual transactions can load into the CMDB (see - lftwai).

- **-nospinner (-spinner)**
  (Optional) Turns off the spinner that displays CI and relationship progress. Use -spinner to enable the progress display.

- **-P**
  (Optional) Specifies preload data to improve performance for large processing. For large input files, supplying the - P parameter preloads a few tables into memory so that they can be processed more quickly. For smaller inputs (< 50 entries), preload is not necessary.

- **-rs**
  (Optional) Replaces symbolic values that CA SDM includes in the XML input file. If you enable this parameter, corresponding values replace the following symbolic values:

  - *now* -- Replaced by a unique date/time string appended with a sequence number to help ensure uniqueness.
  - *userid* -- Indicates the userid specified in the -u parameter.
  - *inputfile* -- Indicates the filename specified in the -I parameter.

- *relationcount* -- Specifies the number of relationships processed so far in this GRLoader run.
- *lastciuuid* -- Specifies the UUID of the most recently processed CI.
- *cicount* -- Specifies the number of CIs processed so far in this GRLoader run.

Examples: Use the -rs Parameter

With -rs enabled, the following example creates 100 CIs named ci1, ci2, …, ci100

```
<GRLoader>
<ci><name>ci*cicount*</name><class>Server</class></ci>
[...repeated 100 times...]
</GRLoader>
```

With -rs enabled, the following example updates the CI description with information about the most recent update.

```
<GRLoader>
<ci>
<name>server1</name>
<description>updated by *userid* on *now* using input file *inputfile*</description>
</ci>
</GRLoader>
```

- **-simci**
  (Optional) Simulates CI operations to predetermine whether a set of transactions creates CIs, and therefore possible ambiguities for other CIs.
- **-simrel**
  (Optional) Simulates relationship operations to predetermine whether a relationship transaction creates a relationship or updates a relationship.
- **-T *trace_level***
  (Optional) Specifies the tracing level. Known tracing levels are 0 (off, the default), 1 (low), 5 (medium) and 10 (verbose). We recommend only using this setting when necessary because much output can result.
- **-tf *filename***
  (Optional) Runs GRLoader using translation rules. *filename* specifies the name of the file that contains the translation rule set.
- **-slump**
  (Optional) Specifies the slump.jar file. This parameter can provide better performance than web services. **Important:** -slump only can be used with the -s parameter to target the following server:
  - Conventional: Primary server
  - Advanced Availability: Application server.

Note: If another CA product is installed, for example, CA Coheshion ACM or CMDB service pack is installed, verify that the slump.jar file is identical to the one that is installed on the target CA SDM system.

- **-C**
  (Optional) Validates the XML input file without any additional processing. This argument only validates the XML tags, not field values.

- **-h (or -?)**
  (Optional) Displays online help.

- **-v**
  (Optional) Displays the GRLoader product version and build date.

- **-maxerror *number***
  (Optional) Specifies the maximum number of errors that can occur before remaining CIs or relationships are skipped.

- **-maxwarn *number***
  (Optional) Specifies the maximum number of warnings that can occur before remaining CIs or relationships are skipped.

- **-chg *nnnn***
  Used with - lftwa and -lftwar. Loads only those transactions associated with change order *nnnn*.

  Note: The Change Order string is not validated when loaded into the CMDB.

- **-cfg *myconfigfile*.cfg**
  (Optional) Specifies the name of the input configuration file.

- **-dt t*enant***
  (Optional) Specifies the tenant assignment for the CI/relationship. You must enable multi-tenancy to use this parameter. You can use PUBLIC to indicate that the object is public. If the tenant access of the user does not authorize creating public objects, the object is created using the default tenant.

- **-sc classname**

  Lists the attributes of CIs in the class you specify.

- **-scx classname**

  Lists the attributes of CIs in the class you specify in XML format. The XML is stored in a file named classname.xml. Any special characters are removed from the class name.

Example: Load CI and Relationship Data

The following example loads the CI and relationship data contained in the filehardware_servers.xml (in the current directory) into the CMDB that resides on the server located on the local computer on port 8080.

```
grloader -u CMDBAdmin -p password -s http://localhost:8080 -i hardware_servers.xml -n
```

JDBC Database Input Options

The following table lists the options that you use in the configuration file and the corresponding command line options when you input JDBC databases.

Note: If you use SQL Server or Oracle databases, CA SDM includes the required JAR files. If you use other database types, you must use the -addjar option to add support for those databases to GRLoader dynamically. Consult your database vendor documentation for the name and location of the necessary JAR files to use JDBC. You can also consult your database vendor or database administrator for specific values and credentials.

GRLoader Option	Command Line Option	Description
grloader.jdbc.driver=*name*	-dbdriver *name*	Specifies the JDBC driver name. **Note:** This driver must be available on the classpath, similar to -addjar. Consult the database vendor for specific values.
grloader.jdbc.url=*URL*	-dburl *URL*	Specifies the JDBC database URL that describes the location of the database which contains the table you want to load.
grloader.jdbc.user=*name*	-dbuser *name*	Specifies the user ID for the JDBC database.
grloader.jdbc.password=*password*	-dbpswd *password*	Specifies the password for the user ID for the JDBC database.
grloader.jdbc.statement=*statement*	-dbstmt *statement*	Specifies the JDBC statement that describes the columns and selection criteria for the data you want to import. **Note:** The column names used in the query statement must match CMDB attribute names. If these names differ, use the SQL *AS* keyword to map database column names to CMDB attributes.

Spreadsheet Input Options

The following table lists the options that you use in the configuration file and the corresponding command line options when you input spreadsheets. You can also usethe {} symbols as delimiters surrounding the lookup field as well as using the keyword EMPTY.

- **boolean**
  Specifies a value from one the following pairs: 1/0, YES/NO, or TRUE/FALSE.

Note: If the input file name ends in .xls or .xlsx when you use the *grloader.inputfile=name* GRLoader option or the *-i* command line argument, GRLoader assumes that it is a spreadsheet.

GRLoader Option	Command Line Option	Description
grloader.spreadsheet.filename=*name*	-ssf	Specifies the Excel spreadsheet file name when it does not contain the .XLS or .XLSX file extension.
grloader.spreadsheet.sheetname=*name*	-sss	Specifies the sheet name. **Default:** The first sheet in the spreadsheet.
grloader.spreadsheet.firstrow=*n*	-ssfr	Set this value to skip over the first *n-1* rows in the spreadsheet.
grloader.spreadsheet.lastrow=*n*	-sslr	Ignores *rows> n (greater than)* in the spreadsheet.
grloader.spreadsheet.firstcol=*x*	-ssfc	Specifies to start processing on this column. You can express this column as a letter or number, depending on your spreadsheet options.
grloader.spreadsheet.lastcol=*x*	-sslc	Ignores *columns > x (greater than)* in the spreadsheet. You can express this column as a letter or number, depending on your spreadsheet options.
grloader.spreadsheet.embeddedseparator	-sses	Specifies a character to separate multiple values contained in a single cell. This option only applies to the relationship type column in a row with multiple embedded relationships. **Default:** semi-colon ":"
grloader.attributedefault.atrname=*value*	-ad attrname=*value*	Provides a default value if you did not specify one in the input source. **Note:** These values do not undergo attribute name or data value translation. **Note:** When you run GRLoader from a batch file, specify the *-ad attr=value* as *-ad attr{value}* to get past the Windows command parser which may remove the equal "=" symbols.
	-dt	Deprecated. Instead, use the -ad tenant=*name* option.
grloader.maxci=*n*	-maxci	Specifies the maximum number of CIs to import before skipping further CI imports.
grloader.maxrel=*n*	-maxrel	Specifies the maximum number of relationships to import before skipping further relationship imports.
N/A	-sc *classname*	Lists the attirbutes of CIs in the class you specify.

GRLoader Option	Command Line Option	Description
N/A	-scx *classname*	Lists the attributes of CIs in the class you specify in XML format.
grloader.workarea.changeorderrequired=*boolean*	-cor	If set to yes, TWA transactions that do not contain a non-blank change order number are ignored.
grloader.ignoreinvalidattributes=*boolean*	-iia	Specifies if you want to ignore invalid attributes. This command suppresses all warning messages about invalid attribute names.

CSV Input Options

The following table lists the options that you use in the configuration file and the corresponding command line options when you input CSV files.

Note: If required, consult your database vendor or database administrator for specific values and credentials.

GRLoader Option	Command Line Option	Description
-i		GRLoader assumes that a file ending in .csv is a CSV file.
grloader.csv.filename=*name*	-csvf *name*	Specifies the filename when it does not end in .csv.
grloader.csv.separator=*x*	-csvsep *x*	Specifies when the CSV file uses other than comma delimiters. You can specify a single character, such as a Tab (\t) or a semicolon.
grloader.csv.escape=*x*	-csvesc *x*	Specifies when the CSV file uses an escape character (\).
grloader.csv.comment=*x*	-csvcom *x*	Specifies when the CSV file uses the comment character (#).
grloader.csv.quote=*x*	-csvquote *x*	Specifies when the CSV file uses the quote character (").

TWA Input Options

The following table lists the options that you use in the configuration file and the corresponding command line options when you input from the TWA.

GRLoader Option	Command Line Option	Description
grloader.workarea.changeorderrequired=yes/no	-cor	GRLoader ignores TWA transactions that do not contain a non-blank Change Order number.

GRLoader Option	Command Line Option	Description

General Options

The following table lists the options that you use in the configuration file and the corresponding command line options when you input from all inputs.

Note: If necessary, consult your database vendor or database administrator for specific values and credentials.

GRLoader Option	Command Line Option	Description
grloader.system.addjar=*xx;yy;zz*	-addjar *xx*	Adds JAR files to the GRLoader classpath. You can use this option with -jdbcdriver. **Note:** The grloader.system.addjar option can only appear once in the configuration file. You can add multiple jars through grloader.system.addjar by separating the filenames with a semi-colon. This option only specifies a single jar file, and you can specify it as many times as required.
grloader.attributedefault.attrname=*value*	-ad attrname=*value*	Provides a default value if you did not specify a value in the input source. **Note:** These values do not undergo attribute name or data value translation. When you run GRLoaderfrom from a batch file, specify -ad attr=value as *-ad attr{value}.* The Windows command parser can delete the equals symbol.
N/A	-ad tenant=*name*	Specifies the tenant name.
grloader.maxci=*n*	-maxci *n*	Specifies the maximum number of CIs to import before skipping further CI imports.
grloader.maxrel=*n*	-maxrel *n*	Specifies the maximum number of relationships to import before skipping further relationship imports.
N/A	-sc *xx*	Lists attributes of CIs in the class *xx*.
N/A	-scx *xx*	Lists attributes of CIs in class *xx* in XML format.
grloader.reader.allowembeddedrelationships=yes/no	-aer	Allows embedded relationships. **Default:** Yes For backward compatibility only
grloader.ignoreinvalidattributes=yes/no	-iia	Ignores invalid attributes by suppressing all warning messages about invalid attribute names.

GRLoader Option	Command Line Option	Description
grloader.updatealways=yes/no		

Example Display CI Class Attributes

When you create input for GRLoader, list the attributes associated with a specific class.

To list the attributes, execute the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080 -sc [class name]
```

- **sc**
  Lists attributes of CIs in a class that you specify.

- **class name**
  Specifies any valid CA CMDB class name.

Example: List Attributes for Class Server

```
grloader  - u username  - p password  - s http://sdm-host:8080 -sc Server

10:33:01.997 CI and Relationship Loader for CA Service Desk Manager

List of attributes in class(Server) extension(har_serx)

ATTRIBUTE NAME                    DATA TYPE
acquire_date                      Date
active_date                       Date
alarm_id                          STRING(64)
ambiguity                         Integer
asset_count                       Integer
asset_num                         STRING(64)
audit_userid                      SREL(cnt.combo_name)
```

Example Display CI Class Attributes in XML Format

When you create input for GRLoader, list the attributes associated with a specific class in XML format. The command creates the file [class name].xml with the result.

To list the attributes in XML format, execute the following command:

```
grloader  - u username  - p password  - s http://sdm-host:8080 -scx [class name]
```

- **scx**
  Lists attributes of CIs in XML format in a class that you specify.

- **class name**
  Specifies any valid CA CMDB class name.

Example: List Attributes for Class Server

```
grloader  - u username  - p password  - s http://sdm-host:8080 -scx Server

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<GRLoader>
 <ci>
    <acquire_date></acquire_date>                       <!-- Date -->
    <active_date></active_date>                         <!-- Date -->
    <alarm_id></alarm_id>                               <!-- String(64) -->
    <ambiguity></ambiguity>                             <!-- Integer -->
    <asset_count></asset_count>                         <!-- Integer -->
    <asset_num></asset_num>                             <!-- String(64) -->
    <audit_userid lookup="combo_name"></audit_userid>   <!-- SREL cnt -->
```

Note: If the class name contains special characters, they are removed.

CI Reconciliation

CI Reconciliation Attributes

Reconciliation associates imported CI data with CIs in the CMDB.

Reconciliation uses the following CI identifying attributes:

- Name
- Serial Number
- Asset Number
- System Name
- DNS Name
- MAC Address

You must specify at least one of these values when you create or reference an existing CI.

The following table shows the results of the reconciliation process:

Name	Serial Number	Asset Number	System Name	DNS Name	MAC Address	Result
Unique	Null	Null	Null	Null	Null	CI Created
Null	Unique	Null	Null	Null	Null	CI Created
Null	Null	Unique	Null	Null	Null	CI Created

Name	Serial Number	Asset Number	System Name	DNS Name	MAC Address	Result
Null	Null	Null	Unique	Null	Null	CI Created
Null	Null	Null	Null	Unique	Null	CI Created
Null	Null	Null	Null	Null	Unique	CI Created
Duplicate	Duplicate	Duplicate	Unique	Duplicate	Duplicate	CI Created
Unique	Duplicate	Duplicate	Duplicate	Duplicate	Duplicate	Recognized as Duplicate CI
Null	Null	Null	Null	Unique	Unique	CI Created
Null	Null	Null	Null	Duplicate	Unique	Recognized as Duplicate CI
Null	Null	Null	Null	Unique	Duplicate	Recognized as Duplicate CI
Duplicate	Duplicate	Unique	Duplicate	Duplicate	Duplicate	CI Created
Duplicate	Unique	Duplicate	Duplicate	Duplicate	Duplicate	CI Created
Duplicate	Duplicate	Duplicate	Duplicate	Duplicate	Unique	Recognized as Duplicate CI
Duplicate	Duplicate	Duplicate	Duplicate	Unique	Duplicate	Recognized as Duplicate CI
Duplicate	Duplicate	Duplicate	Duplicate	Unique	Unique	Recognized as Duplicate CI

Transaction Work Area Attributes

Contents

The Transaction Work Area (twa) tables are:

- **ci_twa_ci**
  A single table that includes all attributes across all CA CMDB families. Table data is stored in denormalized form to enable customers and services to understand and manipulate the content more easily.

- **ci_twa_relation**
  Complements the ci_twa_ci table. Contains relationship information.

- **ci_twa_statusnames**
  Descriptive labels for row status.

External processes update these tables and GRLoader reads them during transaction processing. When processing is complete, GRLoader updates the row_status and tran_message columns to indicate whether the transaction has completed successfully.

Note: If multiple errors or warnings occur, the messages are concatenated.

ci_twa_ci Attributes

The ci_twa_ci table contains attributes for CI transactions.

Column Name	Notes
id	Transaction identifier
last_mod_dt	Sets the current date every time the row is added or updated.
tran_dt	Sets the current date and time if no value is supplied when row is added.
creation_date	Sets the current date and time when row is added.
delete_flag	Sets to zero (0) if no other value is supplied when row is added.
tran_status	Sets to zero (0) if no other value is supplied when row is added.

ci_twa_relation Attributes

The ci_twa_relation table contains attributes for relationship transactions.

Column Name	Notes
id	Transaction identifier
last_mod_dt	Sets the current date every time the row is added or updated.
tran_dt	Sets the current date and time if no value is supplied when row is added.
creation_date	Sets the current date and time when row is added.
delete_flag	Sets to zero (0) if no other value is supplied when row is added.
tran_status	Set to zero (0) if no other value is supplied when row is added.

CMDB Web Services

CA CMDB provides a set of high-level web services that supports CMDBf Web Services Standard version 1.0. These services allow external CMDBf-aligned applications and also registered Management Data Repositories (MDRs) to interact with CA CMDB, including federated MDRs in accordance with the CMDBf/DMTF standard.

You can find the CMDBf specification in the following document:

`http://cmdbf.org/schema/1-0-0/CMDBf%20v1.0.pdf`

Web Services Deployment

CMDB installation automatically deploys CMDB web services. If you want, you can redeploy the web services.

To redeploy CMDB Web Services

1. Execute the following command:
   : install-dir \sdk\websvc\cmdbf

2. Deploy the following files:

   - deploy.wsdd

   - cmdbf.jar

3. Execute the following file:
   deploy_cmdbws.bat
   The CMDB web services are deployed.

Web Service Components

Contents

CA CMDB Web Services consists of two defined services:

- **Registration Service**
  Allows clients to create\update CIs and Relationships. The endpoint can be located at the following address:

  ```
  http://<servername>:< port >/axis/services/RegistrationPort
  ```

- **Query Service**
  Allows clients to query for CIs and Relationships. The endpoint can be located at the following address:

  ```
  http://<servername>:< port >/axis/services/QueryPort
  ```

Registration Service

The Registration service uses push mode federation. The fundamentals of push mode federation are as follows:

- The client invokes the Register operation for configuration items or relationships that it wants to register. Each item or relationship must be associated with at least one record type supported by the Registration service.

  Note: The CMDBf Register web service either creates a new CI or, if that CI already exists, updates it. If the CI already exists and is Inactive, the CI is set to Active and all attributes passed to it are updated. To prevent updates to Inactive CIs, send Inactive as one of the attributes.

- The Registration service responds with the registration status for each item or relationship named in the Register operation. The status is either accepted or declined.

The management data repository (MDR) also uses the Register operation to update registered data. An update can consist of any combination of the following:

- Changes to existing data, such as a property value change
- Deregistering a previously registered record type for this configuration item or relationship

MDR Registration

You must do the following to register an MDR:

1. Create a valid MDR manually before using CMDBf web services to register a CI.
2. Set the MdrName to your MDR Name.
3. Set the MdrClass to “cmdbf” (a static value).

Query Service

The Query service contains a GraphQuery operation that can be used for anything from a simple instance query to a much more complex topological query. A GraphQuery request describes items and relationships of interest in the form of a graph. Constraints can be applied to the nodes (items) and edges (relationships) in that graph to further refine them.

The GraphQuery response contains the items and relationships that, in combination, compose a graph that satisfies the constraints of the graph in the query. A graph query is only one level deep.

Login

You log in by passing credential information either through Java or a SOAP message. The following examples show you how you can log in.

Example: Java

```
QueryBindingStub binding;

binding = (QueryBindingStub) new QueryServiceLocator().getQueryPort(new URL
(Endpoint));

SOAPHeaderElement Header = new SOAPHeaderElement("http://schemas.xmlsoap.org/soap
/envelope/", "securityHeader");

Header.setPrefix("sec");

javax.xml.soap.SOAPElement Element = null;

Element = Header.addChildElement("username");
Element.addTextNode("CMDBAdmin");
Element = Header.addChildElement("password");
Element.addTextNode("password");
```

```
binding.setHeader(Header);
```

Example: SOAP Message

```
<soapenv:Header>
        <sec:securityHeader  xmlns:sec="http://schemas.xmlsoap.org/soap/enveloe/">
        <sec:username>CMDBAdmin</sec:username>
        <sec:password>password</sec:password>
        </sec:securityHeader>
        </soapenv:Header>
```

CA CMDB Web Services Access

Contents

You can access CMDB web services by using one of the following methods:

- Create your own message for the SOAP interface to call your endpoint.
- Write your own Java program to access the CMDB endpoint.

Code to Return All CIs From Every Family in CMDB

You can use the following code to return all CIs from every Family in CMDB:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:
dat="http://cmdbf.org/schema/1-0-0/datamodel">
   <soapenv:Header>
        <sec:securityHeader xmlns:sec="http://schemas.xmlsoap.org/soap/envelope/">
                <sec:username>cmdbadmin</sec:username>
                <sec:password>miramar</sec:password>
        </sec:securityHeader>
   </soapenv:Header>
   <soapenv:Body>
      <dat:query>
        <itemTemplate suppressFromResult="false" id="All">
[constraints go here]
         </itemTemplate>
      </dat:query>
   </soapenv:Body>
</soapenv:Envelope>
//*********************************************//
```

Sample Java Program

To assist you with web services client application development, CMDB provides the following sample Java programs:

- RegistrationServiceTestCase.java shows you how to create two CIs and a Relationship.
- QueryServiceTestCase.java shows you how to query your CMDB for all CIs.

You can find sample programs at the following location:

```
%NX_ROOT%\sdk\websvc\cmdbf\
```

WSDL Document

The location of the Web Services Description Language (WSDL) document that you need depends on the function of CMDB you intend to use. The following locations are available:

- The default location of the WSDL for the CMDBf Web Services for Registration is the following URL:

  ```
  http://<servername>:<port>/axis /services/RegistrationPort?wsdl
  ```

- The default location of the WSDL for the CMDBf Web Services for graphQuery is the following URL:

  ```
  http://<servername>:<port>/axis/services/QueryPort?wsdl
  ```

Note: Many servlet containers use a port number different from 80. For example, Tomcat defaults to port 8080, which is established during installation.

Security Considerations

There are important security considerations when deploying web services. The default configuration when using HTTP is insecure, as it is for all information in web service calls sent between the client and the server in plain text over the network using the HTTP protocol. This configuration includes application data and login methods, and it can include passwords. Administrators who deploy web services are encouraged to consider security carefully and to take additional configuration steps at the application and network levels to secure your web service environment.

Important! The default web service configuration used with HTTP is insecure and vulnerable to security threats that can include password discovery, session fixation, and data spying, and so on.

CMDBf Implementation CA CMDB Limitations

Contents

CMDB has limitations in its CMDBf implementation. The following CMDBf pseudo-schema highlights some limitation areas:

```
<query>
        <itemTemplate id="xs:ID" suppressFromResult="xs:boolean">
                (<contentSelector ...>...</contentSelector> ?
                <instanceIdConstraint>...</instanceIdConstraint> ?
                <recordConstraint>
                        <recordType ... /> *
                        <propertyValue ...>...</propertyValue> *
                </recordConstraint> *)
                |
                (<xpathExpression...>...</xpathExpression> *)
                xs:any
        </itemTemplate> *
        <relationshipTemplate id="xs:ID" suppressFromResult="xs:boolean">
                (<contentSelector ...>...</contentSelector> ?
                <instanceIdConstraint>...</instanceIdConstraint> ?
                <recordConstraint>
                        <recordType>...</recordType> *
                        <propertyValue>...</propertyValue> *
                </recordConstraint> *)
                |
                (<xpathExpression ...>...</xpathExpression> *)
                <sourceTemplate ref="xs:IDREF" minimum="xs:int"?
                 maximum="xs:int"?/>
                <targetTemplate ref="xs:IDREF" minimum="xs:int"?
                 maximum="xs:int"?/>
                <depthLimit ... /> ?
                xs:any
        </relationshipTemplate> *
</query>
```

Item Template Limitations

The CMDB implementation uses the CMDBf specification with the following item template limitations:

- Multiple RecordConstraints under one ItemTemplate are handled as Logical OR, not Logical AND.
- suppressFromResult="xs:boolean" is not supported.
  CMDB always displays the results.
- <contentSelector matchedRecords="xs:*boolean*">:matchedRecords="true" is supported, but matchedRecords="false" is not.
  CMDB only supports one selectedRecordType per contentSelector.
- <recordConstraint> only supports one <recordType ... /> expression; for example <recordType namespace="http://cmdb.ca.com/Hardware" localName="Hardware.Server"/>
  The localName expression must identify a valid CMDB family.
  Replace each space in a family name that includes spaces with a dash (-). For example, replace Software.Application Server with Software.Application-Server.

- <propertyValue namespace="xs:anyURI" localName="xs:NCName" recordMetadata="xs:boolean" matchAny="xs:boolean">
  recordMetadata is not supported.
  matchAny is set to the default value of false; this value allows "Logical AND" and "Logical OR" CMDBf queries on all the property values. "Logical AND" queries are not supported.
  “like” operators are not supported.
  “equals” does not support caseSensitive, or negate.

- <xpathExpression...>...</xpathExpression>: is not implemented.

Registration Limitations

Registration has the following limitations:

- Multiple record elements under one Item element or Relationship element
- Additional RecordType

Relationship Template Support and Limitations

CMDB supports the following relationshipTemplate features:

- contentSelector
- relationshipTemplate ID
- recordConstraint -- can use propertySelectors
- sourceTemplate
- targetTemplate

CMDB *does not* support the following relationshipTemplate features:

- Source/Target Template @minimum
- Source/Target Template @maximum
- Depth Limit with @MaxIntermediateItems
- Depth Limit with @intermediateItem Template
- instanceIdConstraint
- xpathExpression
- suppressFromResult in relationship Template

Example: Register Request relationshipTemplate Using a contentSelector and propertySelectors Under the recordConstraint

```
<relationshipTemplate  id="rels">
            <contentSelector>
```

```
                    <selectedRecordType namespace=" http://cmdb.ca.com/r1"
localName="is-deployed-by">
                              <selectedProperty namespace=" http://cmdb.ca.com/r1"
localName="last_mod_by"/>
                              <selectedProperty namespace=" http://cmdb.ca.com/r1"
localName="last_mod_dt"/>
                              <selectedProperty namespace=" http://cmdb.ca.com/r1"
localName="child"/>
                              <selectedProperty namespace=" http://cmdb.ca.com/r1"
localName="parent"/>
                    </selectedRecordType>
               </contentSelector>
                               <sourceTemplate ref="Linux1" />
                               <targetTemplate ref="Linux2" />
                               <recordConstraint>
                                    <recordType namespace=" http://cmdb.ca.com/r1"
localName="is-deployed-by"/>
                                         <propertyValue namespace=" http://cmdb.ca.com
/r1" localName="parent" matchAny="true">
                                         <equal>test</equal>
                                         </propertyValue>
                                </recordConstraint>
</relationshipTemplate>
```

Example: Response (edges portion)

```
<edges templateId="rels">
         <relationship xsi:type="ns3:RelationshipType" xmlns:ns3="http://cmdbf.org
/schema/1-0-0/datamodel">
               <source>
                    <mdrId xsi:type="xsd:string">http://cmdb.ca.com/r1</mdrId>
                    <localId xsi:type="xsd:string">nr:
C2B975A96C03934BA61080C0F79C8BD2</localId>
               </source>
               <target>
                    <mdrId xsi:type="xsd:string">http://cmdb.ca.com/r1</mdrId>
                    <localId xsi:type="xsd:string">nr:
B985B5297C46224283D0E5F2632A2A44</localId>
               </target>
               <record xsi:type="ns3:RecordType">
                    <recordMetadata>
                        <recordId xsi:type="xsd:string">bmhier:400004</recordId>
                    </recordMetadata>
                  <is-deployed-by xmlns="http://cmdb.ca.com/r1/is-deployed-by">
                     <child>ali5</child>
                     <last_mod_dt>6 Oct 2008 16:34:48 GMT</last_mod_dt>
                     <parent>ali</parent>
                     <last_mod_by>ServiceDesk</last_mod_by>
                  </is-deployed-by>
               </record>
               <instanceId xsi:type="ns3:MdrScopedIdType">
                  <mdrId xsi:type="xsd:string">http://cmdb.ca.com/r1</mdrId>
                  <localId xsi:type="xsd:string">bmhier:400004</localId>
```

```
                </instanceId>
            </relationship>
</edges>
```

Generic Limitations

The following generic limitations apply:

- <recordMetadata>
  <recordId>...</recordId>
  <lastModified>...</lastModified> ?
  <baselineId>...</baselineId> ?
  <snapshotId>...</snapshotId> ?
  xs:any </recordMetadata>:

  Note: recordMetadata only returns recordId, and the xs:any.

  Other values have no meaning to CMDB.

- CMDB does not support case-sensitivity for the equal, contains, and like operators.
- CMDB does not support escape sequences as unique wild card characters.
- CMDBf supports XSD date and XSD dateTime formats:
  "YYYY-MM-DD" -XSD date
  "YYYY-MM-DDThh:mm:ss" -XSD dateTime

Date Data Type

The Date Data type is specified in the following form:

YYYY-MM-DD

where:

- **YYYY**
  Specifies the year.
- **MM**
  Specifies the month.
- **DD**
  Specifies the day of the month.

Note: All components are required.

DateTime Data Type

The DateTime data type is used to specify both a date and a time on that date.

dateTime is specified in the following form:

YYYY-MM-DDThh:mm:ss

where:

- **YYYY**
  Specifies the year.
- **MM**
  Specifies the month.
- **DD**
  Specifies the day.
- **T**
  Specifies the start of the required time section.
- **hh**
  Specifies the hour.
- **mm**
  Specifies the minute.
- **ss**
  Specifies the second.

Note: All components are required.

Multi-Tenancy and CIs

How Multi-Tenancy Affects CIs

The following CA CMDB objects are *tenanted*:

- CIs and their associated extension tables
- CI relationships
- Management Data Repository (MDR) providers
- MDR mappings

To create, edit, and list CIs effectively, you must understand how multi-tenancy affects CIs. When you create, list, or update CIs, consider the following:

- When multi-tenancy is installed, the Role Detail form includes Tenant Access and Tenant Write Access drop-down lists on its Authorization tab that contains the following options:
  - Contact's Tenant
  - Single Tenant
  - Tenant Group
  - All Tenants

  The specified Tenant Access affects how you can work with CIs in the CA CMDB-related applications.
- If the Tenant Access or Tenant Write Access type is not specified for the contact, the default role is used.
- On the Role Detail form, the Update Public check box controls whether a user in the role is authorized to create or update public data. This check box is effective only for users associated with the service provider, as tenant users are restricted to read-only access to data not belonging to their tenant.

Important! Users associated with a tenant other than the service provider can only create or update objects associated with their own tenant unless authorized by their role. Users associated with the service provider are permitted to create or update objects belonging to tenants other than their own.

CI Lists and Multi-Tenancy Relationships

The following table shows the results of listing CIs in CA CMDB-related applications with multi-tenancy enabled.

This table is a partial listing of the many possible combinations of role access options, and how they affect the various applications.

Role Tenant Access Option	Web UI	CA APM	Visualizer	GRLoader	CA Cohesion ACM
Contact's Tenant	Lists CIs in the same tenant and public	Lists all CIs	Lists CIs in the same tenant and public	Lists CIs in the same tenant and public	Lists CIs in the same tenant and public
Single Tenant	Lists CIs in the same tenant and public	Lists all CIs	Lists CIs in the same tenant and public	Lists CIs in the same tenant and public	Lists CIs in the same tenant and public
Tenant Group					

Role Tenant Access Option	Web UI	CA APM	Visualizer	GRLoader	CA Cohesion ACM
	Lists CIs in the all tenants in a tenant group and public	Lists all CIs	Lists CIs in the all tenants in a tenant group and public	Lists CIs in the all tenants in a tenant group and public	Lists CIs in the all tenants in a tenant group and public
All Tenants	Lists all CIs	Lists all CIs	Lists all CIs	Lists all CIs	Lists all CIs

CI Creation and Multi-Tenancy Relationships

The following table shows the results of creating CIs in CA CMDB-related applications with multi-tenancy enabled.

This table is a partial listing of the many possible combinations of role access options, and how they affect the various applications.

Role Tenant Access Option	Web UI	CA APM	Visualizer	GRLoader	CA Cohesion ACM
Contact's Tenant	CI tenant is the one assigned to the signed-on user	CI tenant is created as public	Uses the Web UI to create CIs	CI tenant is the default tenant associated with the signed-on user **Note:** We recommend that you set up a distinct contact for every data source. The contact definition should specify a role that is Contact's Tenant.	CI tenant is the one assigned to the signed-on user
Single Tenant	CI tenant is the one assigned to the signed-on user's proxy	CI tenant is created as public	Uses the Web UI to create CIs	CI tenant is the default tenant associated with the signed-on user **Note:** We recommend that you set up a distinct contact for every data source. The contact definition should specify a role which is contact-tenant.	CI tenant is the one assigned to the signed-on user's proxy
Tenant Group	CI tenant can be selected from list in the UI that includes only those tenants in the group **Note:** The default tenant can be overridden by using the GRLoader -dt option.	CI tenant is created as public	Uses the Web UI to create CIs	Can use the <tenant> option to assign a tenant. **Note:** We recommend that you set up a distinct contact for every data source. The contact definition should specify a role which is contact-tenant.	CI is created as public unless -dt is specified
All Tenants	CI tenant can be selected from a list in the UI	CI tenant is		Can use the <tenant> option to assign a tenant. If a tenant is not specified, the default is public.	

Role Tenant Access Option	Web UI	CA APM	Visualizer	GRLoader	CA Cohesion ACM
		created as public	Uses the Web UI to create CIs	**Note:** We recommend that you set up a distinct contact for every data source. The contact definition should specify a role that is Contact's Tenant.	CI is created as public unless -dt is specified

CI Update and Multi-Tenancy Relationships

The following table shows the results of updating CIs in CA CMDB-related applications with multi-tenancy enabled. Consider the following when you update CIs:

- Only CIs that can be listed can be updated.
- The tenant attribute can only be changed by using the command line.
- CA Cohesion ACM does not populate the <tenant> attribute.

This table is a partial listing of the many possible combinations of role access options, and how they affect the various applications.

Role Tenant Access Option	Web UI	CA APM	Visualizer	GRLoader	CA Cohesion ACM
Contact's Tenant	Can update a CI in same tenant Role and service provider determine the public read /write access	Can update any CI	Uses the Web UI to update CIs	Can update a CI in same tenant Role and service provider determine the public read/write access	Can update a CI in same tenant Role and service provider determine the public read/write access
Single Tenant	Can update a CI in same tenant Role and service provider determine the public read /write access	Can update any CI	Uses the Web UI to update CIs	Can update a CI in same tenant Role and service provider determine the public read/write access	Can update a CI in same tenant Role and service provider determine the public read/write access
Tenant Group	Can update a CI in same tenant Cannot update CIs in the tenant group Role and service provider determine the public read /write access CI relationship updates across tenants requires that the contact must be a service provider tenant	Can update any CI	Uses the Web UI to update CIs	Can update a CI in same tenant Cannot update CIs in the tenant group Role and service provider determine the public read/write access CI relationship updates across tenants requires that the contact must be a service provider tenant	Can update a CI in same tenant Cannot update CIs in the tenant group Role and service provider determine the public read/write access CI relationship updates across tenants requires that the contact must be a service provider tenant

Role Tenant Access Option	Web UI	CA APM	Visualizer	GRLoader	CA Cohesion ACM
All Tenants	Can update any CI	Can update any CI	Uses the Web UI to update CIs	Can update any CI	Can update any CI

Generate API Documentation for RESTful Services

You can use jax-doclets-0.9.0.jar file (Third-party product) to generate the API documentation for all the CA Service Desk Manager RESTful services. This library file also dynamically generates the API documentation during the product customizations.

Complete the following steps in CA SDM to deploy the jax-doclets-0.9.0.jar library file:

Note: The Third-party product (jax-doclets-.0.9.0.jar) is available as a separate media and is not included with the CA Service Desk Manager DVD1 media.

Follow these steps:

1. Log in to the CA SDM server where RESTful web services are deployed.
2. Copy the jax-doclets-0.9.0.jar file to the NX_ROOT/java/lib directory.
3. Undeploy the RESTful Web Services by executing the following command from the NX_ROOT /bin directory:

   ```
   (Windows) pdm_rest_util.cmd –undeploy
   (UNIX) ./pdm_rest_util.sh –undeploy
   ```

4. Deploy the RESTful Web Services by executing the following command from the NX_ROOT/bin directory:

   ```
   (Windows) pdm_rest_util.cmd –deploy
   (UNIX) ./pdm_rest_util.sh –deploy
   ```

   After the RESTful Web Services are deployed successfully, the REST docs will be available in the NX_ROOT/Doc folder.

5. Repeat steps 1-4 on all the CA SDM servers where RESTful web services are deployed.

Objects and Attributes

This page lists the objects and attributes that define CA SDM. The system uses objects and attributes to build notification text, scoreboard queries, and data partition constraints. The *FACTORY Optional* statement that accompanies each object, defines access to the object, including its relation attribute, a common name, the security group that can access it, the type of lists produced, and how those lists can be sorted. If omitted, the object is treated according to default specifications.

Note: When an object is documented as a containing a LOCAL *DB Field*, the attribute maps to a local variable instead of a database column. Objects that are documented as a BREL *Data Type*, refer to a backward single relationship (SREL). For more information about default specifications and detailed lists of the attributes of each object, see the chapter "Object Definition Syntax."

This article contains the following topics:

attached_sla Object

The object details are as follows:

1. Associated Table: Attached_SLA
2. Factories: default, ttv_slas
3. REL_ATTR: id
4. Common Name: ticket_type
5. Function Group:

6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
_mapped_chg	_mapped_chg	INTEGER	chg id	
_mapped_cr	_mapped_cr	STRING	call_req persid	
_mapped_iss	_mapped_iss	STRING	issue persistent_id	
_mapped_iss_wf	_mapped_iss_wf	INTEGER	isswf id	
_mapped_wf	_mapped_wf	INTEGER	wf id	
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
last_ttv_upd	last_ttv_upd	LOCAL_TIME		
map_sdsc	map_sdsc	STRING	srv_desc code	REQUIRED
persistent_id	persid	STRING		
sla_viol_status	sla_viol_status	INTEGER		
ticket_id	ticket_id	INTEGER		REQUIRED S_KEY
ticket_type	ticket_type	STRING		REQUIRED
time_to_violation	time_to_violation	LOCAL_TIME		
ttv_event	ttv_event	STRING	att_evt persid	

attr_control Object

The object details are as follows:

1. Associated Tables: dependent_control and usp_attr_control
2. Factories: default
3. REL_ATTR: id
4. Common Name: attrname

Function Group: admin

REST Operations: CREATE READ UPDATE

Attribute	Data Type	SREL References	Flags
control		SREL dependent_control	Dependent control
attrname	STRING		Name of controlled attribute
locked	INTEGER		1 = attribute is read-only
required	INTEGER		1= attribute is required
delete_flag	INTEGER	SREL actbool	Required; on new default: 0

Attribute	Data Type	SREL References	Flags
last_mod_by		SREL cnt	On new default user; on CI set user
last_mod_dt	DATE		On CI set now

auto_close Object

The object details are as follows:

1. Associated Table: usp_auto_close
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. Tenant: optional
7. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
sys	symbol	STRING		Required
cr_ach	request	INTEGER		Required On new default: 0
in_ach	incident	INTEGER		Required On new default: 0
pr_ach	problem	INTEGER		Required On new default: 0
chg_ach	change order	INTEGER		Required On new default: 0
iss_ach	issue	INTEGER		Required On new default: 0
delete_flag		INTEGER	actbool	On CI set now
description	description	STRING		
last_mod_dt		DATE		On CI set now
last_mod_by		DATE	cnt	On CI set user On new default user

aty Object

The object details are as follows:

1. Associated Table: Act_Type
2. Factories: default, chgaty, craty, issaty, mgsaty

3. REL_ATTR: code
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
chg_default_ survey	chg_default_survey	INTEGER	survey_tpl id	
chg_notify_info	chg_notify_info	STRING	splmac persid	
chg_send_ survey	chg_send_survey	INTEGER		
chg_survey_ method	chg_survey_ method	INTEGER	ct_mth id	
chg_survey_ msgbody	chg_survey_ msgbody	STRING		
chg_survey_ msgtitle	chg_survey_msgtitl	STRING		
code	code	STRING		UNIQUE REQUIRED S_KEY
cr_default_ survey	cr_default_survey	INTEGER	survey_tpl id	
cr_notify_info	cr_notify_info	STRING	splmac persid	
cr_send_survey	cr_send_survey	INTEGER		
cr_survey_method	cr_survey_method	INTEGER	ct_mth id	
cr_survey_msgbody	cr_survey_msgbody	STRING		
cr_survey_msgtitle	cr_survey_msgtitle	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
description	description	STRING		
cr_flag	flag1	INTEGER	bool_tab enum	
chg_flag	flag2	INTEGER	bool_tab enum	
iss_flag	flag3	INTEGER	bool_tab enum	
mgs_flag	flag4	INTEGER	bool_tab enum	
kd_flag	flag5	INTEGER	bool_tab enum	
id	id	INTEGER		UNIQUE REQUIRED KEY
internal	internal	INTEGER		
iss_default_survey	iss_default_survey	INTEGER	survey_tpl id	
iss_notify_info	iss_notify_info	STRING	splmac persid	
iss_send_ survey	iss_send_survey	INTEGER		
iss_survey_ method	iss_survey_method	INTEGER	ct_mth id	
iss_survey_ msgbody	iss_survey_ msgbody	STRING		
iss_survey_ msgtitle	iss_survey_msgtitl	STRING		
kd_notify_info	kd_notify_info	STRING	splmac persid	

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_dt	last_mod_dt	LOCAL_TIME		
mgs_notify_info	mgs_notify_info	STRING	splmac persid	
notify_msg_ack	notify_ack	STRING		
persistent_id	persid	STRING		
sym	sym	STRING		REQUIRED S_KEY

audlog Object

The object details are as follows:

1. Associated Table: Audit_Log
2. Factories: default
3. REL_ATTR: code
4. Common Name: audobj_persid
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
analyst	analyst	UUID	ca_contact uuid	
attr_after_val	attr_after_val	STRING		
attr_before_val	attr_before_val	STRING		
attr_name	attr_name	STRING		
aud_opr	aud_opr	INTEGER		
audobj_name	audobj_name	STRING		
audobj_persid	audobj_persid	STRING		
audobj_trkid	audobj_trkid	STRING		
audobj_uniqueid	audobj_uniqueid	STRING		
change_date	change_date	LOCAL_TIME		
id	id	INTEGER		UNIQUE REQUIRED KEY
int1_rsrved	int1_rsrved	INTEGER		
int2_rsrved	int2_rsrved	INTEGER		
persistent_id	persid	STRING		
str1_rsrved	str1_rsrved	STRING		

bhvtpl Object

The object details are as follows:

1. Associated Table: Behavior_Template
2. Factories: default
3. REL_ATTR: id
4. Common Name: description
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
context_attrname	context_attrname	STRING		
context_attrval	context_attrval	INTEGER		
context_type	context_type	STRING		REQUIRED
delete_flag	del	INTEGER	actbool enum	REQUIRED
description	description	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
modified_date	last_mod_dt	LOCAL_TIME		
macro_condition	macro_condition	STRING	splmac persid	
object_id	object_id	INTEGER		REQUIRED
object_type	object_type	STRING		REQUIRED
persistent_id	persid	STRING		
transition_errmsg	transition_errmsg	STRING		
transition_test	transition_test	STRING	splmac persid	

BU_TRANS Object

The object details are as follows:

1. Associated Table: BU_TRANS
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Document Hit Date	BU_DATE	LOCAL_TIME		
Processed by Bubble Up Flag	BU_PROCESSED	INTEGER		
Document Rating	BU_RATING	REAL		
Document ID	DOC_ID	INTEGER	SKELETONS id	
No Rating Flag	HIT_NO_VOTE	INTEGER		
Hit Origin	HIT_ORIGIN	INTEGER		
id	ID	INTEGER		REQUIRED KEY
Category Id	INDEX_ID	INTEGER	O_INDEXES id	
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Contact ID	USER_ID	UUID	ca_contact uuid	

ADMIN_TREE Object

The object details are as follows:

1. Associated Table: admin_tree
2. Factories: default
3. REL_ATTR: id
4. Common Name: CAPTION
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
CAPTION	CAPTION	STRING		
DESCRIPTION	DESCRIPTION	STRING		
HAS_CHILDREN	HAS_CHILDREN	INTEGER		
id	ID	INTEGER		KEY
KT_ADMIN	KT_ADMIN	INTEGER		
KT_KS_CAPTION	KT_KS_CAPTION	STRING		
KT_KS_FLAG	KT_KS_FLAG	INTEGER		
KT_MANAGER	KT_MANAGER	INTEGER		
last_mod_dt	last_mod_dt	LOCAL_TIME		
PARENT_ID	PARENT_ID	SREL		
RESOURCE	RESOURCE	STRING		
SD_ADMIN	SD_ADMIN	INTEGER		

alg Object

The object details are as follows:

1. Associated Table: Act_Log
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: description
5. Function Group: call_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
action_desc	action_desc	STRING		
analyst	analyst	UUID	ca_contact uuid	
call_req_id	call_req_id	STRING	call_req persid	
description	description	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
internal	internal	INTEGER		
session	knowledge_ session	STRING		
k_tool	knowledge_ tool	STRING		
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
system_time	system_time	LOCAL_TIME		
time_spent	time_spent	DURATION		
time_stamp	time_stamp	LOCAL_TIME		
type	type	STRING	act_type code	

am_asset_map Object

The object details are as follows:

1. Associated Table: Am_Asset_Map
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: dmuuid
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
dmuuid	am_dmuuid	STRING		
domain_id	am_domain_id	INTEGER		
server	am_server	STRING		
type	am_type	INTEGER		
unit_domain_id	am_unit_domain_id	INTEGER		
unit_id	am_unit_id	INTEGER		
id	id	INTEGER		UNIQUE REQUIRED KEY
int1_rsrved	int1_rsrved	INTEGER		
int2_rsrved	int2_rsrved	INTEGER		
ob_persid	ob_persid	STRING		
ob_type	ob_type	STRING		
persistent_id	persid	STRING		
str1_rsrved	str1_rsrved	STRING		
str2_rsrved	str2_rsrved	STRING		
schema_ver	version	INTEGER		REQUIRED

arcpur_rule Object

The object details are as follows:

1. Associated Table: Archive_Purge_Rule
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: name
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
add_query	add_query	STRING		
arc_file_name	arc_file_name	STRING		
conf_obj_name	conf_obj_name	STRING		
days_inactive	days_inactive	INTEGER		REQUIRED
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		

Attribute	DB Field	Data Type	SREL References	Flags
name	name	STRING		REQUIRED UNIQUE REQUIRED S_KEY
oper_type	oper_type	INTEGER		REQUIRED
persistent_id	persid	STRING		
reoccur_interv	reoccur_interv	DURATION		
sched	sched	STRING	bpwshft persid	

atev Object

The object details are as follows:

1. Associated Table: Attached_Events
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: user_smag
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
cancel_time	cancel_time	LOCAL_TIME		
event_tmpl	event_tmpl	STRING	evt persid	REQUIRED S_KEY
fire_time	fire_time	LOCAL_TIME		
first_fire_time	first_fire_time	LOCAL_TIME		
group_name	group_name	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		
num_fire	num_fire	INTEGER		
obj_id	obj_id	STRING		REQUIRED
owning_ast	owning_ast	INTEGER	attached_sla id	
persistent_id	persid	STRING		
start_time	start_time	LOCAL_TIME		
status_flag	status_flag	INTEGER		
user_smag	user_smag	STRING		
wait_time	wait_time	DURATION		

atomic_cond Object

The object details are as follows:

1. Associated Table: Atomic_Condition
2. Factories: default
3. REL_ATTR: id
4. Common Name: description
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
cond_code	cond_code	STRING		
connecter	connecter	INTEGER		REQUIRED
delete_flag	del	INTEGER	actbool enum	REQUIRED
description	description	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
l_paran	l_paran	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
lval	lval	STRING	atyp_asc code	REQUIRED
operator	operator	INTEGER		REQUIRED
owning_macro	owning_macro	STRING	splmac persid	
persistent_id	persid	STRING		
r_paran	r_paran	INTEGER		REQUIRED
rval	rval	STRING		
rval_assoc	rval_assoc	STRING	atyp_asc code	
sequence	sequence	INTEGER		REQUIRED

act_type_assoc Object

The object details are as follows:

1. Associated Table: Act_Type_Assoc
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
act_type	act_type	STRING	act_type code	
code	code	STRING		UNIQUE REQUIRED S_KEY
description	description	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
internal	int1_rsrved	INTEGER		
int2_rsrved	int2_rsrved	INTEGER		
int3_rsrved	int3_rsrved	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
log_me_f	log_me_f	INTEGER		
ob_type	ob_type	STRING		
ob_type_attr	ob_type_attr	STRING		
persistent_id	persid	STRING		
str1_rsrved	str1_rsrved	STRING		
str2_rsrved	str2_rsrved	STRING		
str3_rsrved	str3_rsrved	STRING		
sym	sym	STRING		REQUIRED

ca_cmpny Object

The object details are as follows:

1. Associated Table: ca_company
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
alias	alias	STRING		
authentication_password	authentication_password	STRING		
authentication_user_name	authentication_user_name	STRING		
bbs	bbs	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
Company Name	company_name	STRING		
company_type	company_type	INTEGER	ca_company_type id	
id	company_uuid	UUID		UNIQUE REQUIRED KEY
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		
description	description	STRING		
exclude_registration	exclude_registration	integer		
delete_flag	inactive	integer	actbool enum	
last_update_date	last_update_date	LOCAL_TIME		
last_update_user	last_update_user	STRING		
location_uuid	location_uuid	UUID	ca_location location_uuid	
month_fiscal_year_ends	month_fiscal_year_ends	integer		
parent_company_uuid	parent_company_uuid	UUID	ca_company company_uuid	
primary_contact_uuid	primary_contact_uuid	UUID	ca_contact uuid	
version_number	version_number	integer		
web_address	web_address	STRING		

ca_tou Object

The object details are as follows:

1. Associated Table: ca_tou
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
name	name	STRING		REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
terms_of_usage_text		STRING		
version_number	version_number	INTEGER		DEFAULT 0
creation_user	creation_user		cnt	DEFAULT USER
creation_date	creation_date	DATE		
last_mod_dt	last_mod_dt	DATE		
last_update_date	last_update_date	DATE	cnt	
delete_flag	del	INTEGER	actbool enum	REQUIRED

caextwf_inst Object

The object details are as follows:

1. Associated Table: usp_caextwf_instances
2. Factories: default
3. REL_ATTR: id
4. Common Name: procname
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag		actbool.enum		REQUIRED
instance_id	instance_id	STRING(255)		
object_persid	object_persid	STRING(60)		
procname	procname	STRING(32768)		
starttime	starttime	DATE		
endtime	endtime	DATE		

caextwf_sfrm Object

The object details are as follows:

1. Associated Table: usp_caextwf_start_forms
2. Factories: default
3. REL_ATTR: id
4. Common Name: procname

5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
object_persid	object_persid	STRING(60)		
caextwf_form	caextwf_form	STRING(255)		
caextwf_path	caextwf_path	STRING(32768)		
procname		STRING(0)		

closure_code Object

The object contains the following:

1. Associated Table: usp_closure_code
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	Data Type	SREL References	Flags
id	Integer		Unique
producer_id	String 20		
persistent_id	String 60		
delete_flag	SREL	actbool.enum	Standard active indicator Required
sym	String 40		Required
code	String 40		Required
last_mod_by	SREL	cnt.id (http://cnt.id)	
last_mod_date	DATE		
description	String 40		
tenant	SREL		

cmth Object

The object details are as follows:

1. Associated Table: Contact_Method

2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: notification_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
cm_template	cm_template	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		DATE ON_CI {NOW}
description	nx_desc	STRING (40)		
producer_id		LOCAL STRING (20)		
persistent_id	persid	STRING (30)		
supports_smtp	supports_smtp	SREL	bool.enum	
sym	sym	STRING		UNIQUE REQUIRED S_KEY
write_file	write_file	INTEGER		

cnote Object

The object details are as follows:

1. Associated Table: Note_Board
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: text
5. Function Group: announcement
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
active	active_flag	INTEGER	bool_tab enum	REQUIRED
close_date	close_date	LOCAL_TIME		
cnote_type	cnote_type	INTEGER		
control_group	control_group	UUID		
del	del	INTEGER		

id	id	INTEGER		UNIQUE REQUIRED KEY
internal	internal	INTEGER		
location	loc_id	UUID	ca_location location_uuid	
organization	organization	UUID	ca_organization uuid	
persistent_id	persid	STRING		
posted_by	posted_by	UUID	ca_contact uuid	
posted_date	posted_date	LOCAL_TIME		
text	text	STRING		

cnt Object

The object details are as follows:

1. Associated Table: ca_contact, usp_contact
2. Factories: default, agt, cst, grp
3. REL_ATTR: id
4. Common Name: combo_name
5. Function Group: contact
6. ca_contact Table
7. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
access_type	access_type	SREL	acctyp.id (http://acctyp.id)	
admin_org	admin_organization_ uuid	UUID	ca_organization uuid	
alias	alias	STRING		
alt_phone	alt_phone_ number	STRING		
cnthandling_list		BREL	contact_handling	
contact_num	alternate_ identifier	STRING		
notes	comment	STRING		
company	company_uuid	UUID	ca_company company_uuid	
type	contact_type	integer	ca_contact_type id	
id	contact_uuid	UUID		UNIQUE REQUIRED KEY

Attribute	DB Field	Data Type	SREL References	Flags
billing_code	cost_center	INTEGER	ca_resource_cost_center id	
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		
dept	department	INTEGER	ca_resource_department id	
email_address	email_address	STRING		
exclude_ registration	exclude_ registration	integer		
fax_phone	fax_number	STRING		
first_name	first_name	STRING		
floor_location	floor_location	STRING		
delete_flag	inactive	integer	actbool enum	
job_function	job_function	integer		
position	job_title	integer	ca_job_title id	
last_name	last_name	STRING		
last_mod	last_update_date	LOCAL_TIME		
last_mod_by	last_update_user	STRING		
location	location_uuid	UUID	ca_location location_uuid	
mail_stop	mail_stop	STRING		
middle_name	middle_name	STRING		
mobile_phone	mobile_phone_ number	STRING		
organization	organization_ uuid	UUID	ca_organization uuid	
pemail_address	pager_email_ address	STRING		
beeper_phone	pager_number	STRING		
phone_number	pri_phone_ number	STRING		
roles	roles	LIST		
room_location	room_location	STRING		
supervisor_ contact_uuid	supervisor_ contact_uuid	UUID	ca_contact uuid	
userid	userid	STRING		
version_number	version_number	integer		

cnt_role Object

The object details are as follows:

1. Associated Table: usp_cnt_role
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attributes	Data Type	Related Object	Flags
id	INTEGER		UNIQUE
contact	SREL	cnt	
role_obj	SREL	role	
is_default	INTEGER		
last_mod_dt	DATE		

cost_cntr Object

The object details are as follows:

1. Associated Table: ca_resource_cost_center
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		
exclude_registration	exclude_registration	integer		
id	id	INTEGER		UNIQUE REQUIRED KEY

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	inactive	integer	actbool enum	
last_mod	last_update_date	LOCAL_TIME		
last_update_user	last_update_user	STRING		
name	name	STRING		
version_number	version_number	integer		

country Object

The object details are as follows:

1. Associated Table: ca_country
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
description	description	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
delete_flag	inactive	integer	actbool enum	
last_mod	last_update_date	LOCAL_TIME		
last_update_user	last_update_user	STRING		
name	name	STRING		
version_number	version_number	integer		

lr Object

The object details are as follows:

1. Associated Table: Notify_Log_Header
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: msg_hdr

5. Function Group: notify
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
cmth_used	cmth_used	INTEGER	ct_mth id	
cntxt_obj	cntxt_obj	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod	last_mod	LOCAL_TIME		
nlh_ack_by	nlh_ack_by	LOCAL_TIME		
ack_time	nlh_ack_time	DURATION		
contact	nlh_c_addressee	UUID	ca_contact uuid	
nlh_c_alias	nlh_c_alias	UUID		
notify_method	nlh_cm_method	INTEGER	noturg enum	
email_address	nlh_email	STRING		
end_date	nlh_end	LOCAL_TIME		
msg_hdr	nlh_hdr	STRING		
msg_text	nlh_msg	STRING		
msg_html	nlh_msg_html	STRING		
pri_event	nlh_pri	INTEGER		
start_date	nlh_start	LOCAL_TIME		REQUIRED
status	nlh_status	INTEGER		
activity_notify	nlh_transition	INTEGER		
notify_type	nlh_type	INTEGER		
msg_ack	nlh_user_ack	STRING		

symptom_code Object

The object details are as follows:

1. Associated Table: usp_symptom_code
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Field	Data type	Reference	Flags
delete_flag	SREL	actbool.enum	ON_NEW
description	STRING (4000)		
id	INTEGER UNIQUE		
producer_id	LOCAL STRING (20)		
persistent_id	LOCAL STRING (60)		
last_mod_by	SREL	cnt	ON_NEW {USER} ON_CI {USER}
last_mod_dt	DATE		ON_CI {NOW}
sym	STRING 60		

state Object

The object details are as follows:

1. Associated Table: ca_state_province
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		
exclude_registration	exclude_registration	integer		
id	id	INTEGER		UNIQUE REQUIRED KEY
delete_flag	inactive	integer	actbool enum	
last_mod_dt	last_update_date	LOCAL_TIME		
last_mod_by	last_update_user	STRING		
sym	symbol	STRING		
version_number	version_number	integer		

crt Object

The object details are as follows:

1. Associated Table: Call_Req_Type
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: call_mgr_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
code	code	nvarchar(10)		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
display_name	display_name	nvarchar 30		
id	id	INTEGER		UNIQUE REQUIRED KEY
description	nx_desc	nvarchar 30		
persistent_id	persid	nvarchar 30		
sym	sym	nvarchar 30		REQUIRED

ctab Object

The object details are as follows:

1. Associated Table: Controlled_Table
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
desc	nx_desc	nvarchar(40)		
obj_name	obj_name	nvarchar 30		

Attribute	DB Field	Data Type	SREL References	Flags
persistent_id	persid	nvarchar 30		
sym	sym	nvarchar 30		UNIQUE REQUIRED S_KEY

ctimer Object

The object details are as follows:

1. Associated Table: Cr_Call_Timers
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: color
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
beep	beep	INTEGER		
color	color	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
text	text	STRING		
threshold	threshold	DURATION		REQUIRED

ctp Object

The object details are as follows:

1. Associated Table: ca_contact_type
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		
description	description	STRING		
exclude_registration	exclude_registration	integer		
id	id	INTEGER		UNIQUE REQUIRED KEY
delete_flag	inactive	integer	actbool enum	
last_mod_dt	last_update_date	LOCAL_TIME		
last_mod_by	last_update_user	STRING		
sym	name	STRING		
user_uuid	user_uuid	UUID	ca_contact uuid	
version_number	version_number	integer		
view_internal	view_internal	integer		

dblocks Object

The object details are as follows:

1. Associated Table: Virtual internal table
2. Factories: default
3. REL_ATTR: id
4. Common Name: Id
5. Function Group: dblock
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
name		STRING 0		
table_name		STRING 0		
factory_name		SREL	prod_list.sym	
lock_hash		INTEGER		
lock_uuid		UUID		
lock_string		STRING 0		
lock_owner		STRING 0		
when_taken		DATE		
process		STRING 0		

Attribute	DB Field	Data Type	SREL References	Flags
request		INTEGER		
delete_flag		SREL	actbool.enum	

dcon Object

The object details are as follows:

1. Associated Table: Domain_Constraint
2. Factories: default
3. REL_ATTR: id
4. Common Name: constraint_majic
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
persistent_id	persid	STRING		REQUIRED
delete_flag	del	INTEGER	actbool enum	REQUIRED
alias	alias	INTEGER		
last_mod_dt	last_mod_dt	LOCAL_TIME		
last_mod_by	last_mod_by	STRING	ca_contact uuid	REQUIRED
dom_id	dom_id	INTEGER	Domain id	REQUIRED
tbl_id	tbl_id	INTEGER	Controlled_Table id	REQUIRED
type	type	INTEGER	Domain_Constraint_Type	REQUIRED
error_msg	error_msg	STRING	enum	
constraint_majic	constraint_majic	STRING		
constraint_SQL	constraint_sql	STRING		

dcon_typ Object

The object details are as follows:

1. Associated Table: Domain_Constraint_Type
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym

5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
enum	enum	INTEGER		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
description	nx_desc	nvarchar(40)		
persistent_id	persid	nvarchar 30		
sym	sym	nvarchar(12)		UNIQUE REQUIRED S_KEY

dept Object

The object details are as follows:

1. Associated Table: ca_resource_department
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		
exclude_registration	exclude_registration	integer		
id	id	INTEGER		UNIQUE REQUIRED KEY
delete_flag	inactive	integer	actbool enum	
last_mod	last_update_date	LOCAL_TIME		
last_update_user	last_update_user	STRING		
name	name	STRING		
version_number	version_number	integer		

dlgsrvr Object

The object details are as follows:

1. Associated Table: Delegation_Server
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
anon_userid	anon_userid	STRING		
appl_addr	appl_addr	STRING		
default_assignee	default_assignee	UUID	ca_contact uuid	
default_userid	default_userid	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
metafile	metafile	STRING		
description	nx_desc	STRING		
password	password	STRING		
server	server	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY
transport	transport	INTEGER		

dmn Object

The object details are as follows:

1. Associated Table: Domain
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	

Attribute	DB Field	Data Type	SREL References	Flags
last_mod	last_mod_dt	LOCAL_TIME		
desc	nx_desc	STRING		
persistent_id	persid	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY

doc_rep Object

The object details are as follows:

1. Associated Table: Document_Repository
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
archive_path	archive_path	STRING		
archive_type	archive_type	INTEGER		
cgi_path	cgi_path	STRING		
default_rep	default_rep	INTEGER		
delete_flag	del	INTEGER	actbool enum	REQUIRED
file_limit_size	file_limit_size	INTEGER		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
prohibited_file_ext	prohibited_ext	STRING		
protocol	protocol	STRING		
repository_type	repository_type	INTEGER		
retrieve_path	retrieve_path	STRING		
server	server	STRING		
servlet_path	servlet_path	STRING		
sym	sym	STRING		REQUIRED S_KEY
upload_path	upload_path	STRING		

ext_entity_map Object

The object details are as follows:

1. Associated Table: External_Entity_Map
2. Factories: default, sd_chg_map
3. REL_ATTR: persistent_id
4. Common Name: xschema_code
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
int1_rsrved	int1_rsrved	INTEGER		
int2_rsrved	int2_rsrved	INTEGER		
int3_rsrved	int3_rsrved	INTEGER		
int4_rsrved	int4_rsrved	INTEGER		
int5_rsrved	int5_rsrved	INTEGER		
int6_rsrved	int6_rsrved	INTEGER		
lstr1_rsrved	lstr1_rsrved	STRING		
lstr2_rsrved	lstr2_rsrved	STRING		
ob_persid	ob_persid	STRING		
ob_type	ob_type	STRING		
persistent_id	persid	STRING		
str1_rsrved	str1_rsrved	STRING		
str2_rsrved	str2_rsrved	STRING		
xentity_id	xentity_id	STRING		REQUIRED
xschema_code	xschema_code	STRING		REQUIRED
xschema_ver	xschema_ver	INTEGER		REQUIRED

fmgrp Object

The object details are as follows:

1. Associated Table: Form_Group
2. Factories: default, all_fmgrp
3. REL_ATTR: id

4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
sym	sym	STRING		REQUIRED S_KEY

gl_code Object

The object details are as follows:

1. Associated Table: ca_resource_gl_code
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		
exclude_ registration	exclude_ registration	integer		
id	id	INTEGER		UNIQUE REQUIRED KEY
delete_flag	inactive	integer	actbool enum	
last_mod	last_update_date	LOCAL_TIME		
last_update_user	last_update_user	STRING		
name	name	STRING		
version_number	version_number	integer		

grc Object

The object details are as follows:

1. Associated Table: ca_resource_class
2. Factories: default
3. REL_ATTR: id
4. Common Name: type
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		
exclude_ registration	exclude_ registration	integer		
family	family_id	INTEGER	ca_resource_ family id	
id	id	INTEGER		UNIQUE REQUIRED KEY
delete_flag	inactive	integer	actbool enum	
last_mod	last_update_date	LOCAL_TIME		
last_update_user	last_update_user	STRING		
type	name	STRING		
parent_id	parent_id	SREL		
nsm_class	usp_nsm_class	INTEGER	buscls id	
version_number	version_number	integer		

grpmem Object

The object details are as follows:

1. Associated Table: Group_Member
2. Factories: default

3. REL_ATTR: persistent_id
4. Common Name:
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
group	group_id	UUID		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
manager_flag	manager_flag	INTEGER		
member	member	UUID	ca_contact uuid	REQUIRED
notify_flag	notify_flag	INTEGER		

hier Object

The object details are as follows:

1. Associated Table: Asset_Assignment
2. Factories: default
3. REL_ATTR: id
4. Common Name: license_num
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
child	hier_child	byte(16)	ca_owned_ resource uuid	REQUIRED S_KEY
license_num	hier_license_num	nvarchar(40)		
log_date	hier_log_date	INTEGER		REQUIRED
parent	hier_parent	byte(16)	ca_owned_ resource uuid	REQUIRED S_KEY
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	byte(16)	ca_contact uuid	
last_mod_dt	last_mod_dt	INTEGER		
persistent_id	persid	nvarchar(30)		

ical_alarm Object

The object details are as follows:

1. Associated Table: usp_ical_alarm

2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	Data Type	Remarks
sym	STRING	Required
alarm_value	STRING	

ical_event_template Object

The object details are as follows:

1. Associated Table: usp_ical_event_template
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	Data Type	Remarks
code	STRING	Required
sym	INTEGER	Required
alarm	SREL ical_alarm	
start_date	STRING	
end_date	STRING	
obj_type	SREL actlog_prod_list	
categories	STRING	
summary	STRING	
description	STRING	
url	STRING	
extra_entries	STRING	

imp Object

The object details are as follows:

1. Associated Table: Impact
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
enum	enum	INTEGER		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
description	nx_desc	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY
value	value	INTEGER		

in Object

The object details are as follows:

1. Associated Table: Call_Req
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: ref_num

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
active	active_flag	INTEGER	bool_tab enum	REQUIRED
active_prev	LOCAL	SREL	bool.enum	
affected_ resource	affected_rc	UUID	ca_owned_ resource uuid	
assignee	assignee	UUID		
assignee_prev	LOCAL	SREL	agt.id (http://agt.id)	
call_back_date	call_back_date	LOCAL_TIME		
call_back_flag	call_back_flag	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
category	category	STRING	prob_ctg persid	
category_prev	LOCAL	SREL	pcat.persistent_id	
caused_by_chg	caused_by_chg	SREL	chg.id (http://chg.id)	
change	change	INTEGER	chg id	
charge_back_id	charge_back_id	STRING		
close_date	close_date	LOCAL_TIME		
cr_tticket	cr_tticket	INTEGER		
created_via	created_via	INTEGER	interface id	
customer	customer	UUID	ca_contact uuid	REQUIRED
event_token	event_token	STRING		
extern_ref	extern_ref	STRING		
group	group_id	UUID		
group_prev	LOCAL	SREL	grp.id (http://grp.id)	
id	id	INTEGER		UNIQUE REQUIRED KEY
impact	impact	INTEGER	impact enum	
impact_prev	LOCAL	SREL	imp.enum	
incident_priority	incident_priority	INTEGER		
last_act_id	last_act_id	STRING		
last_mod_dt	last_mod_dt	LOCAL_TIME		
log_agent	log_agent	UUID	ca_contact uuid	REQUIRED
macro_ predicted_ violation	macro_predict_ viol	INTEGER		
open_date	open_date	LOCAL_TIME		
outage_end_ time	outage_end_ time	LOCAL_TIME		
outage_start_ time	outage_start_ time	LOCAL_TIME		
parent	parent	STRING	call_req persid	
persistent_id	persid	STRING		
predicted_sla_ violation	predicted_sla_ viol	INTEGER		
priority	priority	INTEGER	pri enum	REQUIRED
priority_prev	LOCAL	SREL	pri.enum	
problem	problem	STRING		
ref_num	ref_num	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
				UNIQUE REQUIRED S_KEY
resolve_date	resolve_date	LOCAL_ TIME		
rootcause	rootcause	INTEGER	rootcause id	
extern_token	sched_token	STRING		
severity	severity	INTEGER	sevrty enum	
severity_prev	LOCAL	SREL	sev.enum	
sla_violation	sla_violation	INTEGER		
base_template	solution	STRING	call_req persid	
status	status	STRING	cr_stat code	
status_prev	LOCAL	SREL	crs.code	
string1	string1	STRING		
string2	string2	STRING		
string3	string3	STRING		
string4	string4	STRING		
string5	string5	STRING		
string6	string6	STRING		
summary	summary	STRING		
support_lev	support_lev	STRING	srv_desc code	
template_name	template_name	STRING	cr_template template_name	
time_spent_ sum	time_spent_ sum	DURATION		
type	type	STRING	crt code	
urgency	urgency	INTEGER	urgncy enum	
urgency_prev	LOCAL	SREL	urg.enum	

in_trans Object

The object details are as follows:

1. Associated Tables: in_trans
2. Factories: default
3. REL_ATTR: id
4. Common Name: condition_error
5. Function Group: call_mgr_reference

6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
status	status	STRING	crs	Specifies the current ticket status.
new_status	new status	STRING	crs	Specifies the new ticket status.
is default		INTEGER		Default transition that appears when the Status field is empty. On new default: 0
must_comment		INTEGER		Comment required when using a transition. On new default: 0
delete_flag	del		actbool	Required. On new default: 0
condition			macro	Site condition macro to approve transition.
condition_error		STRING		Error message for site condition.
description		STRING		Description of this transition.
last_mod_by			cnt	On new default user; on CI set user
last_mod_dt		DATE		On CI set user now

INDEX_DOC_LINKS Object

The object details are as follows:

1. Associated Table: INDEX_DOC_LINKS
2. Factories: default
3. REL_ATTR: id
4. Common Name: RELATIONAL_ID
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SRE References	Flags
Document ID	DOC_ID	INTEGER	SKELETONS id	
id	ID	INTEGER		REQUIRED KEY
Category ID	INDEX_ID	INTEGER	O_INDEXES id	
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Relational ID	RELATIONAL_ID	STRING		

intfc Object

The object details are as follows:

1. Associated Table: Interface
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
code	code	STRING		UNIQUE REQUIRED
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
desc	nx_desc	STRING		
persistent_id	persid	STRING		
sym	sym	STRING		UNIQUE REQUIRED

job_func Object

The object details are as follows:

1. Associated Table: ca_job_function
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
exclude_ registration	exclude_ registration	integer		
id	id	INTEGER		UNIQUE REQUIRED KEY
delete_flag	inactive	integer	actbool enum	
last_mod	last_update_date	LOCAL_TIME		
last_update_user	last_update_user	STRING		
name	name	STRING		
version_number	version_number	integer		

kc Object

The object details are as follows:

1. Associated Table: usp_kpi
2. Factories: default
3. REL_ATTR: id
4. Common Name: kpi_name
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
kpi_name	name	STRING		REQUIRED
sys_name	sys_name	STRING		
kpi_type	type	INTEGER		REQUIRED
delete_flag	status		actbool	REQUIRED
process_type	process_type	INTEGER		
stored_query_id	stored_query_id	STRING	crsq	
user_context	user_context	UUID	cnt	
sql_query	sql_query	STRING		
description	description	STRING		
refresh_time	refresh_time	INTEGER		REQUIRED
metric_type	metric_type	INTEGER		REQUIRED
curr_kpi_time_ stamp	curr_kpi_time_ stamp	INTEGER		
version_number	version_number	INTEGER		
tenant	tenant	STRING		
last_mod_by	last_mod_by	UUID	cnt	

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_dt	last_mod_dt	DATE		

KCAT Object

The object details are as follows:

1. Associated Table: O_INDEXES
2. Factories: default
3. REL_ATTR: id
4. Common Name: CAPTION
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
DESCRIPTION	DESCRIPTION	STRING		
AUTHOR_ID	AUTHOR_ID	UUID	ca_contact uuid	
CAPTION	CAPTION	STRING		REQUIRED
DOC_TEMPLATE	DOC_TEMPLATE	INTEGER	CI_DOC_ TEMPLATES id	
HAS_CHILDREN	HAS_CHILDREN	INTEGER		
HAS_DOCS	HAS_DOCS	INTEGER		
id	ID	INTEGER		KEY
KEYWORDS	KEYWORDS	STRING		
ON_COPY_PASTE	ON_COPY_PASTE	INTEGER		
ON_CUT_PASTE	ON_CUT_PASTE	INTEGER		
last_mod_dt	LAST_MOD_DT	LOCAL_ TIME		Indicates the timestamp of when this record was last modified.
last_mod_by	LAST_MOD_BY	SREL	cnt	Specifies the UUID of the contact who modified this record.
OWNER_ID	OWNER_ID	UUID	ca_contact uuid	
PARENT_ID	PARENT_ID	SREL	O_INDEXES id	
ALLOW_QA	ALLOW_QA			

Attribute	DB Field	Data Type	SREL References	Flags
		INTEGER		
PERMISSION_INDEX_ID	PERMISSION_INDEX_ID	INTEGER	O_INDEXES id	
READ_PGROUP	READ_PGROUP	INTEGER	P_GROUPS id	
persistent_id	persid	STRING		
PGROUP TYPE	PGROUP_TYPE	INTEGER		Indicates if the P Groups is based on Roles or Groups: **1** -- Groups (Default) **2** -- Roles
producer_id	producer_id	STRING		
RELATIONAL_ID	RELATIONAL_ID	STRING		
SUBJECT_EXPERT_ID	SUBJECT_EXPERT_ID	UUID	ca_contact uuid	
WF_TEMPLATE	WF_TEMPLATE	SREL	CI_WF_TEMPLATES id	
WRITE_PGROUP	WRITE_PGROUP	INTEGER	P_GROUPS id	

kcd Object

The object details are as follows:

1. Associated Table: usp_kpi_data
2. Factories: default
3. REL_ATTR: id
4. Function Group: admin
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
kpi_id	kpi_id	INTEGER	kc	
kpi_time_ stamp	kpi_time_ stamp	DATE		
metric_type	type	INTEGER		REQUIRED
kpi_value	kpi_value	INTEGER		REQUIRED
duration_count	duration_count	INTEGER		
duration_sum	duration_sum	INTEGER		
duration_max	duration_max	INTEGER		
duration_ average	duration_ average	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
execute_time	execute_time	INTEGER		
version_number	version_number	INTEGER		

kdlinks Object

The object details are as follows:

1. Associated Table: kdlinks
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: sd_obj_type
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Request Linked	cr	STRING	call_req persid	
id	ID	INTEGER		KEY
Issue Linked	iss	STRING	issue persistent_id	
Document	kd	INTEGER	SKELETONS id	
Analyst	last_mod_by	UUID	ca_contact uuid	
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Link Type	link_type	INTEGER		
Ticket ID	sd_obj_id	INTEGER		
Ticket Type	sd_obj_type	STRING		

KT_REPORT_CARD Object

The object details are as follows:

1. Associated Table: KT_REPORT_CARD
2. Factories: default
3. REL_ATTR: id
4. Common Name: SUBJECT_ID
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		KEY
SUBJECT_ID	SUBJECT_ID	nvarchar (40)		
PAST_DAYS	PAST_DAYS	INTEGER		
ORG_STATISTICS	ORG_STATISTICS	INTEGER		
DOCUMENTS_ SUBMITTED	DOCUMENTS_ SUBMITTED	INTEGER		
DOCUMENTS_ PUBLISHED	DOCUMENTS_ PUBLISHED	INTEGER		
TOTAL_HITS	TOTAL_HITS	INTEGER		
AVERAGE_ EFFECTIVENESS_ RATING	AVERAGE_ EFFECTIVENESS_ RATING	INTEGER		
TOTAL_ SOLUTION_ COUNT	TOTAL_ SOLUTION_ COUNT	INTEGER		
creation_user	creation_user	nvarchar (64)		
creation_date	creation_date	INTEGER		
last_update_user	last_update_user	nvarchar (64)		
last_update_date	last_update_date	INTEGER		
TOTAL_VOTES	TOTAL_VOTES	INTEGER		
AVG_RATING	AVG_RATING	DOUBLE		
USER_SLV_CNT	USER_SLV_CNT	INTEGER		
LINKED_ KNOWLEDGE_BY_OTHERS	LINKED_ KNOWLEDGE_BY_OTHERS	INTEGER		
LINKED_ KNOWLEGE_BY_ ME	LINKED_ KNOWLEGE_BY_ ME	INTEGER		
CLOSED_TICKETS	CLOSED_TICKETS	INTEGER		
TICKETS_WITH_ KNOWLEDGE	TICKETS_WITH_ KNOWLEDGE	INTEGER		
TICKETS_HAD_ SEARCH_ ACTIVITIES	TICKETS_HAD_ SEARCH_ ACTIVITIES	INTEGER		
KNOWLEDGE_ SUBMIT_FROM_ TICKET	KNOWLEDGE_ SUBMIT_FROM_ TICKET	INTEGER		
TIME_TO_PUBLISH	TIME_TO_PUBLISH	INTEGER		
MY_COMMENTS	MY_COMMENTS	INTEGER		
DOCUMENTS_ RETIRED	DOCUMENTS_ RETIRED	INTEGER		
TIME_TO_FIX	TIME_TO_FIX	INTEGER		
FLAGS_FIXED	FLAGS_FIXED	INTEGER		
		INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
COMMENTS_ON_MY_DOCUMENTS	COMMENTS_ON_MY_DOCUMENTS			
FIRST_CALL_RES_WITH_KNOW	FIRST_CALL_RES_WITH_KNOW	INTEGER		
FIRST_CALL_RES_WITHOUT_KNOW	FIRST_CALL_RES_WITHOUT_KNOW	INTEGER		
CONTRIBUTOR_ UUID	CONTRIBUTOR_ UUID	SREL	cnt	TENANCY_UNRESTRICTED
IS_SUPERVISOR	IS_SUPERVISOR	INTEGER		
SUPERVISOR_ID	SUPERVISOR_ID	SREL	cnt	TENANCY_UNRESTRICTED
MY_ORG_REF_ID	MY_ORG_REF_ID	SREL	KT_REPORT_CARD	
PAST_DAYS_TEXT	PAST_DAYS_TEXT	nvarchar (20)		Populates from the resource file.
LAST_MOD_DT_ TEXT	LAST_MOD_DT_ TEXT	nvarchar (20)		Specifies the KRC calculation date.
DOCUMENTS_PUBLISHED_ PERCENT	DOCUMENTS_PUBLISHED_ PERCENT	nvarchar (4)		
AVG_HITS	AVG_HITS	nvarchar (20)		
AVG_RATING_ TEXT	AVG_RATING_ TEXT	nvarchar (100)		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt	

ktd Object

The object details are as follows:

1. Associated Table: usp_kpi_ticket_data
2. Factories: default
3. REL_ATTR: id
4. Function Group: admin
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
end_time	end_time	INTEGER		REQUIRED
prev_time	prev_time	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
obj_name	obj_name	STRING		REQUIRED
obj_id	obj_id	INTEGER		REQUIRED
obj_type	obj_type	STRING		
field_name	field_name	STRING		
field_value	field_value	STRING		
next_value	next_value	STRING		
operation	operation	STRING		
attr_obj	attr_obj	STRING		
attr_from_id	attr_from_id	INTEGER		
attr_to_id	attr_to_id	INTEGER		
attr_from_uuid	attr_from_uuid	UUID		
attr_to_uuid	attr_to_uuid	UUID		
ktd_duration	duration	INTEGER		REQUIRED
user_context	user_context	UUID	cnt	

kwrd Object

The object details are as follows:

1. Associated Table: Knowledge_Keywords
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
sym	sym	STRING		REQUIRED S_KEY

loc Object

The object details are as follows:

1. Associated Table: ca_location

2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
address1	address_1	STRING		
address2	address_2	STRING		
address3	address_3	STRING		
address4	address_4	STRING		
address5	address_5	STRING		
address6	address_6	STRING		
city	city	STRING		
description	comment	STRING		
contact_address_ flag	contact_address_ flag	integer		
country	country	integer	ca_country id	
county	county	STRING		
creation_date	creation_date	LOCAL_TIM E		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIM E		
exclude_ registration	exclude_ registration	integer		
fax_number	fax_number	STRING		
geo_coord_type	geo_coord_type	integer		
geo_coords	geo_coords	STRING		
delete_flag	inactive	integer	actbool enum	
last_mod	last_update_date	LOCAL_TIM E		
last_update_user	last_update_user	STRING		
name	location_name	STRING		
id	location_uuid	UUID		UNIQUE REQUIRED KEY
mail_address_1	mail_address_1	STRING		
mail_address_2	mail_address_2	STRING		
mail_address_3	mail_address_3	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
mail_address_4	mail_address_4	STRING		
mail_address_5	mail_address_5	STRING		
mail_address_6	mail_address_6	STRING		
pri_phone_number	pri_phone_number	STRING		
primary_contact_uuid	primary_contact_uuid	UUID		
site	site_id	integer	ca_site id	
state	state	integer	ca_state_ province id	
version_number	version_number	integer		
zip	zip	STRING		

LONG_TEXTS Object

The object details are as follows:

1. Associated Table: LONG_TEXTS
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: REF_PERSID
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Chunk	ACTUAL_TEXT	STRING		
Cunk Order	CNT_ORDER	INTEGER		
id	ID	INTEGER		KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Document ID	REF_PERSID	STRING		

mfrmod Object

The object details are as follows:

1. Associated Table: ca_model_def
2. Factories: default
3. REL_ATTR: id

4. Common Name: sym
5. Function Group: ci_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
abbreviation	abbreviation	STRING		
resource_class	class_id	INTEGER	ca_resource_ class id	
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
current_as_of_ date	current_as_of_ date	integer		
delete_time	delete_time	LOCAL_TIME		
exclude_ registration	exclude_ registration	integer		
family_id	family_id	INTEGER		
delete_flag	inactive	integer	actbool enum	
last_mod	last_update_ date	LOCAL_TIME		
last_update_ user	last_update_ user	STRING		
manufacturer	manufacturer_ uuid	UUID	ca_company company_uuid	
id	model_uuid	UUID		UNIQUE REQUIRED KEY
sym	name	STRING		
operating_ system	operating_ system	integer		
preferred_seller_uu id	preferred_seller_uu id	UUID		
version_number	version_number	integer		
model_name	description	STRING		

mgsalg Object

The object details are as follows:

1. Associated Table: Mgs_Act_Log
2. Factories: default
3. REL_ATTR: id
4. Common Name: description

5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
action_desc	action_desc	STRING		
analyst	analyst	UUID	ca_contact uuid	
id	id	INTEGER		UNIQUE REQUIRED KEY
internal	internal	INTEGER		
last_mod_dt	last_mod_dt	LOCAL_TIME		
mgs_id	mgs_id	INTEGER	managed_survey id	
persistent_id	persid	STRING		
system_time	system_time	LOCAL_TIME		
time_spent	time_spent	DURATION		
time_stamp	time_stamp	LOCAL_TIME		
type	type	STRING	act_type code	

mgsstat Object

The object details are as follows:

1. Associated Table: Mgs_Status
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
active	active	INTEGER		
code	code	STRING		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
hold	hold	INTEGER		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
modified_date	last_mod_dt	LOCAL_TIME		

Attribute	DB Field	Data Type	SREL References	Flags
persistent_id	persid	STRING		
sym	sym	STRING		REQUIRED

nr Object

The object details are as follows:

1. Associated Table: ca_owned_resource, usp_owned_resource
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
backup_ services_ contact_uuid		SREL	cnt	Specifies the name of the contact responsible for backup services.
billing_contact_ uuid		SREL	cnt	Specifies the name of the contact responsible for billing.
disaster_ recovery_ contact_uuid		SREL	cnt	Specifies the name of the contact responsible for disaster recovery services.
id	id	UUID		
network_contact _uuid		SREL	cnt	Specifies the name of the contact responsible for network operations.
producer_id	producer_id	LOCAL STRING 30		
persistent_id	persid	LOCAL STRING 60		
chgnr	chgnr	LREL	chg asset	
issnr	issnr	LREL	iss asset	
cntref	cntref	LREL	cnt:PDM cenv	
orgref	orgref	LREL	org:PDM oenv	
acquire_date	acquire_date	LOCAL_TI ME		
		UUID		

Attribute	DB Field	Data Type	SREL References	Flags
asset_source_ uuid	asset_source_ uuid			
loc_cabinet	cabinet_locati on	STRING		
company_bought _ for_uuid	company_bou ght_for_uuid	UUID	ca_company company_uuid	
expense_code	cost_center	INTEGER	ca_resource_ cost_center id	
creation_date	creation_date	LOCAL_TI ME		
creation_system	creation_syste m	STRING		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TI ME		
department	department	INTEGER	ca_resource_ department id	
exclude_ registration	exclude_ registration	INTEGER		
expense_code	expense_code	SREL	cost_cntr	
loc_floor	floor_location	STRING		
gl_code	gl_code	integer		
support_contact1 _uuid		SREL	cnt	Specifies the name of the first contact responsible for support services.
support_contact2 _uuid		SREL	cnt	Specifies the name of the second contact responsible for support services.
support_contact3 _uuid		SREL	cnt	Specifies the name of the third contact responsible for support services.
system_name	host_name	STRING		
delete_flag	inactive	integer	actbool enum	
install_date	installation_da te	LOCAL_TI ME		
alarm_id	ip_address	STRING		
last_mod	last_update_d ate	LOCAL_TI ME		
last_mod_by	last_update_u ser	STRING		
license_number	license_ information	STRING		
license_uuid	license_uuid	UUID		

Attribute	DB Field	Data Type	SREL References	Flags
location	location_uuid	UUID	ca_location location_uuid	
mac_address	mac_address	STRING 64		
dns_name	dns_name	STRING 100		
repair_org	maintenance_ org_uuid	UUID	ca_organizatio n uuid	
vendor_repair	maintenance_ vendor_uuid	UUID	ca_company company_uuid	
manufacturer	manufacturer_ uuid	UUID	ca_company company_uuid	
model	model_uuid	UUID	ca_model_def model_uuid	
product_version	product_versi on	STRING 16		
operating_system	operating_syst em	INTEGER		
org_bought_for_ uuid	org_bought_fo r_ uuid	UUID	ca_organizatio n uuid	
id	own_resource _ uuid	UUID		UNIQUE REQUIRED KEY
product_version	product_versi on	STRING		
purchase_order_i d	purchase_orde r_id	STRING		
requisition_id	requisition_id	STRING		
resource_alias	resource_alias	STRING		
class	resource_class	INTEGER	ca_resource_ class id	
resource_contact	resource_cont act_uuid	UUID	ca_contact uuid	
description	resource_ description	STRING		
ufam	ufam	INTEGER		
is_selected	is_selected	LOCAL INTEGER		
family	resource_famil y	INTEGER	ca_resource_ family id	
name	resource_nam e	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
resource_owner_uuid	resource_owner_ uuid	UUID	ca_contact uuid	
asset_count	resource_quantity	INTEGER		
status	resource_status	INTEGER	ca_resource_ status id	
asset_num	resource_tag	STRING		
child_hier	child_hier	BREL	hier.parent	
parent_hier	parent_hier	BREL	hier.child	
asset_log	asset_log	BREL	nr_com.asset_ id	
assoc_cr	assoc_cr	QREL	cr	
all_creq	all_creq	BREL	cr.affected_ resource	
all_open_creq	all_open_creq	QREL	cr	
bm_child_hier	bm_child_hier	QREL	bmhier	
bm_parent_hier	bm_parent_hier	QREL	bmhier	
assoc_reqs	assoc_reqs	QREL	cr	
service_org	responsible_org_ uuid	UUID	ca_organization uuid	
vendor_restore	responsible_ vendor_uuid	UUID	ca_company company_uuid	
loc_room	room_location	STRING		
serial_number	serial_number	STRING		
loc_shelf	shelf_location	STRING		
loc_slot	slot_location	STRING		
status_date	status_date	LOCAL_TIME		
supplier	supply_vendor_ uuid	UUID	ca_company company_uuid	
version_number	version_number	INTEGER		

nr_com Object

The object details are as follows:

1. Associated Table: NR_Comment
2. Factories: default

3. REL_ATTR: id
4. Common Name: writer_name
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
attr_name	attr_name	STRING		
log	com_comment	STRING		
log_date	com_dt	LOCAL_TIME		REQUIRED
asset_id	com_par_id	UUID	ca_owned_resource uuid	REQUIRED S_KEY
writer_name	com_userid	STRING		REQUIRED S_KEY
id	id	INTEGER		UNIQUE REQUIRED KEY
new_value	new_value	STRING		
old_value	old_value	STRING		
writer_id	writer_id	UUID		

nrf Object

The object details are as follows:

1. Associated Table: ca_resource_family
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
producer_id	producer_id	LOCAL STRING 20		
persistent_id	persid	LOCAL STRING 60		
description	description	STRING		
creation_date	creation_date	LOCAL_TIME		

Attribute	DB Field	Data Type	SREL References	Flags
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		
exclude_registration	exclude_registration	INTEGER		
delete_flag	inactive	SREL	actbool enum	REQUIRED
include_reconciliation	include_reconciliation	INTEGER		
last_update_date	last_update_date	LOCAL_TIME		
last_update_user	last_update_user	STRING		
sym	name	STRING 255		
extension_name	table_extension_name	STRING		
version_number	version_number	INTEGER		
physical_table_name	physical_table_name	STRING 30		

O_COMMENTS Object

The object details are as follows:

1. Associated Table: O_COMMENTS
2. Factories: default
3. REL_ATTR: id
4. Common Name: COMMENT_TEXT
5. Function Group: kd
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		KEY
producer_id	producer_id	LOCAL STRING (20)		
persistent_id	persistent_id	LOCAL STRING (60)		
DOC_ID	DOC_ID	SREL	KD	TENANCY_ UNRESTRICTED
SUPPRESS_ OEVENTS	SUPPRESS_ OEVENTS	INTEGER		
VER_COUNT	VER_COUNT	INTEGER		
USER_NAME	USER_NAME	STRING 50		

Attribute	DB Field	Data Type	SREL References	Flags
USER_ID	USER_ID	SREL	cnt	
COMMENT_ TEXT	COMMENT_ TEXT	STRING 255		REQUIRED
COMMENT_ TIMESTAMP	COMMENT_ TIMESTAMP	DATE		
EMAIL_ ADDRESS	EMAIL_ ADDRESS	STRING 75		
TICKET		LOCAL STRING		
FLG_TYPE	FLG_TYPE	SREL	KT_FLG_ TYPE	
ASSIGNEE	ASSIGNEE	SREL	cnt	
DEADLINE_ DATE	DEADLINE_ DATE	DATE		
CLOSE_DATE	CLOSE_DATE	DATE		
FLG_STATUS	FLAG_STATUS	SREL	KT_FLG_ STATUS	
CLOSE_DESC	CLOSE_DESC	STRING 2000		
FLG_CODE	FLG_CODE	STRING 50		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt	
tenant	tenant	UUID	ca_tenant	

O_EVENTS Object

The object details are as follows:

1. Associated Table: O_EVENTS
2. Factories: default
3. REL_ATTR: id
4. Common Name: EVENT_NAME
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Change details	ACTION	STRING		
Document ID	ENTITY_ID	INTEGER	SKELETONS id	
Change Type	EVENT_NAME	STRING		
Date and Time	EVENT_TIMESTAMP	LOCAL_TIME		
id	ID	INTEGER		KEY

Attribute	DB Field	Data Type	SREL References	Flags
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
For future use	VER_COUNT	INTEGER		
Change Type Enum	WF_ACTION_ID	INTEGER		
User ID	WF_USER_ID	UUID	ca_contact uuid	

opsys Object

The object details are as follows:

1. Associated Table: ca_resource_operating_system
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		
exclude_registration	exclude_registration	integer		
id	id	INTEGER		UNIQUE REQUIRED KEY
delete_flag	inactive	integer	actbool enum	
last_mod	last_update_date	LOCAL_TIME		
last_update_user	last_update_user	STRING		
name	name	STRING		
version_number	version_number	integer		

options Object

The object details are as follows:

1. Associated Table: Options
2. Factories: default
3. REL_ATTR: persistent_id

4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
action	action	INTEGER		
action_status	action_status	STRING		
app_name	app_name	STRING		
default_value	default_value	STRING		
deinstall_script	deinstall_script	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
error_msg	error_msg	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
install_script	install_script	STRING		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
option_name	option_name	STRING		
persistent_id	persid	STRING		
readme	readme	STRING		
sequence	sequence	INTEGER		
sym	sym	STRING		REQUIRED
validation	validation	STRING		
value	value	STRING		
value_active	value_active	INTEGER		

o rg Object

The object details are as follows:

1. Associated Table: Internal_Organization
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: organization

ca_organization Table

REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
org_num	abbreviation	STRING		
alt_phone_cc	alt_phone_cc	integer		
alt_phone	alt_phone_number	STRING		
comment	comment	STRING		
company	company_uuid	UUID	ca_company company_uuid	
contact	contact_uuid	UUID	ca_contact uuid	
billing_code	cost_center	integer	ca_resource_cost_center id	
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		
email_addr	email_address	STRING		
exclude_registration	exclude_registration	integer		
fax_cc	fax_cc	integer		
fax_phone	fax_number	STRING		
delete_flag	inactive	integer	actbool enum	
last_mod	last_update_date	LOCAL_TIME		
last_update_user	last_update_user	STRING		
location	location_uuid	UUID	ca_location location_uuid	
name	org_name	STRING		
id	organization_uuid	UUID		UNIQUE REQUIRED KEY
pemail_addr	pager_email_address	STRING		
parent_org_uuid	parent_org_uuid	UUID		
pri_phone_cc	pri_phone_cc	integer		
phone_number	pri_phone_number	STRING		
version_number	version_number	integer		

usp_organization Table

Attribute	DB Field	Data Type	SREL References	Flags
iorg_assigned_svr	iorg_assigned_svr	INTEGER		
service_type	iorg_service_type	STRING	srv_desc code	
last_mod	last_mod	LOCAL_TIME		
id	organization_uuid	UUID		
owning_contract	owning_contract	INTEGER	svc_contract id	

outage_type Object

The object details are as follows:

1. Associated Table: usp_outage_type
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	Data Type	Reference	Flags
delete_flag	SREL actbool.enum	del	ON_NEW
description	STRING (4000)		
id	INTEGER		UNIQUE
producer_id	LOCAL STRING (20)		
persistent_id	LOCAL STRING (60)		
last_mod_by	SREL	cnt.id (http://cnt.id)	ON_NEW {USER} ON_CI {USER}
last_mod_dt	DATE		ON_CI {NOW}
sym	STRING (60)		

P_GROUPS Object

The object details are as follows:

1. Associated Table: P_GROUPS
2. Factories: default
3. REL_ATTR: id

4. Function Group:

5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
GRP_LIST	GRP_LIST	STRING		
GRP_LIST_KEY	GRP_LIST_KEY	STRING		
GROUP_LIST_N	(local attr)	STRING		
TYPE	TYPE	INTEGER		Indicates if the P Groups is based on Roles or Groups: **1** -- Groups (Default) **2** -- Roles
id	ID	INTEGER		KEY
contained_groups	contained_groups	BREL	usp_group_pgroup	
contained_roles	contained_roles	BREL	usp_role_pgroup	
last_mod_dt	last_mod_dt	DATE		Indicates the timestamp of when this record was last modified.
last_mod_by	last_mod_by	UUID	cnt	Specifies the UUID of the contact who last modified this record
producer_id	producer_id	STRING		
persistent_id	persid	STRING		

perscnt Object

The object details are as follows:

1. Associated Table: Person_Contacting

2. Factories: default

3. REL_ATTR: id

4. Common Name: sym

5. Function Group: reference

6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY

position Object

The object details are as follows:

1. Associated Table: ca_job_title
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		
exclude_registration	exclude_registration	integer		
id	id	INTEGER		UNIQUE REQUIRED KEY
delete_flag	inactive	integer	actbool enum	
last_mod_dt	last_update_date	LOCAL_TIME		
last_mod_by	last_update_user	STRING		
sym	name	STRING		
version_number	version_number	integer		

pr Object

The object details are as follows:

1. Associated Table: Call_Req
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: ref_num

5. Function Group: call_mgr

6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
active	active_flag	INTEGER	bool_tab enum	REQUIRED
active_prev	LOCAL	SREL	bool.enum	
affected_ resource	affected_rc	UUID	ca_owned_ resource uuid	
assignee	assignee	UUID	agt.id (http://agt.id)	
assignee_prev	LOCAL	SREL	pcat.persistent_id	
call_back_date	call_back_date	LOCAL_ TIME		
call_back_flag	call_back_flag	INTEGER		
category	category	STRING	prob_ctg persid	
category_prev	LOCAL	SREL		
caused_by_chg	caused_by_chg	SREL	chg.id (http://chg.id)	
change	change	INTEGER	chg id	
charge_back_id	charge_back_ id	STRING		
close_date	close_date	LOCAL_ TIME		
cr_tticket	cr_tticket	INTEGER		
created_via	created_via	INTEGER	interface id	
customer	customer	UUID	ca_contact uuid	REQUIRED
event_token	event_token	STRING		
extern_ref	extern_ref	STRING		
group	group_id	UUID		
group_prev	LOCAL	SREL	grp.id (http://grp.id)	
id	id	INTEGER		UNIQUE REQUIRED KEY
impact	impact	INTEGER	impact enum	
impact_prev	LOCAL	SREL	imp.enum	
incident_priority	incident_priority	INTEGER		
last_act_id	last_act_id	STRING		
last_mod_dt	last_mod_dt	LOCAL_TI ME		
log_agent	log_agent	UUID	ca_contact uuid	REQUIRED
macro_ predicted_ violation	macro_predict_ viol	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
open_date	open_date	LOCAL_ TIME		
outage_end_time	outage_end_ time	LOCAL_TI ME		
outage_start_ time	outage_start_ time	LOCAL_TI ME		
parent	parent	STRING	call_req persid	
persistent_id	persid	STRING		
predicted_sla_ violation	predicted_sla_vi ol	INTEGER		
priority	priority	INTEGER	pri enum	REQUIRED
priority_prev	LOCAL	SREL	pri.enum	
problem	problem	STRING		
ref_num	ref_num	STRING		UNIQUE REQUIRED S_KEY
resolve_date	resolve_date	LOCAL_ TIME		
rootcause	rootcause	INTEGER	rootcause id	
extern_token	sched_token	STRING		
severity	severity	INTEGER	sevrty enum	
severity_prev	LOCAL	SREL	sev.enum	
sla_violation	sla_violation	INTEGER		
base_template	solution	STRING	call_req persid	
status	status	STRING	cr_stat code	
status_prev	LOCAL	SREL	crs.code	
string1	string1	STRING		
string2	string2	STRING		
string3	string3	STRING		
string4	string4	STRING		
string5	string5	STRING		
string6	string6	STRING		
summary	summary	STRING		
support_lev	support_lev	STRING	srv_desc code	
template_name	template_name	STRING	cr_template template_name	
time_spent_ sum	time_spent_ sum	DURATION		
type	type	STRING	crt code	
urgency	urgency	INTEGER	urgncy enum	

Attribute	DB Field	Data Type	SREL References	Flags
urgency_prev	LOCAL	SREL	urg.enum	

pr_trans Object

The object details are as follows:

1. Associated Tables: pr_trans
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
status	status	STRING	crs	Specifies the current ticket status.
new_status	new status	STRING	crs	Specifies the new ticket status.
is default		INTEGER		Default transition that appears when the Status field is empty. On new default: 0
must_comment		INTEGER		Comment required when using a transition. On new default: 0
delete_flag	del		actbool	Required. On new default: 0
condition			macro	Site condition macro to approve transition.
condition_error		STRING		Error message for site condition.
description		STRING		Description of this transition.
last_mod_by			cnt	On new default user; on CI set user
last_mod_dt		DATE		On CI set user now

prod Object

The object details are as follows:

1. Associated Table: Product
2. Factories: default

3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY

quick_tpl_types Object

The object details are as follows:

1. Associated Table: Quick_Template_Types
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
enum	enum	INTEGER		UNIQUE REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
description	nx_desc	STRING		
persistent_id	persid	STRING		
sym	sym	STRING		

rc Object

The object details are as follows:

1. Associated Table: Rootcause

2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY

resocode Object

This object is a reference object to denote the resolution code of the request or incident.

The object details are as follows:

1. Associated Table: usp_resolution_code
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	Data Type	Reference	Flags
delete_flag	SREL	actbool.enum	ON_NEW
description	STRING		
id	INTEGER		UNIQUE
persistent_id	STRING		
last_mod_by	SREL	cnt	ON_NEW {USER} ON_CI {USER}
last_mod_dt	DATE		ON_CI {NOW}
sym	STRING		REQUIRED

resomethod Object

This object is a reference object to denote the resolution method of the request or incident.

The object details are as follows:

1. Associated Table: usp_resolution_method
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	Data Type	Reference	Flags
delete_flag	SREL	actbool.enum	ON_NEW
description	STRING		
id	INTEGER		UNIQUE
persistent_id	STRING		
last_mod_by	SREL	cnt	ON_NEW {USER} ON_CI {USER}
last_mod_dt	DATE		ON_CI {NOW}
sym	STRING		REQUIRED

response Object

The object details are as follows:

1. Associated Table: Response
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
chg_flag	chg_flag	INTEGER		S_KEY
cr_flag	cr_flag	INTEGER		S_KEY

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
in_flag	in_flag	INTEGER		S_KEY
iss_flag	iss_flag	INTEGER		S_KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
pr_flag	pr_flag	INTEGER		S_KEY
response	response	STRING		
response_owner	response_owner	UUID	ca_contact uuid	S_KEY
sym	sym	STRING		REQUIRED S_KEY

rest_access Object

The object details are as follows:

1. Associated Table: usp_rest_access
2. Factories: rest_access
3. REL_ATTR: id
4. Common Name: access_key
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE DELETE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		KEY
producer_id		LOCAL STRING 20		
persistent_id		LOCAL STRING 60		
access_key	access_key	INTEGER		REQUIRED
contact	contact	SREL	cnt.id (http://cnt.id)	REQUIRED
secret_key	secret_key	STRING 64		
expiration_date	expiration_date	DATE		
suppress_trigger		LOCAL INTEGER		

rrf Object

The object details are as follows:

1. Associated Table: Remote_Ref
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
arch_type	arch_type	STRING		
code	code	STRING		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
exec_str	exec_str	STRING		
function_group	function_group	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
pcexec_str	pcexec_str	STRING		
sym	sym	STRING		REQUIRED

rss Object

The object details are as follows:

1. Associated Table: ca_resource_status
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: ci_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
delete_time	delete_time	LOCAL_TIME		
exclude_registration	exclude_registration	integer		
id	id	INTEGER		UNIQUE REQUIRED KEY
delete_flag	inactive	integer	actbool enum	
last_update_date	last_update_date	LOCAL_TIME		
last_update_user	last_update_user	STRING		
sym	name	STRING		
version_number	version_number	integer		

seq Object

The object details are as follows:

1. Associated Table: Sequence_Control
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
code	code	STRING		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
prefix	prefix	STRING		
suffix	suffix	STRING		
sym	sym	STRING		REQUIRED

sev Object

The object details are as follows:

1. Associated Table: Severity
2. Factories: default

3. REL_ATTR: enum
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
enum	enum	INTEGER		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
description	nx_desc	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY

SHOW_OBJ Object

The object details are as follows:

1. Associated Table: SHOW_OBJ
2. Factories: default
3. REL_ATTR: id
4. Common Name: OBJ_PERSID
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attributes	DB Field	Data Type	SREL References	Flags
Expiration Date	EXPIRE_DATE	LOCAL_TIME		
id	ID	INTEGER		KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Object ID	OBJ_PERSID	STRING		
Password	PWD	STRING		

site Object

The object details are as follows:

1. Associated Table: ca_site

2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
alias	alias	STRING		
contact	contact_uuid	UUID	ca_contact uuid	
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
delete_time	delete_time	LOCAL_TIME		
exclude_registration	exclude_registration	integer		
id	id	INTEGER		UNIQUE REQUIRED KEY
delete_flag	inactive	integer	actbool enum	
last_mod	last_update_date	LOCAL_TIME		
last_update_user	last_update_user	STRING		
name	name	STRING		
version_number	version_number	integer		

slatpl Object

The object details are as follows:

1. Associated Table: SLA_Template
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
elapsed	elapsed	DURATION		REQUIRED
event	event	STRING	evt persid	

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
object_type	object_type	STRING		
persistent_id	persid	STRING		
service_type	service_type	STRING	srv_desc code	REQUIRED
sym	sym	STRING		REQUIRED S_KEY

special_handling Object

The object details are as follows:

1. Associated Table: usp_special_handling
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Field	Data Type	Reference	Flags
id	INTEGER UNIQUE		
producer_id	LOCAL STRING (20)		
persistent_id	LOCAL STRING (60)		
delete_flag	SREL	actbool	REQUIRED. ON_NEW
sym	STRING (60)		REQUIRED
description	STRING (4000)		
alert_icon_url	STRING (1000)		
alert_text	STRING (60)		
autodisplay_notes	SREL	bool.enum	ON_NEW
escalate_urgency	SREL	bool.enum	ON_NEW
cnthandling_list	BREL	contact_handling.special_handling	DYNAMIC
last_mod_by	SREL	cnt	ON_NEW {USER} ON_CI SET {USER}
last_mod_dt	DATE		ON_CI_SET {NOW}

svc_contract Object

The object details are as follows:

1. Associated Table: Service_Contract
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
active	active	INTEGER	actbool enum	
contract_num	contract_num	STRING		
delete_flag	del	INTEGER	actbool enum	
dflt_chgcat_st	dflt_chgcat_st	STRING	srv_desc code	
dflt_cnt_st	dflt_cnt_st	STRING	srv_desc code	
dflt_isscat_st	dflt_isscat_st	STRING	srv_desc code	
dflt_nr_st	dflt_nr_st	STRING	srv_desc code	
dflt_pcat_st	dflt_pcat_st	STRING	srv_desc code	
dflt_pri_st	dflt_pri_st	STRING	srv_desc code	
expiration	expiration	LOCAL_TIME		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
description	nx_desc	STRING		
service_type	org_svc_type	STRING	srv_desc code	
persistent_id	persid	STRING		
svc_advocate	svc_advocate	UUID	ca_contact uuid	
svc_owner	svc_owner	UUID	ca_contact uuid	
sym	sym	STRING		

typecnt Object

The object details are as follows:

1. Associated Table: Type_Of_Contact
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym

5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY

tz Object

The object details are as follows:

1. Associated Table: Timezone
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: timezone
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
code	code	STRING		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
dst_delta	dst_delta	INTEGER		
end_abs_date	end_abs_date	LOCAL_TIME		
end_day	end_day	INTEGER		
end_mon	end_mon	INTEGER		
end_pos	end_pos	INTEGER		
gmt_delta	gmt_delta	INTEGER		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
start_abs_date	start_abs_date	LOCAL_TIME		

Attribute	DB Field	Data Type	SREL References	Flags
start_day	start_day	INTEGER		
start_mon	start_mon	INTEGER		
start_pos	start_pos	INTEGER		
sym	sym	STRING		REQUIRED S_KEY

tspan Object

The object details are as follows:

1. Associated Table: Timespan
2. Factories: default
3. REL_ATTR: sym
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
code	code	STRING		UNIQUE REQUIRED
end_day	end_day	STRING		
end_hour	end_hour	STRING		
end_minute	end_minute	STRING		
end_month	end_month	STRING		
end_year	end_year	STRING		
id	id	INTEGER		UNIQUE KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
desc	nx_desc	STRING		
start_day	start_day	STRING		
start_hour	start_hour	STRING		
start_minute	start_minute	STRING		
start_month	start_month	STRING		
start_year	start_year	STRING		
sym	sym	STRING		UNIQUE REQUIRED
trigger_day	trigger_day	STRING		
trigger_hour	trigger_hour	STRING		
trigger_minute	trigger_minute	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
trigger_month	trigger_month	STRING		
trigger_year	trigger_year	STRING		

tab Object

The object details are as follows:

1. Associated Table: usp_tab
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: Security
6. REST Operations: CREATE READ UPDATE

Attribute Name	Data Type	Relationship Object	Flags
id	INTEGER		UNIQUE
name	STRING		REQUIRED
code	STRING		UNIQUE; REQUIRED
display_name	STRING		REQUIRED
delete_flag	SREL	actbool	REQUIRED
description	STRING		
menu_bar_obj	SREL	menu_bar	
web_form_obj	SREL	web_form	
last_mod_dt	DATE		
last_mod_by	SREL	cnt	

transition_type Object

The object details are as follows:

1. Associated Table: transition_type
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. Tenant: optional

7. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
sym		STRING		Required
ss_flag		INTEGER		Required On new default: 0
ss_button_text		STRING		Required
ss_header_text		STRING		Required
delete_flag	del		actbool	Required On new default: 0
description		STRING		
last_mod_dt		DATE		On CI set now
last_mod_by			cnt	On CI set user On new default user

urg Object

The object details are as follows:

1. Associated Table: Urgency
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. Function Group: prioritization
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
enum	enum	INTEGER		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
description	nx_desc	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY
value	value	INTEGER		

USP_PREFERENCES Object

The object details are as follows:

1. Associated Table: USP_PREFERENCES
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Contact ID	ANALYST_ID	UUID	ca_contact uuid	
Knowledge Categories - Documents Per Page	ARC_DOCS_TO_DISPLAY	INTEGER		
Assignee	ASSIGNEE	INTEGER		
Author	AUTHOR	INTEGER		
FAQ Rating	BU_RESULT	INTEGER		
Mouseover Menus	CLASSIC_RESULTSET_CONTEXT	INTEGER		
Created Via	CREATED_VIA	INTEGER		
Creation Date	CREATION_DATE	INTEGER		
Current Task	CURRENT_ACTION	INTEGER		
Custom 1	CUSTOM1	INTEGER		
Custom 2	CUSTOM2	INTEGER		
Custom 3	CUSTOM3	INTEGER		
Custom 4	CUSTOM4	INTEGER		
Custom 5	CUSTOM5	INTEGER		
Custom Num 1	CUSTOM_NUM1	INTEGER		
Custom Num 2	CUSTOM_NUM2	INTEGER		
Document ID	DOC_ID	INTEGER		
Document Template	DOC_TEMPLATE	INTEGER		
Document Type	DOC_TYPE	INTEGER		
Document Version	DOC_VERSION	INTEGER		
Expiration Date	EXPIRATION_DATE	INTEGER		
GLOBALSD_ACTIVE_ZONE	GLOBALSD_ACTIVE_ZONE	INTEGER		
Hits	HITS	INTEGER		
id	ID	INTEGER		REQUIRED KEY

Attribute	DB Field	Data Type	SREL References	Flags
INBOX_COUNTER	INBOX_COUNTER	INTEGER		
Initiator	INITIATOR	INTEGER		
Item	ITEM	INTEGER		
KT_REPORT_CARD_APAST_DAYS	KT_REPORT_CARD_PAST_DAYS	INTEGER		
KT_REPORT_CARD_SCREEN_DEFAULT	KT_REPORT_CARD_SCREEN_DEFAULT	INTEGER		
Last Accepted Date	LAST_ACCEPTED_DATE	INTEGER		
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Modify Date	MODIFY_DATE	INTEGER		
Knowledge Documents View Mode	ONE_B_DOC_VIEW_MODE	INTEGER		
Knowledge Documents Per Page	ONE_B_DOCS_TO_DISPLAY	INTEGER		
Knowledge Documents Show Details Flag	ONE_B_HIDE_DETAILS	INTEGER		
EBR Match Type	ONE_B_MATCH_TYPE	INTEGER		
EBR Search Fields	ONE_B_SEARCH_FIELDS	INTEGER		
EBR Search Order	ONE_B_SEARCH_ORDER	STRING		
EBR Search Type	ONE_B_SEARCH_TYPE	INTEGER		
EBR Word Parts	ONE_B_WORD_PARTS	INTEGER		
Owner	OWNER	INTEGER		
Primary Category	PRIMARY_INDEX	INTEGER		
Workflow Priority	PRIORITY	INTEGER		
Product	PRODUCT	INTEGER		
Published Date	PUBLISHED_DATE	INTEGER		
Review Date	REVIEW_DATE	INTEGER		
Solution Count	SD_ACCEPTED_HITS	INTEGER		
Impact	SD_IMPACT	INTEGER		
Priority	SD_PRIORITY	INTEGER		
Root Cause	SD_ROOTCAUSE	INTEGER		
SD_SEARCH_FIELDS_CR	SD_SEARCH_FIELDS_CR	INTEGER		
SD_SEARCH_FIELDS_ISS	SD_SEARCH_FIELDS_ISS	INTEGER		
Severity	SD_SEVERITY	INTEGER		
Urgency	SD_URGENCY	INTEGER		
Start Date	START_DATE	INTEGER		
Status	STATUS	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
Subject Expert	SUBJECT_EXPERT	INTEGER		
User Defined ID	USER_DEF_ID	INTEGER		
WEB_LAST_LOGIN	WEB_LAST_LOGIN	LOCAL_TIME		
WEB_POPUP1_HEIGHT	WEB_POPUP1_HEIGHT	INTEGER		
WEB_POPUP1_WIDTH	WEB_POPUP1_WIDTH	INTEGER		
WEB_POPUP2_HEIGHT	WEB_POPUP2_HEIGHT	INTEGER		
WEB_POPUP2_WIDTH	WEB_POPUP2_WIDTH	INTEGER		
WEB_POPUP3_HEIGHT	WEB_POPUP3_HEIGHT	INTEGER		
WEB_POPUP3_WIDTH	WEB_POPUP3_WIDTH	INTEGER		
WEB_POPUP4_HEIGHT	WEB_POPUP4_HEIGHT	INTEGER		
WEB_POPUP4_WIDTH	WEB_POPUP4_WIDTH	INTEGER		
WEB_ROLE_ID	WEB_ROLE_ID	STRING		
WEB_PREFERENCES	WEB_PREFERENCES	INTEGER		
WEB_SUPPRESS_TOUR	WEB_SUPPRESS_TOUR	INTEGER		
WEB_TOOLBAR_TAB	WEB_TOOLBAR_TAB	INTEGER		
WF_TEMPLATE	WF_TEMPLATE	INTEGER		

usp_exlist_format Object

The object details are as follows:

1. Associated Table: usp_exlist_format
2. Factories: default
3. REL_ATTR: id
4. Common Name: file_extension
5. Function Group: admin
6. Tenant: optional

Attribute	DB Field	Data Type	SREL References	Flags
file_extension		STRING		REQUIRED
mime_type		STRING		REQUIRED
xslt_name		STRING		
delete_flag		del	actbool enum	REQUIRED. On new default: 0

USP_PROPERTIES Object

The object details are as follows:

1. Associated Table: USP_PROPERTIES
2. Factories: default
3. REL_ATTR: id
4. Common Name: PROPERTY_NAME
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		REQUIRED KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Property Default	PROPERTY_DEFAULT	STRING		
Property Description	PROPERTY_DESCRIPTION	STRING		
Property Name	PROPERTY_NAME	STRING		S_KEY
Property Type	PROPERTY_TYPE	STRING		
Property Value	PROPERTY_VALUE	STRING		

usp_session_ticket Object

The object details are as follows:

1. Associated Table: usp_session_ticket
2. REL_ATTR: id
3. Common Name: session_persid
4. Function Group: change_reference
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
producer_id		LOCAL_STRING 20		
persistent_id	persid	STRING 30		
delete_flag	del	SREL	actbool.enum	REQUIRED
sym	sym	STRING 60		REQUIRED
description	description	STRING 240		

modified_date	last_mod_dt	DATE	
last_mod_by	last_mod_by	SREL	cnt.id (http://cnt.id)

usq Object

The object details are as follows:

1. Associated Table: User_Query
2. Factories: default
3. REL_ATTR: id
4. Common Name: label
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
expanded	expanded	INTEGER		
factory	factory	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
label	label	STRING		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
obj_persid	obj_persid	STRING		
parent	parent	INTEGER	usq id	
persistent_id	persid	STRING		
role_persid	role_persid	STRING		
query	query	STRING	crsq code	
query_set	query_set	INTEGER		
query_type	query_type	INTEGER		
sequence	sequence	INTEGER		REQUIRED

vpt Object

The object details are as follows:

1. Associated Table: ca_company_type
2. Factories: default

3. REL_ATTR: id
4. Common Name: sym
5. Function Group: ci_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
creation_date	creation_date	LOCAL_TIME		
creation_user	creation_user	STRING		
description	description	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
delete_flag	inactive	integer	actbool enum	
last_mod	last_update_date	LOCAL_TIME		
last_update_user	last_update_user	STRING		
sym	name	STRING		
version_number	version_number	integer		

wrkshft Object

The object details are as follows:

1. Associated Table: Bop_Workshift
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: sym
5. Function Group: workshifts
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
description	description	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
sched	sched	STRING		
sym	sym	STRING		REQUIRED

usq Object

The object details are as follows:

1. Associated Table: User_Query
2. Factories: default
3. REL_ATTR: id
4. Common Name: label
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
expanded	expanded	INTEGER		
factory	factory	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
label	label	STRING		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
obj_persid	obj_persid	STRING		
parent	parent	INTEGER	usq id	
persistent_id	persid	STRING		
role_persid	role_persid	STRING		
query	query	STRING	crsq code	
query_set	query_set	INTEGER		
query_type	query_type	INTEGER		
sequence	sequence	INTEGER		REQUIRED

Access

This article contains the following topics:

acctyp_role Object

The object details are as follows:

1. Associated Table: usp_acctyp_role
2. Factories: default

3. REL_ATTR: id
4. Common Name:
5. Function Group: Security
6. REST Operations: CREATE READ UPDATE

Attributes	Data Type	Related Object	Flags
id	INTEGER		
access_type	SREL	acctyp	
role_obj	SREL	role	
is_default	INTEGER		
last_mod_dt	DATE		

acctyp Object

The object details are as follows:

1. Associated Table: Access_Type_v2
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
access_level	access_level	INTEGER	acc_lvls enum	REQUIRED
default_flag	default_flag	INTEGER		
delete_flag	del	INTEGER	actbool enum	REQUIRED
description	description	STRING		
external_auth	external_auth	INTEGER		REQUIRED
grant_level	grant_level	INTEGER	acc_lvls enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
ldap_access_grou	ldap_access_group	STRING	ldap_group_id	
pin_field	pin_field	STRING		
persistent_id	persid			

Attribute	DB Field	Data Type	SREL References	Flags
		LOCAL STRING 60		
roles	roles	LIST		
sym	sym	STRING		REQUIRED S_KEY
user_auth	User_auth	INTEGER		REQUIRED
view_internal	view_internal	INTEGER		REQUIRED
wsp	wsp	INTEGER		
cmdlind_role	cmdline_role	INTEGER	role id	
reporting_role	reporting_role	INTEGER	role id	
web_service_role	web_service_role	INTEGER	role id	
rest_web_service_role	rest_web_service_role	SREL	role.id (http://role.id)	

acc_lvls Object

The object details are as follows:

1. Associated Table: Access_Levels
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
enum	enum	INTEGER		UNIQUE REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
description	nx_desc	STRING		
persistent_id	persid	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY

Attachment Objects

This topic contains the following information:

attmnt Object

The object details are as follows:

1. Associated Table: Attachment
2. Factories: default
3. REL_ATTR: id
4. Common Name: created_dt
5. Function Group: call_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
attmnt_name	attmnt_name	STRING		
attmnt_uuid	attmnt_uuid	UUID		
created_by	created_by	UUID	ca_contact uuid	
created_dt	created_dt	LOCAL_TIME		
delete_flag	del	INTEGER	actbool enum	REQUIRED
description	description	STRING		
exec_cmd	exec_cmd	STRING	rem_ref code	
file_date	file_date	LOCAL_TIME		
file_name	file_name	STRING		
file_size	file_size	INTEGER		
file_type	file_type	STRING		
folder_id	folder_id	INTEGER	attmnt_folder id	
folder_path_ids	folder_path_ids	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
inherit_permission_id	inherit_permission_id	INTEGER		
KDS_ATTACHED	KDS_ATTACHED	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact uuid	Specifies the UUID of the contact who last modified this record.

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_dt	last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
link_only	link_only	INTEGER	bool_tab enum	
link_type	link_type	STRING 255		
orig_file_name	orig_file_name	STRING		
persistent_id	persid	STRING		
pgroup_type	pgroup_type	INTEGER		Indicates if the P Groups is based on Roles or Groups: **1** -- Groups (Default) **2** -- Roles
read_pgroup	read_pgroup	INTEGER	P_GROUPS id	
rel_file_path	rel_file_path	STRING		
repository	repository	SREL	doc_rep persid	
sec_uuid	sec_uuid	UUID		
status	status	STRING		
tenant	tenant	UUID	ca_tenant	Specifies the UUID of the tenant.
write_pgroup	write_pgroup	INTEGER	P_GROUPS id	
zip_flag	zip_flag	INTEGER		

attmnt_folder Object

The object details are as follows:

1. Associated Table: attmnt_folder
2. Factories: default
3. REL_ATTR: id
4. Common Name: folder_name
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
folder_name	folder_name	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
folder_path_ids	folder_path_ids	STRING		
folder_type	folder_type	INTEGER		
has_children	has_children	INTEGER		
id	id	INTEGER		REQUIRED KEY
inherit_ permission_id	inherit_ permission_id	INTEGER	attmnt_folder id	
last_mod_date	last_mod_date	LOCAL_TIME		
parent_id	parent_id	SREL	attmnt_folder id	
read_pgroup	read_pgroup	INTEGER	P_GROUPS id	
repository	repository	SREL	doc_rep persid	
write_pgroup	write_pgroup	INTEGER	P_GROUPS id	

Boolean Objects

This topic contains the following information:

rev_bool Object

The object details are as follows:

1. Associated Table: Reverse_Boolean_Table
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER		REQUIRED
enum	enum	INTEGER		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
desc	nx_desc	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY

actbool Object

The object details are as follows:

1. Associated Table: Active_Boolean_Table
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER		REQUIRED
description	description	STRING		
enum	enum	INTEGER		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		
sym	sym	STRING		S_KEY

actrbool Object

The object details are as follows:

1. Associated Table: Active_Reverse_Boolean_Table
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER		REQUIRED
description	description	STRING		
enum	enum	INTEGER		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		
sym	sym	STRING		S_KEY

Business Management

This topic contains the following information:

bmcls Object

The object details are as follows:

1. Associated Table: Business_Management_Class
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
description	nx_desc	STRING		
persistent_id	persid	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY

bmhier Object

The object details are as follows:

1. Associated Table: Business_Management
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
bm_rep	bm_rep	INTEGER	busrep id	
cost	cost	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
child	hier_child	UUID	ca_owned_resource uuid	REQUIRED
parent	hier_parent	UUID	ca_owned_resource uuid	
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
description	nx_desc	STRING		
persistent_id	persid	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY

bmrep Object

The object details are as follows:

1. Associated Table: Business_Management_Repository
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
hostname	hostname	STRING		UNIQUE REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
description	nx_desc	STRING		
password	password	STRING		
persistent_id	persid	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY
userid	userid	STRING		

bms Object

The object details are as follows:

1. Associated Table: Business_Management_Status
2. Factories: default
3. REL_ATTR: status_no

4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
description	nx_desc	STRING		
persistent_id	persid	STRING		
status_no	status_no	INTEGER		UNIQUE REQUIRED S_KEY
sym	sym	STRING		UNIQUE REQUIRED S_KEY

USP

This article contains the following topics:

USP_PREFERENCES Object

The object details are as follows:

1. Associated Table: USP_PREFERENCES
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Contact ID	ANALYST_ID	UUID	ca_contact uuid	
Knowledge Categories - Documents Per Page	ARC_DOCS_TO_DISPLAY	INTEGER		
Assignee	ASSIGNEE	INTEGER		
Author	AUTHOR	INTEGER		
FAQ Rating	BU_RESULT	INTEGER		
Mouseover Menus	CLASSIC_RESULTSET_CONTEXT	INTEGER		
Created Via	CREATED_VIA	INTEGER		
Creation Date	CREATION_DATE	INTEGER		
Current Task	CURRENT_ACTION	INTEGER		
Custom 1	CUSTOM1	INTEGER		
Custom 2	CUSTOM2	INTEGER		
Custom 3	CUSTOM3	INTEGER		
Custom 4	CUSTOM4	INTEGER		
Custom 5	CUSTOM5	INTEGER		
Custom Num 1	CUSTOM_NUM1	INTEGER		
Custom Num 2	CUSTOM_NUM2	INTEGER		
Document ID	DOC_ID	INTEGER		
Document Template	DOC_TEMPLATE	INTEGER		
Document Type	DOC_TYPE	INTEGER		
Document Version	DOC_VERSION	INTEGER		
Expiration Date	EXPIRATION_DATE	INTEGER		
GLOBALSD_ACTIVE_ZONE	GLOBALSD_ACTIVE_ZONE	INTEGER		
Hits	HITS	INTEGER		
id	ID	INTEGER		REQUIRED KEY
INBOX_COUNTER	INBOX_COUNTER	INTEGER		
Initiator	INITIATOR	INTEGER		
Item	ITEM	INTEGER		
KT_REPORT_CARD_APAST_DAYS	KT_REPORT_CARD_PAST_DAYS	INTEGER		
KT_REPORT_CARD_SCREEN_DEFAULT	KT_REPORT_CARD_SCREEN_DEFAULT	INTEGER		
Last Accepted Date	LAST_ACCEPTED_DATE	INTEGER		
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		

Attribute	DB Field	Data Type	SREL References	Flags
Modify Date	MODIFY_DATE	INTEGER		
Knowledge Documents View Mode	ONE_B_DOC_VIEW_MODE	INTEGER		
Knowledge Documents Per Page	ONE_B_DOCS_TO_DISPLAY	INTEGER		
Knowledge Documents Show Details Flag	ONE_B_HIDE_DETAILS	INTEGER		
EBR Match Type	ONE_B_MATCH_TYPE	INTEGER		
EBR Search Fields	ONE_B_SEARCH_FIELDS	INTEGER		
EBR Search Order	ONE_B_SEARCH_ORDER	STRING		
EBR Search Type	ONE_B_SEARCH_TYPE	INTEGER		
EBR Word Parts	ONE_B_WORD_PARTS	INTEGER		
Owner	OWNER	INTEGER		
Primary Category	PRIMARY_INDEX	INTEGER		
Workflow Priority	PRIORITY	INTEGER		
Product	PRODUCT	INTEGER		
Published Date	PUBLISHED_DATE	INTEGER		
Review Date	REVIEW_DATE	INTEGER		
Solution Count	SD_ACCEPTED_HITS	INTEGER		
Impact	SD_IMPACT	INTEGER		
Priority	SD_PRIORITY	INTEGER		
Root Cause	SD_ROOTCAUSE	INTEGER		
SD_SEARCH_FIELDS_CR	SD_SEARCH_FIELDS_CR	INTEGER		
SD_SEARCH_FIELDS_ISS	SD_SEARCH_FIELDS_ISS	INTEGER		
Severity	SD_SEVERITY	INTEGER		
Urgency	SD_URGENCY	INTEGER		
Start Date	START_DATE	INTEGER		
Status	STATUS	INTEGER		
Subject Expert	SUBJECT_EXPERT	INTEGER		
User Defined ID	USER_DEF_ID	INTEGER		
WEB_LAST_LOGIN	WEB_LAST_LOGIN	LOCAL_TIME		
WEB_POPUP1_HEIGHT	WEB_POPUP1_HEIGHT	INTEGER		
WEB_POPUP1_WIDTH	WEB_POPUP1_WIDTH	INTEGER		
WEB_POPUP2_HEIGHT	WEB_POPUP2_HEIGHT	INTEGER		
WEB_POPUP2_WIDTH	WEB_POPUP2_WIDTH	INTEGER		
WEB_POPUP3_HEIGHT	WEB_POPUP3_HEIGHT	INTEGER		
WEB_POPUP3_WIDTH	WEB_POPUP3_WIDTH	INTEGER		

WEB_POPUP4_HEIGHT	WEB_POPUP4_HEIGHT	INTEGER
WEB_POPUP4_WIDTH	WEB_POPUP4_WIDTH	INTEGER
WEB_ROLE_ID	WEB_ROLE_ID	STRING
WEB_PREFERENCES	WEB_PREFERENCES	INTEGER
WEB_SUPPRESS_TOUR	WEB_SUPPRESS_TOUR	INTEGER
WEB_TOOLBAR_TAB	WEB_TOOLBAR_TAB	INTEGER
WF_TEMPLATE	WF_TEMPLATE	INTEGER

usp_conflict

Change order conflicts.

Attribute	Data Type	SREL References	Flags
id	INTEGER		UNIQUE NOT_NULL KEY
persid	STRING 30		
del	INTEGER		NOT_NULL
comments	STRING 1000		
conflict_begin	LOCAL_TIME		
conflict_change	INTEGER	Change_Request	NOT_NULL
conflict_ci	UUID	ca_owned_resource	
conflict_end	LOCAL_TIME		
conflict_status	STRING 30	usp_conflict_status	NOT_NULL
conflict_type	STRING 30	usp_conflict_type	NOT_NULL
creation_dt	LOCAL_TIME		
is_resolved	INTEGER		NOT_NULL
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
source_change	INTEGER	Change_Request	NOT_NULL
tenant	UUID	ca_tenant	

usp_conflict_chg

Change order conflict change.

Attribute	Data Type	SREL References	Flags
id	INTEGER		UNIQUE NOT_NULL KEY
change	INTEGER	Change_Request	NOT_NULL

conflict	INTEGER	usp_conflict	NOT_NULL
conflict_change	INTEGER	Change_Request	
is_cause	INTEGER		NOT_NULL
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
tenant	UUID	ca_tenant	

usp_conflict_status

Change order conflict status.

Attribute	Data Type	SREL References	Flags
id	INTEGER		UNIQUE NOT_NULL KEY
persid	STRING 30		
del	INTEGER		NOT_NULL
code	STRING 30		UNIQUE NOT_NULL
description	STRING 1000		
is_resolved	INTEGER		NOT_NULL
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
sym	STRING 60		UNIQUE NOT_NULL S_KEY
tenant	UUID	ca_tenant	

usp_conflict_type

Change order conflict type.

Attribute	Data Type	SREL References	Flags
id	INTEGER		UNIQUE NOT_NULL KEY
persid	STRING 30		
del	INTEGER		NOT_NULL
code	STRING 30		UNIQUE NOT_NULL
description	STRING 1000		
icon	STRING 1000		
last_mod_dt	LOCAL_TIME		
last_mod_by	UUID	ca_contact	
sym	STRING 60		UNIQUE NOT_NULL S_KEY
tenant	UUID	ca_tenant	

usp_exlist_format Object

The object details are as follows:

1. Associated Table: usp_exlist_format
2. Factories: default
3. REL_ATTR: id
4. Common Name: file_extension
5. Function Group: admin
6. Tenant: optional

Attribute	DB Field	Data Type	SREL References	Flags
file_extension		STRING		REQUIRED
mime_type		STRING		REQUIRED
xslt_name		STRING		
delete_flag		del	actbool enum	REQUIRED. On new default: 0

USP_PROPERTIES Object

The object details are as follows:

1. Associated Table: USP_PROPERTIES
2. Factories: default
3. REL_ATTR: id
4. Common Name: PROPERTY_NAME
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		REQUIRED KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Property Default	PROPERTY_DEFAULT	STRING		
Property Description	PROPERTY_DESCRIPTION	STRING		
Property Name	PROPERTY_NAME	STRING		S_KEY
Property Type	PROPERTY_TYPE	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
Property Value	PROPERTY_VALUE	STRING		

usp_session_ticket Object

The object details are as follows:

1. Associated Table: usp_session_ticket
2. REL_ATTR: id
3. Common Name: session_persid
4. Function Group: change_reference
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
producer_id		LOCAL_STRING 20		
persistent_id	persid	STRING 30		
delete_flag	del	SREL	actbool.enum	REQUIRED
sym	sym	STRING 60		REQUIRED
description	description	STRING 240		
modified_date	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id	

window Object

The object details are as follows:

1. Associated Table: usp_window
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References
sym	sym	STRING 60	
window_type	window_type	INTEGER	usp_window_type
start_date	start_date	LOCAL_TIME	

Attribute	DB Field	Data Type	SREL References
end_date	end_date	LOCAL_TIME	
final_end_date	final_end_date	LOCAL_TIME	
timezone	timezone	STRING 30	
non_global	is_non_global	INTEGER	
icon	icon	INTEGER	
recurs	recurs	INTEGER	
recurrence_ interval	recurrence_interval	INTEGER	
sunday	sunday	INTEGER	
monday	monday	INTEGER	
tuesday	tuesday	INTEGER	
wednesday	wednesday	INTEGER	
thursday	thursday	INTEGER	
friday	friday	INTEGER	
saturday	saturday	INTEGER	
occurrence	occurrence	INTEGER	
description	description	STRING 400	
legend	legend	STRING 100	
color	color	STRING 100	
bgcolor	bgcolor	STRING 100	
style	style	STRING 100	
last_mod_dt	last_mod_dt	LOCAL_TIME	
last_mod_by	last_mod_by	UUID	ca_contact
delete_flag	del	INTEGER	
tenant	tenant	UUID	ca_tenant

window_type Object

The object details are as follows:

1. Associated Table: usp_window_type
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
sym	sym	STRING 60		
description	description	STRING 100		
last_mod_dt	last_mod_dt	LOCAL_TIME		
last_mod_by	last_mod_by	UUID	ca_contact	
delete_flag	del	INTEGER	actbool.enum	REQUIRED

Change Request Objects

This article contains the following topics:

chg Object

The object details are as follows:

1. Associated Table: Change_Request
2. Factories: default
3. REL_ATTR: id
4. Common Name: chg_ref_num
5. Function Group: change_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
actions	actions	STRING		
active	active_flag	INTEGER	bool_tab enum	REQUIRED
active_prev	LOCAL	SREL	bool.enum	
actual_comp_ date	actual_comp_ date	LOCAL_ TIME		

cost	actual_cost	INTEGER		
actual_total_ time	actual_total_ time	DURATION		
affected_contact	affected_contact	UUID	ca_contact uuid	REQUIRED
assignee	assignee	UUID		
assignee_prev	LOCAL	SREL	agt.id (http://agt.id)	
backout_plan	backout_plan	STRING		
business_case	business_case	STRING 4000		
call_back_date	call_back_date	LOCAL_ TIME		
call_back_flag	call_back_flag	INTEGER		
category	category	STRING	chgcat code	
category_prev	LOCAL	SREL	chgcat.code	
cawf_procid	cawf_procid	STRING		
chg_ref_num	chg_ref_num	STRING		UNIQUE REQUIRED S_KEY
chgtype	chgtype	SREL	chgtype.id (http://chgtype.id)	
close_date	close_date	LOCAL_TI ME		
closure_code	closure_code	SREL		
created_via	created_via	INTEGER	interface id	
effort	effort	STRING 4000		
est_comp_date	est_comp_date	LOCAL_TI ME		
est_cost	est_cost	INTEGER		
est_total_time	est_total_time	DURATION		
requested_by		SREL	cnt.id (http://cnt.id)	
external_system_tic ket		STRING (4000)		
orig_user_dept		SREL	dept.id (http://dept.id)	
orig_user_organizati on		SREL	org.id (http://org.id)	
orig_user_admin_or g		SREL	org.id (http://org.id)	
orig_user_cost_cent er		SREL	cost_cntr.id (http://cost_cntr. id)	
flag1	flag1	INTEGER		
flag2	flag2	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
flag3	flag3	INTEGER		
flag4	flag4	INTEGER		
flag5	flag5	INTEGER		
flag6	flag6	INTEGER		
group	group_id	UUID		
group_prev	LOCAL	SREL	grp.id (http://grp.id)	
id	id	INTEGER		UNIQUE REQUIRED KEY
impact	impact	INTEGER	impact enum	
impact_prev	LOCAL	SREL	imp.enum	
justification	justification	STRING 4000		Business Justification
last_mod_by	last_mod_by	UUID	ca_contact uuid	
modified_date	last_mod_dt	LOCAL_TIME		
log_agent	log_agent	UUID	ca_contact uuid	REQUIRED
macro_predicted_violation	macro_predict_ viol	INTEGER		
need_by	need_by	LOCAL_TIME		
open_date	open_date	LOCAL_TIME		
organization	organization	UUID	ca_organization uuid	
orig_user_admin_org		SREL	org	
orig_user_cost_center		SREL	cost_cntr	
orig_user_dept		SREL	dept	
orig_user_organization		SREL	org	
parent	parent	INTEGER	chg id	
persistent_id	persid	STRING		
person_ contacting	person_ contacting	INTEGER	perscon id	
predicted_sla_ violation	predicted_sla_ viol	INTEGER		
priority	priority	INTEGER	pri enum	REQUIRED
priority_prev	LOCAL	SREL	pri.enum	
product	product	INTEGER	product id	
reporting_ method	reporting_ method	INTEGER	repmeth id	

Attribute	DB Field	Data Type	SREL References	Flags
requestor	requestor	UUID	ca_contact uuid	REQUIRED
resolve_date	resolve_date	LOCAL_TIME		
risk	risk	SREL	risk_level	
rootcause	rootcause	INTEGER	rootcause id	
sched_start_date	sched_start_date	LOCAL_TIME		
sched_end_date	sched_end_date	LOCAL_TIME		
sched_duration	sched_duration	LOCAL_TIME		
service_date	service_date	LOCAL_TIME		
service_num	service_num	STRING		
sla_violation	sla_violation	INTEGER		
start_date	start_date	LOCAL_TIME		
status	status	STRING	chgstat code	
status_prev	LOCAL	SREL	chgstat.code	
string1	string1	STRING		
string2	string2	STRING		
string3	string3	STRING		
string4	string4	STRING		
string5	string5	STRING		
string6	string6	STRING		
submittedSurvey		BREL	risk_svy	
summary	summary	STRING		
support_lev	support_lev	STRING	srv_desc code	
template_name	template_name	STRING	chg_template template_name	
type_of_contact	type_of_contact	INTEGER	toc id	
user1	user1	STRING		
user2	user2	STRING		
user3	user3	STRING		
cab	Cab	UUID		
closure_code	Closure_code	INTEGER	Closure_code.id (http://Closure_code.id)	
cab_approval	Cab_approval	INTEGER	Boolean.id (http://Boolean.id)	
target_times	target_times	BREL	tgt_time_mapped_chg	

Attribute	DB Field	Data Type	SREL References	Flags
target_start_last	target_start_last	DATE		
target_hold_last	target_hold_last	DATE		
target_hold_count	target_hold_count	INTEGER		
target_resolved_last	target_resolved_last	DATE		
target_resolved_count	target_resolved_count	INTEGER		
target_closed_last	target_closed_last	DATE		
target_closed_count	target_closed_count	INTEGER		
close_date_prev	close_date_prev	LOCAL DATE		
resolve_date_prev	resolve_date_prev	LOCAL DATE		
target_hold_count_prev	target_hold_count_prev	LOCAL INTEGER		
target_resolved_count_prev	target_resolved_count_prev	LOCAL INTEGER		
target_closed_count_prev	target_closed_count_prev	LOCAL INTEGER		

chg_tpl Object

The object details are as follows:

1. Associated Table: Change_Template
2. Factories: default
3. REL_ATTR: template_name
4. Common Name: template_name
5. Function Group: change_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
quick_tmpl_type	quick_tmpl_type	INTEGER	quick_tpl_types enum	REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
template	template	INTEGER	chg id	
template_class	template_class	STRING		
template_name	template_name	STRING		UNIQUE REQUIRED S_KEY

chg_trans Object

The object details are as follows:

1. Associated Tables: chg_trans
2. Factories: default
3. REL_ATTR: id
4. Common Name: condition_error
5. Function Group: change_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
status	status	STRING	crs	Specifies the current ticket status.
new_status	new status	STRING	crs	Specifies the new ticket status.
is default		INTEGER		Default transition that appears when the Status field is empty. On new default: 0
must_comment		INTEGER		Comment required when using a transition. On new default: 0
delete_flag	del		actbool	Required. On new default: 0
condition			macro	Site condition macro to approve transition.
condition_error		STRING		Error message for site condition.
description		STRING		Description of this transition.
last_mod_by			cnt	On new default user; on CI set user
last_mod_dt		DATE		On CI set user now

chgalg Object

The object details are as follows:

1. Associated Table: Change_Act_Log

2. Factories: default
3. REL_ATTR: id
4. Common Name: description
5. Function Group: change_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Description	description	STRING		
action_desc	action_desc	STRING		
analyst	analyst	UUID	ca_contact uuid	
change_id	change_id	INTEGER	chg id	
id	id	INTEGER		UNIQUE REQUIRED KEY
internal	internal	INTEGER		
knowledge_session	knowledge_session	STRING		
knowledge_tool	knowledge_tool	STRING		
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
system_time	system_time	LOCAL_TIME		
time_spent	time_spent	DURATION		
time_stamp	time_stamp	LOCAL_TIME		
type	type	STRING	act_type code	

chgcat Object

The object details are as follows:

1. Associated Table: Change_Category
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
assignee	assignee	UUID		

Attribute	DB Field	Data Type	SREL References	Flags
auto_assign	auto_assign	INTEGER		
cab	cab	UUID		
cawf_defid	cawf_defid	STRING		
chgtype	chgtype	SREL	chgtype.id (http://chgtype.id)	
children_ok	children_ok	INTEGER		REQUIRED
code	code	STRING		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
group	group_id	UUID		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
modified_date	last_mod_dt	LOCAL_ TIME		
organization	organization	UUID	ca_organization uuid	
owning_ contract	owning_ contract	INTEGER	svc_contract id	
persistent_id	persid	STRING		
risk_survey	risk_survey	SREL	risk_svy_tpl	
schedule	schedule	INTEGER		
ss_sym		STRING		
ss_include		INTEGER	bool	REQUIRED On new default: 0
service_type	service_type	STRING	srv_desc code	
survey	survey	INTEGER	survey_tpl id	
sym	sym	STRING 1000		REQUIRED S_KEY

chgcnf chg Object

The object details are as follows:

1. Associated Table: usp_conflict_chg
2. Factories: default
3. REL_ATTR: code
4. Common Name: last_mod_dt
5. Function Group: chg_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE KEY
last_mod_by	last_mod_by	UUID	ca_contact	User who last updated this.
last_mod_dt	last_mod_dt	LOCAL_TIME		timestamp of last update to this record.
change	change	INTEGER	chg	Pointer to change order involved in conflict.
conflict_change	conflict_change	INTEGER	chg	Pointer to change order involved in conflict.
is_cause	is_cause	INTEGER		Change in change column caused conflict.

chgcnf Object

The object details are as follows:

1. Associated Table: usp_conflict, usp_conflict_status, usp_conflict_type, usp_conflict_chg
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. Function Group: change_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	delete_flag	INTEGER	actbool enum	**0** -- Active **1** -- Inactive
comments	comments	STRING		Reference to comment information.
conflict_begin	conflict_begin	LOCAL_TIME		Start of time period of the conflict.
source_change	source_change	INTEGER	chg	Pointer to change order involved in conflict.
conflict_change	conflict_change	INTEGER	chg	Pointer to change order involved in conflict.
		UUID		Pointer to Configuration Item involved in conflict.

Attribute	DB Field	Data Type	SREL References	Flags
conflict_ci	conflict_ci		ca_owned_resource	
conflict_end	conflict_end	LOCAL_TIME		End of time period of the conflict.
conflict_status	conflict_status	STRING	chgcnf_status	Pointer to usp_conflict_status that indicates the status of this conflict. For example: Resolved, Unresolved, Researching.
conflict_type	conflict_type	STRING	chgcnf_type	Pointer to usp_conflict_type that classifies the type of conflict represented by this record. For example: Schedule Collision.
creation_dt	creation_dt	LOCAL_TIME		Date conflict was last detected.
id	id	INTEGER		UNIQUE KEY
is_resolved	is_resolved	INTEGER		Flag that indicates whether this conflict should be considered resolved. The entry in usp_conflict_status pointed to by conflict_status has an is_resolved flag that is reflected in this column.
last_mod_dt	last_mod_dt	LOCAL_TIME		Last modified timestamp
last_mod_by	last_mod_by	UUID	ca_contact	Last modified by
persistent_id	persid	STRING		Persistent ID.
suppress_log		INTEGER		LOCAL
tenant	tenant	UUID	ca_contact	Reference to Tenant information.

chgcnf status Object

The object details are as follows:

1. Associated Table: usp_conflict_status
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: reference

6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
code	code	STRING		
delete_flag	delete_flag	INTEGER		Logical database delete status.
description	description	STRING		Textual description of the meaning of the status.
id	id	INTEGER		UNIQUE KEY
is_resolved	is_resolved	INTEGER		Used in stored queries to distinguish Resolved and Unresolved conflicts.
last_mod_by	last_mod_by	UUID	ca_contact	User who last updated this
last_mod_dt	last_mod_dt	LOCAL_TIME		Indicates the timestamp of last update to this record.
sym	sym	STRING		Text value displayed to the user.

chgcnf type Object

The object details are as follows:

1. Associated Table: usp_conflict_type
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: change_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
code	code	STRING	actbool	
delete_flag	delete_flag	INTEGER		Logical database delete status.
description	description	STRING		Textual description of the meaning of the status.
icon	icon	STRING		
id	id	INTEGER		UNIQUE KEY
last_mod_by	last_mod_by	UUID	ca_contact	User who last updated this

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_dt	last_mod_dt	LOCAL_TIME		Indicates the timestamp of last update to this record.
sym	sym	STRING		Text value displayed to the user.

chgstat Object

The object details are as follows:

1. Associated Table: Change_Status
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: change_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
active	active	INTEGER		
code	code	STRING		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
hold	hold	INTEGER		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
modified_date	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
resolved	resolved	INTEGER		
sym	sym	STRING		REQUIRED

BSVC--chgtype Object

The object details are as follows:

1. Associated Table: usp_change_type
2. REL_ATTR: id
3. Common Name: sym
4. Function Group: change_reference

5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
producer_id		LOCAL_STRING 20		
persistent_id	persid	STRING 30		
delete_flag	del	SREL	actbool.enum	REQUIRED
sym	sym	STRING 60		REQUIRED
description	description	STRING 240		
modified_date	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id (http://cnt.id)	

Configuration Item

This article contains the following topics:

CI_ACTIONS Object

The object details are as follows:

1. Associated Table: CI_ACTIONS
2. Factories: default
3. REL_ATTR: id
4. Common Name: ACTION_TITLE
5. Function Group: reference

6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Task Order	ACTION_ORDER	INTEGER		
Task Title	ACTION_TITLE	STRING		
Contact ID	ANALYST_ID	UUID	ca_contact uuid	
Group ID	GROUP_ID	UUID	ca_contact uuid	
id	ID	INTEGER		REQUIRED KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Predefined	PREDEFINED	INTEGER		
Current Status ID	STATUS_CURRENT_ID	INTEGER	CI_STATUSES id	
Unpublish Task	UNPUBLISH	INTEGER		
Unretire Task	UNRETIRE	INTEGER		
Workflow Template ID	WF_TEMPLATE_ID	INTEGER	CI_WF_TEMPLATES id	

CI_ACTIONS_ALTERNATE Object

The object details are as follows:

1. Associated Table: CI_ACTIONS_ALTERNATE
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Task ID	ACTION_ID	INTEGER	CI_ACTIONS id	
Contact ID	CONTACT_ID	UUID	ca_contact uuid	
Contact Type	CONTACT_TYPE	INTEGER		
id	ID	INTEGER		REQUIRED KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		

CI_BOOKMARKS Object

The object details are as follows:

1. Associated Table: CI_BOOKMARKS
2. Factories: default

3. REL_ATTR: id
4. Common Name: BOOKMARK_TITLE
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Bookmark Title	BOOKMARK_TITLE	STRING		
Document ID	DOCUMENT_ID	INTEGER	SKELETONS id	
id	ID	INTEGER		REQUIRED KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Contact ID	USER_ID	UUID	ca_contact uuid	

CI_DOC_LINKS Object

The object details are as follows:

1. Associated Table: CI_DOC_LINKS
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
DOC_ID1	DOC_ID1	INTEGER	SKELETONS id	
DOC_ID2	DOC_ID2	INTEGER	SKELETONS id	
SUPPRESS_OEVENTS	SUPPRESS_OEVENTS	INTEGER		
parent_child	parent_child	INTEGER		
id	ID	INTEGER		REQUIRED KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
last_mod_by	last_mod_by	UUID	ca_contact	Specifies the UUID of the contact who last modified this record.
tenant	tenant	UUID	ca_tenant	Specifies the UUID of the tenant.

CI_DOC_TEMPLATES Object

The object details are as follows:

1. Associated Table: CI_DOC_TEMPLATES
2. Factories: default
3. REL_ATTR: id
4. Common Name: TEMPLATE_NAME
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		REQUIRED KEY
Default Template Flag	IS_DEFAULT	INTEGER		
Predefined Flag	IS_PREDEFINED	INTEGER		
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Template HTML	PAGE_HTML	STRING		
Template Name	TEMPLATE_NAME	STRING		

CI_DOC_TYPES Object

The object details are as follows:

1. Associated Table: CI_DOC_TYPES
2. Factories: default
3. REL_ATTR: id
4. Common Name: DOC_TYPE_TXT
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Document Type	DOC_TYPE_TXT	STRING		
id	ID	INTEGER		KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		

ci_managed_attribute Object

The object details are as follows:

1. Associated Table: ci_managed_attribute
2. Factories: default
3. REL_ATTR: id
4. Common Name: attribute_label
5. Function Group: ci
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		KEY
producer_id		LOCAL STRING 20		
persistent_id		LOCAL STRING 60		
attribute_name	attribute_name	STRING 128		Required
attribute_label	attribute_label	STRING 50		Required
description	description	STRING 255		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id (http://cnt.id)	
delete_flag	del	SREL	actbool.enum	
initial_status	initial_status	SREL	ci_planned_change_status.sym	
case_sensitive	case_sensitive	SREL	bool.enum	
attribute_type	attribute_type	INTEGER		
attribute_length	attribute_length	INTEGER		
srel_factory	srel_factory	STRING 26		
srel_rel_attr	srel_rel_attr	STRING 26		
srel_common_name_attr	srel_common_name_attr	STRING 26		
srel_show_dropdown	srel_show_dropdown	SREL	bool.enum	
mdr_name	N/A	LOCAL STRING		
mdr_class	N/A	LOCAL STRING		

ci_managed_chgstat Object

The object details are as follows:

1. Associated Table: ci_verification_policy_act

2. Factories: default
3. REL_ATTR: code
4. Common Name: persistent_id
5. Function Group: ci
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		KEY
producer_id		LOCAL STRING 20		
persistent_id		LOCAL STRING 60		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id (http://cnt.id)	
delete_flag	del	SREL	actbool.enum	Required
code				Required
can_edit_criteria	can_edit_criteria	SREL	bool.enum	Required
verification_active	verification_active	SREL	bool.enum	Required
is_implementation	is_implementation	SREL	bool.enum	Required
autopromote_chg	autopromote_chg	SREL	bool.enum	Required
show_override_buttons	show_override_buttons	SREL	bool.enum	Required
mdr_name	N/A	LOCAL STRING		
mdr_class	N/A	LOCAL STRING		

ci_planned_change Object

The object details are as follows:

1. Associated Table: ci_planned_change
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: persistent_id
5. Function Group: ci
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		KEY
producer_id		LOCAL STRING 20		

Attribute	DB Field	Data Type	SREL References	Flags
persistent_id		LOCAL STRING 60		
attribute_name	attribute_name	SREL	ci_managed_attribute.attribute_name	Required
attribute_value_original	attribute_value_original	STRING 255		
attribute_value_planned	attribute_value_planned	STRING 255		
attribute_value_discovered	attribute_value_discovered	STRING 255		
chg	chg	SREL	chg.id (http://chg.id)	Required
ci	ci	SREL	nr.id (http://nr.id)	
delete_flag	del	SREL	actbool.enum	
description	description	STRING 255		
status	status	SREL	ci_planned_change_status.sym	
incident	incident	in. persistent_id		
last_verification_policy	last_verification_policy	SREL	ci_verification_policy_id	
ci_twa_ci	ci_twa_ci	SREL	ci_twa_ci.id (http://ci_twa_ci.id)	
ci_twa_relation	ci_twa_relation	SREL		
verification_msg	verification_msg	STRING 255		
attribute_value_internal	attribute_value_internal	STRING 255		
attribute_value_disc_internal	attribute_value_disc_internal	STRING 255		
attribute_value_orig_internal	attribute_value_orig_internal	STRING 255		
mdr_name	N/A	LOCAL STRING		
mdr_class	N/A	LOCAL STRING		
attribute_value_planned_sp	N/A	LOCAL SREL	cnt.id (http://cnt.id)	
attribute_value_planned_nonsp	N/A	LOCAL SREL	org.id (http://org.id)	
allow_update	N/A	LOCAL INTEGER		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id (http://cnt.id)	

ci_planned_change_status Object

The object details are as follows:

1. Associated Table: ci_planned_change_status
2. Factories: default
3. REL_ATTR: sym
4. Common Name: name
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		KEY
producer_id		LOCAL STRING 20		
persistent_id		LOCAL STRING 60		
name	name	STRING 128		
sym	sym	STRING 10		Required
description	description	STRING 255		Required
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id (http://cnt.id)	
delete_flag	del	SREL	actbool.enum	
isinitial	isinitial	INTEGER	bool.enum	
isfinal	isfinal	INTEGER	bool.enum	
isselectable	isselectable	INTEGER	bool.enum	

CI_PRIORITIES Object

The object details are as follows:

1. Associated Table: CI_PRIORITIES
2. Factories: default
3. REL_ATTR: id
4. Common Name: PRIORITY
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Workflow Priority	PRIORITY	STRING		

CI_STATUSES Object

The object details are as follows:

1. Associated Table: CI_STATUSES
2. Factories: default
3. REL_ATTR: id
4. Common Name: STATUS
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Predefined Flag	PREDEFINED	INTEGER		
Status Name	STATUS	STRING		
Status Description	STATUS_DESCRIPTION	STRING		
Status Order	STATUS_ORDER	INTEGER		

ci_verification_policy Object

The object details are as follows:

1. Associated Table: ci_verification_policy
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: ci
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		KEY

Attribute	DB Field	Data Type	SREL References	Flags
producer_id		LOCAL STRING 20		
persistent_id		LOCAL STRING 60		
attribute_name	attribute_name	STRING 128		Required
ci_name_pattern	ci_name_pattern	STRING 255		
class_pattern	class_pattern	STRING 255		
delete_flag	del	SREL	actbool.enum	
description	description	STRING 255		
mdr_name_pattern	mdr_name_pattern	STRING 255		
mdr_class_pattern	mdr_class_pattern	STRING 255		
rolename_pattern	rolename_pattern	STRING 255		Required
priority	priority	SREL	pri.enum	
sequence	sequence	INTEGER		Required
service_type	service_type	SREL	no_contract_sdsc.code	
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id (http://cnt.id)	
location_pattern	location_pattern	STRING 255		
isrogue_insert	isrogue_insert	SREL	bool.enum	Required
isvariance	isvariance	SREL	bool.enum	Required
isrogue_update	isrogue_update	SREL	bool.enum	Required
isnotverifiable	isnotverifiable	SREL	bool.enum	Required
action	action	SREL	ci_verification_policy_act.sym	Required
write_twa	write_twa	SREL	ci_verification_twa_act.id (http://ci_verification_twa_act.id)	Required
write_incident	write_incident	SREL	bool.enum	Required
incident_template	incident_template	SREL	cr_tpl.template_name	

Attribute	DB Field	Data Type	SREL References	Flags
autoclose_incident	autoclose_incident	SREL	bool.enum	Required
log_only_mode	log_only_mode	SREL	bool.enum	Required
start_date	start_date	DATE		
end_date	end_date	DATE		
current_date	N/A	LOCAL DATE		
mdr_name	N/A	LOCAL STRING		
mdr_class	N/A	LOCAL STRING		

ci_verification_policy_act Object

The object details are as follows:

1. Associated Table: ci_verification_policy_act
2. Factories: default
3. REL_ATTR: sym
4. Common Name: name
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		KEY
producer_id		LOCAL STRING 20		
persistent_id		LOCAL STRING 60		
description	description	STRING 255		
name	name	STRING 50		Required
sym	sym	STRING 30		Required
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id (http://cnt.id)	

ci_verification_twa_act Object

The object details are as follows:

1. Associated Table: ci_verification_twa_act
2. Factories: default

3. REL_ATTR: id
4. Common Name: name
5. Function Group: ci
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		KEY
producer_id		LOCAL STRING 20		
persistent_id		LOCAL STRING 60		
description	description	STRING 255		
name	name	STRING 50		Required
sym	sym	STRING 32		Required
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id (http://cnt.id)	

CI_WF_TEMPLATES Object

The object details are as follows:

1. Associated Table: CI_WF_TEMPLATES
2. Factories: default
3. REL_ATTR: id
4. Common Name: WF_NAME
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		KEY
Default Flag	IS_DEFAULT	INTEGER		
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Workflow Template Description	WF_DESCRIPTION	STRING		
Workflow Template Name	WF_NAME	STRING		

EBR

This article contains the following topics:

EBR_ACRONYMS Object

The object details are as follows:

1. Associated Table: EBR_ACRONYMS
2. Factories: default
3. REL_ATTR: id
4. Common Name: ACRONYM
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Acronym	ACRONYM	STRING		
id	ID	INTEGER		REQUIRED KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		

EBR_FULLTEXT Object

The object details are as follows:

1. Associated Table: EBR_FULLTEXT
2. Factories: default
3. REL_ATTR: id
4. Common Name: FULL_WORD

5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
DOC_TYPE	DOC_TYPE	INTEGER		
ENTITY_ID	ENTITY_ID	INTEGER		
FULL_WORD	FULL_WORD	STRING		
FULL_WORD_REVERSE	FULL_WORD_ REVERSE	STRING		
id	ID	INTEGER		REQUIRED KEY
PERMISSION_ INDEX_ID	PERMISSION_ INDEX_ID	INTEGER		
PRODUCT	PRODUCT	STRING		
SHORT_WORD	SHORT_WORD	STRING		
TABLE_ID	TABLE_ID	INTEGER		
WORD_COUNT	WORD_COUNT	INTEGER		
WORD_COUNT_PROBLEM	WORD_COUNT_ PROBLEM	INTEGER		
WORD_COUNT_RESOLUTION	WORD_COUNT_ RESOLUTION	INTEGER		
WORD_COUNT_SUMMARY	WORD_COUNT_ SUMMARY	INTEGER		
WORD_COUNT_TITLE	WORD_COUNT_ TITLE	INTEGER		
WORD_IDF	WORD_IDF	INTEGER		
WORD_ORDER	WORD_ORDER	INTEGER		
WORD_TYPE	WORD_TYPE	INTEGER		

EBR_FULLTEXT_ADM Object

The object details are as follows:

1. Associated Table: EBR_FULLTEXT_ADM
2. Factories: default
3. REL_ATTR: id
4. Common Name: FULL_WORD
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
DOC_TYPE	DOC_TYPE	INTEGER		

ENTITY_ID	ENTITY_ID	INTEGER	
FULL_WORD	FULL_WORD	STRING	
FULL_WORD_REVERSE	FULL_WORD_ REVERSE	STRING	
id	ID	INTEGER	REQUIRED KEY
PERMISSION_ INDEX_ID	PERMISSION_ INDEX_ID	INTEGER	
PRODUCT	PRODUCT	STRING	
SHORT_WORD	SHORT_WORD	STRING	
TABLE_ID	TABLE_ID	INTEGER	
WORD_COUNT	WORD_COUNT	INTEGER	
WORD_COUNT_PROBLEM	WORD_COUNT_ PROBLEM	INTEGER	
WORD_COUNT_RESOLUTION	WORD_COUNT_ RESOLUTION	INTEGER	
WORD_COUNT_SUMMARY	WORD_COUNT_ SUMMARY	INTEGER	
WORD_COUNT_TITLE	WORD_COUNT_ TITLE	INTEGER	
WORD_IDF	WORD_IDF	INTEGER	
WORD_ORDER	WORD_ORDER	INTEGER	
WORD_TYPE	WORD_TYPE	INTEGER	

EBR_FULLTEXT_SD Object

The object details are as follows:

1. Associated Table: EBR_FULLTEXT_SD
2. Factories: default
3. REL_ATTR: id
4. Common Name: FULL_WORD
5. Function Group:

Attribute	DB Field	Data Type	SREL References	Flags
DOC_TYPE	DOC_TYPE	INTEGER		
ENTITY_ID	ENTITY_ID	INTEGER		
FULL_WORD	FULL_WORD	STRING		
FULL_WORD_ REVERSE	FULL_WORD_ REVERSE	STRING		
id	ID	INTEGER		REQUIRED KEY

Attribute	DB Field	Data Type	SREL References	Flags
PERMISSION_ INDEX_ID	PERMISSION_INDEX_ID	INTEGER		
PRODUCT	PRODUCT	STRING		
SHORT_WORD	SHORT_ WORD	STRING		
TABLE_ID	TABLE_ID	INTEGER		
WORD_COUNT	WORD_ COUNT	INTEGER		
WORD_COUNT_PROBLEM	WORD_ COUNT_ PROBLEM	INTEGER		
WORD_COUNT_RESOLUTIO N	WORD_COUNT_ RESOLUTION	INTEGER		
WORD_COUNT_SUMMARY	WORD_COUNT_ SUMMARY	INTEGER		
WORD_COUNT_TITLE	WORD_COUNT_ TITLE	INTEGER		
WORD_IDF	WORD_IDF	INTEGER		
WORD_ORDER	WORD_ORDER	INTEGER		
WORD_TYPE	WORD_TYPE	INTEGER		

EBR_FULLTEXT_SD_ADM Object

The object details are as follows:

1. Associated Table: EBR_FULLTEXT_SD_ADM
2. Factories: default
3. REL_ATTR: id
4. Common Name: FULL_WORD
5. Function Group:

Attribute	DB Field	Data Type	SREL References	Flags
DOC_TYPE	DOC_TYPE	INTEGER		
ENTITY_ID	ENTITY_ID	INTEGER		
FULL_WORD	FULL_WORD	STRING		
FULL_WORD_ REVERSE	FULL_WORD_ REVERSE	STRING		
id	ID	INTEGER		REQUIRED KEY
PERMISSION_ INDEX_ID	PERMISSION_ INDEX_ID	INTEGER		
PRODUCT	PRODUCT	STRING		
SHORT_WORD	SHORT_WORD	STRING		
TABLE_ID	TABLE_ID	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
WORD_COUNT	WORD_COUNT	INTEGER		
WORD_COUNT_PROBLEM	WORD_COUNT_PROBLEM	INTEGER		
WORD_COUNT_RESOLUTION	WORD_COUNT_RESOLUTION	INTEGER		
WORD_COUNT_SUMMARY	WORD_COUNT_SUMMARY	INTEGER		
WORD_COUNT_TITLE	WORD_COUNT_ TITLE	INTEGER		
WORD_IDF	WORD_IDF	INTEGER		
WORD_ORDER	WORD_ORDER	INTEGER		
WORD_TYPE	WORD_TYPE	INTEGER		

EBR_INDEXING_QUEUE Object

The object details are as follows:

1. Associated Table: EBR_INDEXING_QUEUE
2. Factories: default
3. REL_ATTR: id
4. Common Name: OBJ_PERSID
5. Function Group:

Attribute	DB Field	Data Type	SREL References	Flags
ACTION	ACTION	INTEGER		
ACTION_DATE	ACTION_DATE	DATE		
id	ID	INTEGER		REQUIRED KEY
INDEXED	INDEXED	INTEGER		
OBJ_PERSID	OBJ_PERSID	STRING		
PRIORITY	PRIORITY	INTEGER		
TEXT	TEXT	STRING		

EBR_KEYWORDS Object

The object details are as follows:

1. Associated Table: EBR_KEYWORDS
2. Factories: default
3. REL_ATTR: id

4. Common Name: FULL_WORD
5. Function Group:

Attribute	DB Field	Data Type	SREL References	Flags
ENTITY_ID	ENTITY_ID	INTEGER		
EXT_TABLE_ID	EXT_TABLE_ID	INTEGER		
FULL_WORD	FULL_WORD	STRING		
id	ID	INTEGER		REQUIRED KEY

EBR_LOG Object

The object details are as follows:

1. Associated Table: EBR_LOG
2. Factories: default
3. REL_ATTR: id
4. Common Name: SEARCH_TEXT
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
ASKED_DATE	ASKED_DATE	LOCAL_TIME		
BEST_IDS	BEST_IDS	STRING		
EXTERNAL_ID	EXTERNAL_ID	STRING		
FILTER_DATA	FILTER_DATA	STRING		
FUZZINESS	FUZZINESS	INTEGER		
id	ID	INTEGER		KEY
KEYWORDS	KEYWORDS	STRING		
MATCH_TYPE	MATCH_TYPE	INTEGER		
METHOD_ PERFORMANCE	METHOD_ PERFORMANCE	INTEGER		
METHOD_TYPE	METHOD_TYPE	INTEGER		
NUM_MATCHES	NUM_MATCHES	INTEGER		
ORDER_DIRECTION	ORDER_DIRECTION	INTEGER		
PRIMARY_ORDER	PRIMARY_ORDER	STRING		
ROWS_FOUND	ROWS_FOUND	INTEGER		
ROWS_TO_FETCH	ROWS_TO_FETCH	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
SEARCH_IN	SEARCH_IN	INTEGER		
SEARCH_QUALITY	SEARCH_QUALITY	INTEGER		
SEARCH_TEXT	SEARCH_TEXT	STRING		
SEARCH_TYPE	SEARCH_TYPE	INTEGER		
SECONDARY_ORDER	SECONDARY_ORDER	INTEGER		
SESSION_ID	SESSION_ID	INTEGER		
SQL_TEXT	SQL_TEXT	STRING		
TOP_MATCH_ID	TOP_MATCH_ID	INTEGER		
UNIQUE_WORD_ COUNT	UNIQUE_WORD_ COUNT	INTEGER		
USER_ID	USER_ID	STRING		
WORD_COUNT	WORD_COUNT	INTEGER		

EBR_METRICS Object

The object details are as follows:

1. Associated Table: EBR_METRICS
2. Factories: default
3. REL_ATTR: id
4. Common Name: METRIC
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Comments	COMMENTS	STRING		
id	ID	INTEGER		REQUIRED KEY
Metric	METRIC	STRING		
Weight	WEIGHT	REAL		

EBR_NOISE_WORDS Object

The object details are as follows:

1. Associated Table: EBR_NOISE_WORDS
2. Factories: default
3. REL_ATTR: id

4. Common Name: NOISE_WORD
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		REQUIRED KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
Noise Word	NOISE_WORD	STRING		

EBR_PATTERNS Object

The object details are as follows:

1. Associated Table: EBR_PATTERNS
2. Factories: default
3. REL_ATTR: id
4. Common Name: PATTERN_NAME
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		REQUIRED KEY
PATTERN_DEFAULT	PATTERN_DEFAULT	STRING		
PATTERN_NAME	PATTERN_NAME	STRING		
PATTERN_VALUE	PATTERN_VALUE	STRING		
PATTERN_VALUE_ADM	PATTERN_VALUE_ADM	STRING		

EBR_PREFIXES Object

The object details are as follows:

1. Associated Table: EBR_PREFIXES
2. Factories: default
3. REL_ATTR: id
4. Common Name: PREFIX

5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		REQUIRED KEY
Prefix	PREFIX	STRING		

EBR_PROPERTIES Object

The object details are as follows:

1. Associated Table: EBR_PROPERTIES
2. Factories: default
3. REL_ATTR: id
4. Common Name: PROPERTY_NAME
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		REQUIRED KEY
PROPERTY_ADMIN	PROPERTY_ADMIN	INTEGER		
PROPERTY_DEFAULT	PROPERTY_DEFAULT	STRING		
PROPERTY_NAME	PROPERTY_NAME	STRING		S_KEY
PROPERTY_TYPE	PROPERTY_TYPE	STRING		
PROPERTY_VALUE	PROPERTY_VALUE	STRING		
PROPERTY_VALUE_ADM	PROPERTY_VALUE_ADM	STRING		

EBR_SUBSTITS Object

The object details are as follows:

1. Associated Table: EBR_SUBSTITS
2. Factories: default
3. REL_ATTR: id
4. Common Name: SYMBOL1
5. Function Group: reference

6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		REQUIRED KEY
SYMBOL1	SYMBOL1	STRING		
SYMBOL2	SYMBOL2	STRING		

EBR_SUFFIXES Object

The object details are as follows:

1. Associated Table: EBR_SUFFIXES
2. Factories: default
3. REL_ATTR: id
4. Common Name: SUFFIX
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		REQUIRED KEY
Suffix	SUFFIX	STRING		

EBR_SYNONYMS Object

The object details are as follows:

1. Associated Table: EBR_SYNONYMS
2. Factories: default
3. REL_ATTR: id
4. Common Name: KEYWORD1
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		REQUIRED KEY
Keyword 1	KEYWORD1	STRING		
Keyword 2	KEYWORD2	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		

EBR_SYNONYMS_ADM Object

The object details are as follows:

1. Associated Table: EBR_SYNONYMS_ADM
2. Factories: default
3. REL_ATTR: id
4. Common Name: KEYWORD1
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	ID	INTEGER		REQUIRED KEY
Keyword 1	KEYWORD1	STRING		
Keyword 2	KEYWORD2	STRING		
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		

Event Objects

This topic contains the following information:

event_log Object

The object details are as follows:

1. Associated Table: event_log
2. Factories: default
3. REL_ATTR: id
4. Common Name: sd_obj_type
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
event	event	INTEGER	event_type id	
id	id	INTEGER		UNIQUE REQUIRED KEY
kd	kd_id	INTEGER	SKELETONS id	
log_time	log_time	LOCAL_TIME		
millitime	millitime	INTEGER		
numdata1	numdata1	INTEGER		
numdata2	numdata2	INTEGER		
sd_obj_id	sd_obj_id	INTEGER		
sd_obj_type	sd_obj_type	STRING		
session	session	INTEGER	session_log id	
textdata1	textdata1	STRING		
textdata2	textdata2	STRING		

event_type Object

The object details are as follows:

1. Associated Table: event_type
2. Factories: default
3. REL_ATTR: id
4. Common Name: description
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
code	code	STRING		UNIQUE REQUIRED S_KEY
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		

evt Object

The object details are as follows:

1. Associated Table: Events

2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
condition	condition	STRING	splmac persid	
delete_flag	del	INTEGER	actbool enum	REQUIRED
delay_time	delay_time	DURATION		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		
modulo_time	modulo_time	DURATION		REQUIRED
obj_type	obj_type	STRING		
on_done_flag	on_done_flag	INTEGER		REQUIRED
persistent_id	persid	STRING		
sym	sym	STRING		REQUIRED unique S_KEY
urgency	urgency	INTEGER		
user_settime	user_settime	INTEGER		REQUIRED
user_smag	user_smag	STRING		
violate_on_ false	violate_on_ false	INTEGER		
violate_on_ true	violate_on_ true	INTEGER		
work_shift	work_shift	STRING	bpwshft persid	

evtdly Object

The object details are as follows:

1. Associated Table: Event_Delay
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: group_name
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
act_delay	act_delay	DURATION		
cancel_time	cancel_time	LOCAL_TIME		
create_time	create_time	LOCAL_TIME		
delay_type	delay_type	INTEGER	evtdlytp enum	
eff_delay	eff_delay	DURATION		
group_name	group_name	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		
obj_id	obj_id	STRING		REQUIRED S_KEY
persistent_id	persid	STRING		
start_time	start_time	LOCAL_TIME		
start_userid	start_userid	UUID	ca_contact uuid	
status_flag	status_flag	INTEGER		
stop_time	stop_time	LOCAL_TIME		
stop_userid	stop_userid	UUID	ca_contact uuid	
support_lev	support_lev	STRING	srv_desc code	

evtdlytp Object

The object details are as follows:

1. Associated Table: Event_Delay_Type
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
enum	enum	INTEGER		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
description	nx_desc	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY

Global Objects

This article contains the following topics:

g_chg_ext Object

The object details are as follows:

1. Associated Table: Global_Change_Extension
2. Factories: default
3. REL_ATTR: id
4. Common Name: chg_ref_num
5. Function Group: change_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
active	active_flag	INTEGER	actrbool enum	REQUIRED
affected_contact	affected_contact	UUID	ca_contact uuid	REQUIRED
assignee	assignee	UUID	ca_contact uuid	
category	category	STRING		
chg_ref_num	chg_ref_num	STRING		REQUIRED
close_date	close_date	LOCAL_TIME		
global_queue_id	global_queue_id	INTEGER	g_queue_names id	
group	group_id	UUID		
id	id	INTEGER		UNIQUE REQUIRED KEY
impact	impact	INTEGER	impact enum	

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_dt	last_mod_dt	LOCAL_TIME		REQUIRED
open_date	open_date	LOCAL_TIME		REQUIRED
priority	priority	INTEGER	pri enum	REQUIRED
remote_id	remote_id	INTEGER		REQUIRED S_KEY
requestor	requestor	UUID	ca_contact uuid	REQUIRED
status	status	STRING	chgstat code	REQUIRED
summary	summary	STRING		

g_chg_queue Object

The object details are as follows:

1. Associated Table: Global_Change_Queue
2. Factories: default
3. REL_ATTR: id
4. Common Name: chg_ref_num
5. Function Group: change_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
active	active_flag	INTEGER	actrbool enum	REQUIRED
affected_contact	affected_contact	UUID		REQUIRED
assignee	assignee	UUID		
category	category	STRING		
chg_ref_num	chg_ref_num	STRING		REQUIRED
close_date	close_date	LOCAL_TIME		
global_queue_id	global_queue_id	INTEGER	g_queue_names id	
group	group_id	UUID		
id	id	INTEGER		UNIQUE REQUIRED KEY
impact	impact	INTEGER	impact enum	
last_mod_dt	last_mod_dt	LOCAL_TIME		REQUIRED
open_date	open_date	LOCAL_TIME		REQUIRED
priority	priority	INTEGER	pri enum	REQUIRED
remote_id	remote_id	INTEGER		REQUIRED S_KEY
remote_sys_id	remote_sys_id	INTEGER	g_srvr remote_sys_id	REQUIRED S_KEY
requestor	requestor	UUID		REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
status	status	STRING	chgstat code	REQUIRED
summary	summary	STRING		

g_cnt Object

The object details are as follows:

1. Associated Table: Global_Contact
2. Factories: default
3. REL_ATTR: id
4. Common Name: combo_name
5. Function Group: multisite_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
contact_num	contact_num	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
email_address	email_address	STRING		
first_name	first_name	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		
last_name	last_name	STRING		
location	loc_id	UUID		
middle_name	middle_name	STRING		
organization	org_id	UUID		
pri_phone_number	pri_phone_number	STRING		
remote_id	remote_id	UUID		REQUIRED S_KEY
remote_sys_id	remote_sys_id	INTEGER	g_srvr remote_sys_id	REQUIRED S_KEY
userid	userid	STRING		

g_cr_ext Object

The object details are as follows:

1. Associated Table: Global_Request_Extension
2. Factories: default
3. REL_ATTR: id

4. Common Name: ref_num
5. Function Group: call_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
active	active_flag	INTEGER	actrbool enum	REQUIRED
assignee	assignee	UUID	ca_contact uuid	
category	category	STRING		
close_date	close_date	LOCAL_TIME		
customer	customer	UUID	ca_contact uuid	REQUIRED
global_queue_ id	global_queue_ id	INTEGER	g_queue_names id	
group	group_id	UUID		
id	id	INTEGER		UNIQUE REQUIRED KEY
impact	impact	INTEGER	impact enum	
last_mod_dt	last_mod_dt	LOCAL_TIME		REQUIRED
open_date	open_date	LOCAL_TIME		REQUIRED
priority	priority	INTEGER	pri enum	REQUIRED
ref_num	ref_num	STRING		REQUIRED
remote_id	remote_id	INTEGER		REQUIRED S_KEY
status	status	STRING	cr_stat code	REQUIRED
summary	summary	STRING		
type	type	STRING	crt code	

g_cr_queue Object

The object details are as follows:

1. Associated Table: Global_Request_Queue
2. Factories: default
3. REL_ATTR: id
4. Common Name: ref_num
5. Function Group: call_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
active	active_flag	INTEGER	actrbool enum	REQUIRED
assignee	assignee	UUID		

Attribute	DB Field	Data Type	SREL References	Flags
category	category	STRING		
close_date	close_date	LOCAL_TIME		
customer	customer	UUID		REQUIRED
global_queue_id	global_queue_id	INTEGER	g_queue_names id	
group	group_id	UUID		
id	id	INTEGER		UNIQUE REQUIRED KEY
impact	impact	INTEGER	impact enum	
last_mod_dt	last_mod_dt	LOCAL_TIME		REQUIRED
open_date	open_date	LOCAL_TIME		REQUIRED
priority	priority	INTEGER	pri enum	REQUIRED
ref_num	ref_num	STRING		REQUIRED
remote_id	remote_id	INTEGER		REQUIRED S_KEY
remote_sys_id	remote_sys_id	INTEGER	g_srvr remote_sys_id	REQUIRED S_KEY
status	status	STRING	cr_stat code	REQUIRED
summary	summary	STRING		
type	type	STRING	crt code	

g_iss_ext Object

The object details are as follows:

1. Associated Table: Global_Issue_Extension
2. Factories: default
3. REL_ATTR: id
4. Common Name: ref_num
5. Function Group: issue_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
active	active_flag	INTEGER	actrbool enum	REQUIRED
assignee	assignee	UUID	ca_contact uuid	
category	category	STRING		
close_date	close_date	LOCAL_TIME		
global_queue_ id	global_queue_ id	INTEGER	g_queue_names id	
group	group_id	UUID		
id	id	INTEGER		UNIQUE REQUIRED KEY

Attribute	DB Field	Data Type	SREL References	Flags
impact	impact	INTEGER	impact enum	
last_mod_dt	last_mod_dt	LOCAL_TIME		REQUIRED
open_date	open_date	LOCAL_TIME		REQUIRED
priority	priority	INTEGER	pri enum	REQUIRED
product	product	INTEGER	product id	
ref_num	ref_num	STRING		REQUIRED
remote_id	remote_id	INTEGER		REQUIRED S_KEY
requestor	requestor	UUID	ca_contact uuid	REQUIRED
status	status	STRING	issstat code	REQUIRED
summary	summary	STRING		

g_iss_queue Object

The object details are as follows:

1. Associated Table: Global_Issue_Queue
2. Factories: default
3. REL_ATTR: id
4. Common Name: ref_num
5. Function Group: issue_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
active	active_flag	INTEGER	actrbool enum	REQUIRED
assignee	assignee	UUID		
category	category	STRING		
close_date	close_date	LOCAL_TIME		
global_queue_id	global_queue_id	INTEGER	g_queue_names id	
group	group_id	UUID		
id	id	INTEGER		UNIQUE REQUIRED KEY
impact	impact	INTEGER	impact enum	
last_mod_dt	last_mod_dt	LOCAL_TIME		REQUIRED
open_date	open_date	LOCAL_TIME		REQUIRED
priority	priority	INTEGER	pri enum	REQUIRED
product	product	INTEGER		
ref_num	ref_num	STRING		REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
remote_id	remote_id	INTEGER		REQUIRED S_KEY
remote_sys_id	remote_sys_id	INTEGER	g_srvr remote_sys_id	REQUIRED S_KEY
requestor	requestor	UUID		REQUIRED
status	status	STRING	isstat code	REQUIRED
summary	summary	STRING		

g_loc Object

The object details are as follows:

1. Associated Table: Global_Location
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
del	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		
loc_name	loc_name	STRING		
remote_id	remote_id	UUID		REQUIRED S_KEY
remote_sys_id	remote_sys_id	INTEGER	g_srvr remote_sys_id	REQUIRED S_KEY

g_org Object

The object details are as follows:

1. Associated Table: Global_Organization
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: inventory
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		
name	org_name	STRING		
remote_id	remote_id	UUID		REQUIRED S_KEY
remote_sys_id	remote_sys_id	INTEGER	g_srvr remote_sys_id	REQUIRED S_KEY

g_prod Object

The object details are as follows:

1. Associated Table: Global_Product
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: multisite_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		
remote_id	remote_id	INTEGER		REQUIRED S_KEY
remote_sys_id	remote_sys_id	INTEGER	g_srvr remote_sys_id	REQUIRED S_KEY
sym	sym	STRING		

g_qname Object

The object details are as follows:

1. Associated Table: Global_Queue_Names
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: multisite_reference

6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
sym	sym	STRING		UNIQUE REQUIRED

g_tblmap Object

The object details are as follows:

1. Associated Table: Global_Table_Map
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
map_definition	map_definition	STRING		REQUIRED
sym	sym	STRING		UNIQUE REQUIRED

g_srvrs Object

The object details are as follows:

1. Associated Table: Global_Servers
2. Factories: default
3. REL_ATTR: remote_sys_id
4. Common Name: sym

5. Function Group: multisite_admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
chg_prefix	chg_prefix	STRING		
cr_prefix	cr_prefix	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
global_name	global_name	STRING		UNIQUE REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
is_master	is_master	INTEGER	bool_tab enum	
iss_prefix	iss_prefix	STRING		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
remote_sys_id	remote_sys_id	INTEGER		UNIQUE REQUIRED
slump_addr	slump_addr	STRING		
sym	sym	STRING		UNIQUE REQUIRED
web_protocol	web_protocol	STRING		
web_server	web_server	STRING		
web_server_port	web_server_port	STRING		
web_url	web_url	STRING		

g_tblrule Object

The object details are as follows:

1. Associated Table: Global_Table_Rule
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
addl_query	addl_query	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY

last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
last_sync_dt	last_sync_dt	LOCAL_TIME		
reoccur_interv	reoccur_interv	DURATION		
sched	sched	STRING	bpwshft persid	
sym	sym	STRING		UNIQUE REQUIRED S_KEY
table_map	table_map	INTEGER	g_tbl_map id	

Issue Objects

This article contains the following topics:

iss Object

The object details are as follows:

1. Associated Table: Issue
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: ref_num
5. Function Group: issue_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
actions	actions	STRING		
active_flag	active_flag	INTEGER		REQUIRED
active_prev	LOCAL	SREL	bool.enum	
actual_comp_date	actual_comp_date	LOCAL_TIME		
actual_cost	actual_cost	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
actual_total_time	actual_total_time	DURATION		
affected_contact	affected_contact	UUID	ca_contact uuid	
assignee	assignee	UUID		
assignee_prev	LOCAL	SREL	agt.id	
backout_plan	backout_plan	STRING		
call_back_date	call_back_date	LOCAL_TIME		
call_back_flag	call_back_flag	INTEGER		
category	category	STRING	isscat code	
category_prev	LOCAL	SREL	pcat.persistent_id	
cawf_procid	cawf_procid	STRING		
close_date	close_date	LOCAL_TIME		
created_via	created_via	INTEGER	interface id	
effort	effort	STRING		
est_comp_date	est_comp_date	LOCAL_TIME		
est_cost	est_cost	INTEGER		
est_total_time	est_total_time	DURATION		
external_system_ticket		STRING		
flag1	flag1	INTEGER		
flag2	flag2	INTEGER		
flag3	flag3	INTEGER		
flag4	flag4	INTEGER		
flag5	flag5	INTEGER		
flag6	flag6	INTEGER		
group	group_id	UUID		
group_prev	LOCAL	SREL	grp.id	
id	id	INTEGER		UNIQUE REQUIRED KEY
impact	impact	INTEGER	impact enum	
impact_prev	LOCAL	SREL	imp.enum	
justification	justification	STRING		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
log_agent	log_agent	UUID	ca_contact uuid	REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
macro_predicted_violation	macro_predict_ viol	INTEGER		
need_by	need_by	LOCAL_TIME		
open_date	open_date	LOCAL_TIME		
organization	organization	UUID	ca_organization uuid	
orig_user_admin_org		SREL	org	
orig_user_cost_ center		SREL	cost_cntr	
orig_user_dept		SREL	dept	
orig_user_ organization		SREL	org	
parent	parent	STRING	issue persistent_id	
persistent_id	persid	STRING		
person_contacting	person_contacting	INTEGER	perscon id	
predicted_sla_ violation	predicted_sla_viol	INTEGER		
priority	priority	INTEGER	pri enum	REQUIRED
priority_prev	LOCAL	SREL	pri.enum	
product	product	INTEGER	product id	
ref_num	ref_num	STRING		UNIQUE REQUIRED S_KEY
reporting_method	reporting_method	INTEGER	repmeth id	
requestor	requestor	UUID	ca_contact uuid	REQUIRED
requested_by		UUID	ca_contact	
resolve_date	resolve_date	LOCAL_TIME		
rootcause	rootcause	INTEGER	rootcause id	
service_date	service_date	LOCAL_TIME		
service_num	service_num	STRING		
sla_violation	sla_violation	INTEGER		
start_date	start_date	LOCAL_TIME		
status	status	STRING	issstat code	
status_prev	LOCAL	SREL	crs.code	
string1	string1	STRING		
string2	string2	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
string3	string3	STRING		
string4	string4	STRING		
string5	string5	STRING		
string6	string6	STRING		
summary	summary	STRING		
support_lev	support_lev	STRING	srv_desc code	
template_name	template_name	STRING	iss_template template_name	
type_of_contact	type_of_contact	INTEGER	toc id	
user1	user1	STRING		
user2	user2	STRING		
user3	user3	STRING		
target_times	target_times			
target_start_last	target_start_last	DATE		
target_hold_last	target_hold_last	DATE		
target_hold_count	target_hold_count	INTEGER		
target_resolved_ last	target_resolved_ last	DATE		
target_resolved_ count	target_resolved_ count	INTEGER		
target_closed_last	target_closed_last	DATE		
target_closed_ count	target_closed_ count	INTEGER		
close_date_prev	close_date_prev	LOCAL DATE		
resolve_date_prev	resolve_date_prev	LOCAL DATE		
target_hold_ count_prev	target_hold_ count_prev	LOCAL INTEGER		
target_resolved_ count_prev	target_resolved_ count_prev	LOCAL INTEGER		
target_closed_ count_prev	target_closed_ count_prev	LOCAL INTEGER		

iss_prp Object

The object details are as follows:

1. Associated Table: Issue_Property
2. Factories: default
3. REL_ATTR: id

4. Common Name: label
5. Function Group: issue_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
error_msg	error_msg	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
label	label	STRING		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
owning_iss	owning_iss	STRING	issue persistent_id	REQUIRED
owning_macro	owning_macro	BOP_REF_STR	macro	REQUIRED
persistent_id	persid	STRING		
required	required	INTEGER	bool_tab enum	
sample	sample	STRING		
sequence	sequence	INTEGER		REQUIRED
value_description	value_description	STRING		
validation_rule	validation_rule	BOP_REF_STR	prpval_rule	REQUIRED
validation_type	validation_type	BOP_REF_STR	prpval_type	REQUIRED
value	value	STRING		

iss_tpl Object

The object details are as follows:

1. Associated Table: Iss_Template
2. Factories: default
3. REL_ATTR: template_name
4. Common Name: template_name
5. Function Group: issue_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
quick_tmpl_ type	quick_tmpl_ type	INTEGER	quick_tpl_ types enum	REQUIRED
template	template	STRING	issue persistent_id	
template_class	template_class	STRING		
template_name	template_name	STRING		UNIQUE REQUIRED S_KEY

iss_trans Object

The object details are as follows:

1. Associated Tables: iss_trans
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: issue_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
status	status	STRING	crs	Specifies the current ticket status.
new_status	new status	STRING	crs	Specifies the new ticket status.
is default		INTEGER		Default transition that appears when the Status field is empty. On new default: 0
must_comment		INTEGER		Comment required when using a transition. On new default: 0
delete_flag	del		actbool	Required. On new default: 0
condition			macro	Site condition macro to approve transition.
condition_error		STRING		Error message for site condition.
description		STRING		Description of this transition.
last_mod_by			cnt	On new default user; on CI set user
last_mod_dt		DATE		On CI set user now

iss_wf Object

The object details are as follows:

1. Associated Table: Issue_Workflow_Task
2. Factories: default
3. REL_ATTR: id
4. Common Name: description
5. Function Group: issue_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
actual_duration	actual_duration	DURATION		
asset	asset	UUID	ca_owned_resource uuid	
assignee	assignee	UUID	ca_contact uuid	
completion_date	completion_date	LOCAL_TIME		
cost	cost	INTEGER		
creator	creator	UUID	ca_contact uuid	
date_created	date_created	LOCAL_TIME		
del	del	INTEGER		REQUIRED
done_by	done_by	UUID	ca_contact uuid	
est_completion_date	est_comp_date	LOCAL_TIME		
est_cost	est_cost	INTEGER		
est_duration	est_duration	DURATION		
group	group_id	UUID		
group_task	group_task	INTEGER		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
object_id	object_id	STRING		REQUIRED
object_type	object_type	STRING		REQUIRED
persistent_id	persid	STRING		
sequence	sequence	INTEGER		REQUIRED
start_date	start_date	LOCAL_TIME		
status	status	STRING	tskstat code	

Attribute	DB Field	Data Type	SREL References	Flags
support_lev	support_lev	STRING	srv_desc code	
task	task	STRING	tskty code	REQUIRED
wf_template	wf_template	INTEGER	wftpl id	

issalg Object

The object details are as follows:

1. Associated Table: Issue_Act_Log
2. Factories: default
3. REL_ATTR: id
4. Common Name: description
5. Function Group: issue_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
action_desc	action_desc	STRING		
analyst	analyst	UUID	ca_contact uuid	
id	id	INTEGER		UNIQUE REQUIRED KEY
internal	internal	INTEGER		
issue_id	issue_id	STRING	issue persistent_id	
knowledge_ session	knowledge_ session	STRING		
knowledge_tool	knowledge_tool	STRING		
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
system_time	system_time	LOCAL_TIME		
time_spent	time_spent	DURATION		
time_stamp	time_stamp	LOCAL_TIME		
type	type	STRING	act_type code	

isscat Object

The object details are as follows:

1. Associated Table: Issue_Category
2. Factories: default

3. REL_ATTR: code
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
assignee	assignee	UUID		
auto_assign	auto_assign	INTEGER		
cawf_defid	cawf_defid	STRING		
children_ok	children_ok	INTEGER		REQUIRED
code	code	STRING		UNIQUE REQUIRED S_KEY
del	del	INTEGER		REQUIRED
group_id	group_id	UUID		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
organization	organization	UUID	ca_organization uuid	
owning_contract	owning_contract	INTEGER	svc_contract id	
persistent_id	persid	STRING		
ss_sym		STRING		
ss_include			bool	REQUIRED On new default: 0
schedule	schedule	INTEGER		
service_type	service_type	STRING	srv_desc code	
survey	survey	INTEGER	survey_tpl id	
sym	sym	STRING 1000		REQUIRED S_KEY

issstat Object

The object details are as follows:

1. Associated Table: Issue_Status
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: reference

6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
active	active	INTEGER		
code	code	STRING		UNIQUE REQUIRED S_KEY
del	del	INTEGER		REQUIRED
hold	hold	INTEGER		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
resolved	resolved	INTEGER		
sym	sym	STRING		REQUIRED

Knowledge Documents Object

This topic contains the following information:

KD Object

The object details are as follows:

1. Associated Table: SKELETONS
2. Factories: default
3. REL_ATTR: id
4. Common Name: TITLE
5. Function Group: kd
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
AVG_RATING	AVG_RATING	DOUBLE		
Document State	ACTIVE_STATE	INTEGER		
Document State Date	ACTIVE_STATE_ DATE			

Attribute	DB Field	Data Type	SREL References	Flags
		LOCAL_TIME		
Assignee ID	ASSIGNEE_ID	UUID	ca_contact uuid	
Author ID	AUTHOR_ID	UUID	ca_contact uuid	
FAQ Rating	BU_RESULT	REAL		
Created Via	CREATED_VIA	INTEGER		
Creation Date	CREATION_DATE	LOCAL_TIME		
Task ID	CURRENT_ACTION_ID	INTEGER	CI_ACTIONS id	
Custom 1	CUSTOM1	STRING		
Custom 2	CUSTOM2	STRING		
Custom 3	CUSTOM3	STRING		
Custom 4	CUSTOM4	STRING		
Custom 5	CUSTOM5	STRING		
Custom Num 1	CUSTOM_NUM1	REAL		
Custom Num 2	CUSTOM_NUM2	REAL		
Document Template ID	DOC_TEMPLATE_ ID	INTEGER	CI_DOC_ TEMPLATES id	
Document Type ID	DOC_TYPE_ID	INTEGER	CI_DOC_ TYPES id	
Document Version	DOC_VERSION	STRING		
Expiration Date	EXPIRATION_DATE	LOCAL_TIME		
EXPIRE_ NOTIFICATION_ SENT	EXPIRE_ NOTIFICATION_ SENT	INTEGER		
Decision Tree Root ID	EXT_DOC_ID	INTEGER		
ebr_search_text	ebr_search_text	STRING		
ebr_min_relevance	ebr_min_relevance	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
ebr_fuzziness	ebr_fuzziness	STRING		
ebr_search_type	ebr_search_type	STRING		
ebr_match_type	ebr_match_type	STRING		
ebr_search_in	ebr_search_in	STRING		
ebr_primary_order	ebr_primary_order	STRING		
ebr_secondary_order	ebr_secondary_order	STRING		
ebr_order_direction	ebr_order_direction	STRING		
ebr_custom_filter	ebr_custom_filter	STRING		
ebr_sd_persid	ebr_sd_persid	STRING		
ebr_filter_data	ebr_flter_data	STRING		
ebr_url_text	ebr_url_text	STRING		
ebr_ks_source	ebr_ks_source	STRING		
ebr_kcat_id	ebr_kcat_id	STRING		
ebr_ad_blc	ebr_ad_blc	STRING		
ebr_serial_num	ebr_serial_num	STRING		
ebr_relevance	ebr_relevance	STRING		
ebr_ks_teaser	ebr_ks_teaser	STRING		
ebr_ks_concepts	ebr_ks_concepts	STRING		
FLG_COUNT	FLG_COUNT	QREL		
FULLWORDS	FULLWORDS	STRING		
Hits	HITS	INTEGER		
id	ID			KEY

Attribute	DB Field	Data Type	SREL References	Flags
		INTEGER		
INDEXED	INDEXED	INTEGER		
Inherit Permissions Flag	INHERIT_PERMISSION	INTEGER		
Initiator	INITIATOR	STRING		
Initiator ID	INITIATOR_ID	UUID	ca_contact uuid	
Inherit Permissions from Category ID	KD_PERMISSION_INDEX_ID	INTEGER	O_INDEXES id	
KS_TYPE	KS_TYPE	INTEGER		
Last Accepted Date	LAST_ACCEPTED_DATE	LOCAL_TIME		
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		Indicates the timestamp of when this record was last modified.
Locked By ID	LOCKED_BY_ID	UUID	ca_contact uuid	
Modify Date	MODIFY_DATE	LOCAL_TIME		
Notes	NOTES	STRING		
Owner ID	OWNER_ID	UUID	ca_contact uuid	
Parent Request	PARENT_CR	STRING	call_req persid	
Parent Issue	PARENT_ISS	STRING	issue persistent_id	
persistent_id	persid	STRING		
Primary Category	PRIMARY_INDEX	INTEGER	O_INDEXES id	
Workflow Priority ID	PRIORITY_ID	INTEGER	CI_PRIORITIES id	
Problem	PROBLEM	STRING		
producer_id	producer_id	STRING		
Published Date	PUBLISHED_DATE			

Attribute	DB Field	Data Type	SREL References	Flags
		LOCAL_TIME		
READ_PGROUP	READ_PGROUP	INTEGER	P_GROUPS id	
PGROUP TYPE	PGROUP_TYPE	INTEGER		Indicates if the P Groups is based on Roles or Groups: 1 -- Groups (Default) 2 -- Roles
QA_STATUS	QA_STATUS	SREL	kt_qa_status.id (http://kt_qa_status.id/)	
Resolution Text	RESOLUTION	STRING		
Resolution Length	RESOLUTION_ LENGTH	INTEGER		
Short Resolution	RESOLUTION_ SHORT	STRING		
Review Date	REVIEW_DATE	LOCAL_TIME		
Solution Count	SD_ACCEPTED_ HITS	INTEGER		
Asset ID	SD_ASSET_ID	UUID	ca_owned_ resource uuid	
Impact ID	SD_IMPACT_ID	INTEGER	impact enum	
PRIMARY_KCAT_ CHANGE_ONKCAT_ DELETE	PRIMARY_KCAT_ CHANGE_ONKCAT_ DELETE	INTEGER		
Priority ID	SD_PRIORITY_ID	INTEGER	pri enum	
PROBLEM_SHORT	PROBLEM_SHORT	STRING 255		
Product ID	SD_PRODUCT_ID	INTEGER	product id	
RESOLUTION_ TEXT	RESOLUTION_ TEXT	STRING		
Root Cause ID	SD_ROOTCAUSE_ ID	INTEGER	rootcause id	
Severity ID	SD_SEVERITY_ID	INTEGER	sevrty enum	

Attribute	DB Field	Data Type	SREL References	Flags
Urgency ID	SD_URGENCY_ID	INTEGER	urgncy enum	
USER_SLV_CNT	USER_SLV_CNT	INTEGER		
SHORTWORDS	SHORTWORDS	STRING		
Start Date	START_DATE	LOCAL_TIME		
Status ID	STATUS_ID	INTEGER	CI_STATUSES id	
Subject Expert ID	SUBJECT_EXPERT_ID	UUID	ca_contact uuid	
SUBMIT_ KNOWLEDGE_ GUEST_USER_ NAME	SUBMIT_ KNOWLEDGE_ GUEST_USER_ NAME	STRING		
SUBMIT_ KNOWLEDGE_ GUEST_MAIL	SUBMIT_ KNOWLEDGE_ GUEST_MAIL	STRING		
Summary	SUMMARY	STRING		
ticket_avoided_cnt	ticket_avoided_cnt	INTEGER		
Title	TITLE	STRING		
User Defined ID	USER_DEF_ID	STRING		
Version Comment	VER_COMMENT	STRING		
Version Count	VER_COUNT	INTEGER		
Version Cross Reference ID	VER_CROSS_REF_ ID	INTEGER		
Workflow Template	WF_TEMPLATE	INTEGER	CI_WF_ TEMPLATES id	
WORD_COUNT_ TOTAL	WORD_COUNT_ TOTAL	INTEGER		
WORDCOUNT	WORDCOUNT	INTEGER		
WORDCOUNTS	WORDCOUNTS	STRING		
WORDORDERS	WORDORDERS	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
WORDPLACES	WORDPLACES	STRING		
WORDSPANS	WORDSPANS	STRING		
WRITE_PGROUP	WRITE_PGROUP	INTEGER	P_GROUPS id	

KD_APPROVAL_METHODS Object

The object details are as follows:

REST Operations: CREATE READ UPDATE

Name	Type	Description	
id	Long		
KD	Long	Knowledge Document's SREL	Tenant implying attribute
CI_WF_TEMPLATES	Long	SREL to CI_WF_TEMPLATES	Tenant implying attribute
KD_ACTION	String	On of: Forward, reject, publish, retire and unretire	
ACTION_ID	Long	SREL to ci_actions	
ASSIGNEE	UUID	User assigned the Knowledge Document	

KD_ATTMNT Object

The object details are as follows:

1. Associated Table: KD_ATTMNT
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
ATTMNT_ID	ATTMNT_ID	INTEGER	attmnt id	
DOC_ID	DOC_ID	INTEGER	SKELETONS id	
id	ID	INTEGER		KEY
last_mod_dt	LAST_MOD_DT	LOCAL_TIME		

Relational Information

This topic contains the following information:

lrel_asset_chgnr Object

The object details are as follows:

1. Associated Table: usp_lrel_asset_chgnr
2. Factories: default
3. REL_ATTR: id
4. Common Name:id
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE DELETE

Attribute	DB Field	Data Type	SREL References	Flags
nr	nr	BREL	nr.id	LREL REQUIRED
chg	chg	BREL	chg.id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id	LREL

lrel_asset_issnr Object

The object details are as follows:

1. Associated Table: usp_lrel_asset_issnr
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE DELETE

Attribute	DB Field	Data Type	SREL References	Flags
nr	nr	BREL	nr.id	LREL REQUIRED
iss	iss	BREL	iss.persistent_id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id	LREL

lrel_att_cntlist_macro_ntf Object

The object details are as follows:

1. Associated Table: usp_lrel_att_cntlist_macro_ntf
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
cnt	cnt	BREL	cnt.id	LREL REQUIRED
macro	macro	BREL	macro.persistent_ id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id	LREL

lrel_att_ctplist_macro_ntf Object

The object details are as follows:

1. Associated Table: usp_lrel_att_ctplist_macro_ntf
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
ctp	ctp	BREL	ctp.id	LREL REQUIRED
macro	macro	BREL	macro.persistent_id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id	LREL

lrel_att_ntflist_macro_ntf Object

The object details are as follows:

1. Associated Table: usp_lrel_att_ntflist_macro_ntf
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
ntfl	ntfl	BREL	ntfl.id	LREL REQUIRED
macro	macro	BREL	macro.persistent_id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id	LREL

lrel_attachments_changes Object

The object details are as follows:

1. Associated Table: usp_lrel_attachments_changes
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE DELETE

Attribute	DB Field	Data Type	SREL References	Flags
attmnt	attmnt	BREL	attmnt id	LREL
chg	chg	BREL	chg id	LREL
last_mod_by	last_mod_by	BREL	ca_contact contact_uuid	LREL
last_mod_dt	last_mod_dt	BREL	cnt.id	LREL

lrel_attachments_issues Object

The object details are as follows:

1. Associated Table: usp_lrel_attachments_issues
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE DELETE

Attribute	DB Field	Data Type	SREL References	Flags
attmnt	attmnt	BREL	attmnt.id	LREL REQUIRED
iss	iss	BREL	iss.persistent_id	LREL REQUIRED
login_id		LOCAL STRING(0)		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id	LREL

lrel_attachments_requests Object

The object details are as follows:

1. Associated Table: usp_lrel_attachments_requests
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE DELETE

Attribute	DB Field	Data Type	SREL References	Flags
attmnt	attmnt	BREL	attmnt.id	LREL REQUIRED
cr	cr	BREL	cr.persistent_id	LREL REQUIRED
login_id		LOCAL STRING(0)		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id	LREL

lrel_aty_events Object

The object details are as follows:

1. Associated Table: usp_lrel_aty_events
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Remarks
aty	aty	BREL	aty.code	LREL REQUIRED
evt	evt	BREL	evt.persistent_id	LREL REQUIRED
last_mod_dt	last_mod_dt	LOCAL_TIME		
last_mod_by	last_mod_by	BREL	cnt.id	LREL

lrel_bm_reps_assets Object

The object details are as follows:

1. Associated Table: usp_lrel_bm_reps_assets
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference

Attribute	DB Field	Data Type	SREL References	Flags
bmrep	bmrep	BREL	bmrep.id	LREL REQUIRED
nr	nr	BREL	nr.id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id	LREL

lrel_bm_reps_bmhiers Object

The object details are as follows:

1. Associated Table: usp_lrel_bm_reps_bmhiers
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference

Attribute	DB Field	Data Type	SREL References	Flags
bmrep	bmrep	BREL	bmrep.id (http://bmrep.id)	LREL REQUIRED
bmhier	bmhier	BREL	bmhier.id (http://bmhier.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_cenv_cntref Object

The object details are as follows:

1. Associated Table: usp_lrel_cenv_cntref
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE DELETE

Attribute	DB Field	Data Type	SREL References	Flags
nr	nr	BREL	nr.id (http://nr.id)	LREL REQUIRED
cnt	cnt	BREL	cnt.id (http://cnt.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_dist_cntlist_mgs_ntf Object

The object details are as follows:

1. Associated Table: usp_lrel_dist_cntlist_mgs_ntf
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
cnt	cnt	BREL	cnt.id (http://cnt.id)	LREL REQUIRED
mgs	mgs	BREL	mgs.id (http://mgs.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_dist_ctplist_mgs_ntf Object

The object details are as follows:

1. Associated Table: usp_lrel_dist_cntlist_mgs_ntf
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
ctp	ctp	BREL	ctp.id (http://ctp.id)	LREL REQUIRED
mgs	mgs	BREL	mgs.id (http://mgs.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	

lrel_dist_ntflist_mgs_ntf Object

The object details are as follows:

1. Associated Table: usp_lrel_dist_ntflist_mgs_ntf
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
ntfl	ntfl	BREL	ntfl.id (http://ntfl.id)	LREL REQUIRED
mgs	mgs	BREL	mgs.id (http://mgs.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	

lrel_false_action_act_f Object

The object details are as follows:

1. Associated Table: usp_lrel_false_action_act_f
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
macro	macro	BREL	macro.persistent_id	LREL REQUIRED
evt	evt	BREL	evt.persistent_id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_false_bhv_false Object

The object details are as follows:

1. Associated Table: lrel_false_bhv_false
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
macro	macro	BREL	macro.persistent_id	LREL REQUIRED
bhvtpl	bhvtpl	BREL	bhvtpl.id (http://bhvtpl.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_kwrds_crsolref Object

The object details are as follows:

1. Associated Table: usp_lrel_kwrds_crsolref
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
kwrd	kwrd	BREL	kwrd.id (http://kwrd.id)	LREL REQUIRED
crsol	crsol	BREL	crsol.persistent_id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_notify_list_cntchgntf Object

The object details are as follows:

1. Associated Table: usp_lrel_notify_list_cntchgntf
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE DELETE

Attribute	DB Field	Data Type	SREL References	Flags
cnt	cnt	BREL	cnt.id (http://cnt.id)	LREL REQUIRED
chg	chg	BREL	chg.id (http://chg.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_notify_list_cntissntf Object

The object details are as follows:

1. Associated Table: usp_lrel_notify_list_cntissntf
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE DELETE

Attribute	DB Field	Data Type	SREL References	Flags
cnt	cnt	BREL	cnt.id (http://cnt.id)	LREL REQUIRED
iss	iss	BREL	iss.persistent_id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_notify_list_cntntf Object

The object details are as follows:

1. Associated Table: usp_lrel_notify_list_cntntf
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE DELETE

Attribute	DB Field	Data Type	SREL References	Flags
cnt	cnt	BREL	cnt.id (http://cnt.id)	LREL REQUIRED
cr	cr	BREL	cr.persistent_id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_ntfr_cntlist_att_ntfrlist Object

The object details are as follows:

1. Associated Table: usp_lrel_ntfr_cntlist_att_ntfrlist
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
cnt	cnt	BREL	cnt.id (http://cnt.id)	LREL REQUIRED
ntfr	ntfr	BREL	ntfr.id (http://ntfr.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_ntfr_ctplist_att_ntfrlist Object

The object details are as follows:

1. Associated Table: usp_lrel_ntfr_ctplist_att_ntfrlist
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
ctp	ctp	BREL	ctp.id (http://ctp.id)	LREL REQUIRED
ntfr	ntfr	BREL	ntfr.id (http://ntfr.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_ntfr_macrolist_att_ntfrlist Object

The object details are as follows:

1. Associated Table: usp_lrel_ntfr_macrolist_att_ntfrlist
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
macro	macro	BREL	macro.persistent_id	LREL REQUIRED
ntfr	ntfr	BREL	ntfr.id (http://ntfr.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_ntfr_ntflist_att_ntfrlist Object

The object details are as follows:

1. Associated Table: usp_lrel_ntfr_ntflist_att_ntfrlist
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
macro	macro	BREL	macro.persistent_id	LREL REQUIRED
ntfl	ntfl	BREL	ntfl.id (http://ntfl.id)	LREL REQUIRED
ntfr	ntfr	BREL	ntfr.id (http://ntfr.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_oenv_orgref Object

The object details are as follows:

1. Associated Table: usp_lrel_oenv_orgref
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE DELETE

Attribute	DB Field	Data Type	SREL References	Flags
nr	nr	BREL	nr.id (http://nr.id)	LREL REQUIRED
org	org	BREL	org.id (http://org.id)	LREL REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_status_codes_tsktypes Object

The object details are as follows:

1. Associated Table: usp_lrel_status_codes_tsktypes
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
tskstat	tskstat	BREL	tskstat.code	LREL REQUIRED
tskty	tskty	BREL	tskty.code	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_svc_grps_svc_chgcat Object

The object details are as follows:

1. Associated Table: usp_lrel_svc_grps_svc_chgcat
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
cnt	cnt	BREL	cnt.id (http://cnt.id)	LREL REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
chgcat	chgcat	BREL	chgcat.code	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_svc_grps_svc_isscat Object

The object details are as follows:

1. Associated Table: usp_lrel_svc_grps_svc_isscat
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
cnt	cnt	BREL	cnt.id (http://cnt.id)	LREL REQUIRED
isscat	isscat	BREL	isscat.code	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_svc_grps_svc_pcat Object

The object details are as follows:

1. Associated Table: usp_lrel_svc_grps_svc_pcat
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
cnt	cnt	BREL	cnt.id (http://cnt.id)	LREL REQUIRED
pcat	pcat	BREL	pcat.persistent_id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_svc_grps_svc_wftpl Object

The object details are as follows:

1. Associated Table: usp_lrel_svc_grps_svc_wftpl
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
cnt	cnt	BREL	cnt.id (http://cnt.id)	LREL REQUIRED
wftpl	wftpl	BREL	wftpl.id (http://wftpl.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_svc_locs_svc_chgcat Object

The object details are as follows:

1. Associated Table: usp_lrel_svc_locs_svc_chgcat
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
loc	loc	BREL	loc.id (http://loc.id)	LREL REQUIRED
chgcat	chgcat	BREL	chgcat.code	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_svc_locs_svc_groups Object

The object details are as follows:

1. Associated Table: usp_lrel_svc_locs_svc_groups
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
loc	loc	BREL	loc.id (http://loc.id)	LREL REQUIRED
cnt	cnt	BREL	cnt.id (http://cnt.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_svc_locs_svc_isscat Object

The object details are as follows:

1. Associated Table: usp_lrel_svc_locs_svc_isscat
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference

6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
loc	loc	BREL	loc.id (http://loc.id)	LREL REQUIRED
isscat	isscat	BREL	isscat.code	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_svc_locs_svc_pcat Object

The object details are as follows:

1. Associated Table: usp_lrel_svc_locs_svc_pcat
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
loc	loc	BREL	loc.id (http://loc.id)	LREL REQUIRED
pcat	pcat	BREL	pcat.persistent_id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_svc_schedules_chgcat_svc Object

The object details are as follows:

1. Associated Table: usp_lrel_svc_schedules_chgcat_svc
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: security

6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
wrkshft	wrkshft	BREL	wrkshft.persistent_id	LREL REQUIRED
chgcat	chgcat	BREL	chgcat.code	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_svc_schedules_isscat_svc Object

The object details are as follows:

1. Associated Table: usp_lrel_svc_schedules_isscat_svc
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
isscat	isscat	BREL	isscat code	LREL
wrkshft	wrkshft	BREL	wrkshft.persistent_id	LREL REQUIRED
isscat	isscat	BREL	isscat.code	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_svc_schedules_pcat_svc Object

The object details are as follows:

1. Associated Table: usp_lrel_svc_schedules_pcat_svc
2. Factories: default
3. REL_ATTR: id
4. Common Name:

5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
wrkshft	wrkshft	BREL	wrkshft.persistent_id	LREL REQUIRED
pcat	pcat	BREL	pcat.persistent_id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_true_action_act_t Object

The object details are as follows:

1. Associated Table: usp_lrel_true_action_act_t
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
macro	macro	BREL	macro.persistent_id	LREL REQUIRED
evt	evt	BREL	evt.persistent_id	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

lrel_true_bhv_true Object

The object details are as follows:

1. Associated Table: usp_lrel_true_bhv_true
2. Factories: default
3. REL_ATTR: id
4. Common Name:

5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
macro	macro	BREL	macro.persistent_id	LREL REQUIRED
bhvtpl	bhvtpl	BREL	bhvtpl.id (http://bhvtpl.id)	LREL REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	BREL	cnt.id (http://cnt.id)	LREL

Macro

This topic contains the following information:

macro Object

The object details are as follows:

1. Associated Table: Spell_Macro
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
usr_string1	fragment	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		
lock_object	lock_object	INTEGER		REQUIRED
msg_html	msg_html	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
ob_type	ob_type	STRING		REQUIRED
persistent_id	persid	STRING		
sym	sym	STRING		REQUIRED UNIQUE
type	type	STRING	splmactp persid	REQUIRED
usr_integer1	usr_integer1	INTEGER		
usr_integer2	usr_integer2	INTEGER		
usr_integer3	usr_integer3	INTEGER		
usr_string2	usr_string2	STRING		
usr_string3	usr_string3	STRING		
usr_string4	usr_string4	STRING		

macro_type Object

The object details are as follows:

1. Associated Table: Spell_Macro_Type
2. Factories: default, edit_macros
3. REL_ATTR: code, persistent_id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
arg_list	arg_list	STRING		
code	code	STRING		UNIQUE REQUIRED
delete_flag	del	INTEGER	actbool enum	REQUIRED
display_name	display_name	STRING		
execute_script	execute_script	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		
lock_object_flag	lock_object_flag	INTEGER		
persistent_id	persid	STRING		
sym	sym	STRING		REQUIRED
tech_desc	tech_desc	STRING		
validate_script	validate_script	STRING		

pdmMacroControlType Object

This object contains design view control types. The object details are as follows:

1. Associated Table: usp_pdmMacroControlType
2. Factories: default
3. REL_ATTR: enum
4. Common Name: name
5. UI_INFO: NOLOOKUP
6. Function Group: admin

Attribute	DB Field	Data Type	SREL References	Flags
enum	enum	INTEGER		
sym	sym	STRING		
description	description	STRING		
delete_flag	del	INTEGER		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt	

pdmMacroParam Object

This object describes an argument of a web macro. The object details are as follows:

1. Associated Table: usp_pdmMacroParam
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. UI_INFO: NOLOOKUP
6. Function Group: admin

Attribute	DB Field	Data Type	SREL References	Flags
macro	macro	SREL	pdmMacro	
name	name	STRING		REQUIRED
caption	caption	STRING		REQUIRED
description	description	STRING		
tooltip	tooltip	STRING		
help_form	help_form	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
is_required	is_required	INTEGER		
is_advanced	is_advanced	INTEGER		
default_value	default_value	STRING		
type	type	SREL	pdmMacroParamType	REQUIRED
size_textbox	size_textbox	INTEGER		
value_list	value_list	STRING		
delete_flag	del	SREL	actbool	REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt	

pdmMacroParamType Object

This object contains design view control types. The object details are as follows:

1. Associated Table: usp_pdmMacroParamType
2. Factories: default
3. REL_ATTR: enum
4. Common Name: name
5. UI_INFO: NOLOOKUP
6. Function Group: admin

Attribute	DB Field	Data Type	SREL References	Flags
enum	enum	INTEGER		
sym	sym	STRING		
description	description	STRING		
delete_flag	del	INTEGER		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt	

pdmMacroType Object

This object contains macro form types (detail or list). The object details are as follows:

1. Associated Table: usp_pdmMacroType
2. Factories: default
3. REL_ATTR: enum
4. Common Name: name

5. UI_INFO: NOLOOKUP
6. Function Group: admin

Attribute	DB Field	Data Type	SREL References	Flags
enum	enum	INTEGER		
sym	sym	STRING		
description	description	STRING		
delete_flag	del	INTEGER		
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt	

Layout

This article contains the following topics:

menu_bar Object

The object details are as follows:

1. Associated Table: usp_menu_bar
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: Security
6. REST Operations: CREATE READ UPDATE

Attribute Name	Data Type	Relationship Object	Flags
id	INTEGER		UNIQUE
name	STRING		REQUIRED
code	STRING		UNIQUE; REQUIRED
delete_flag	SREL	actbool	REQUIRED
description	STRING		
htmpl_name	STRING		
last_mod_by	SREL	cnt	
last_mod_dt	DATE		

menu_tree Object

The object details are as follows:

1. Associated Table: usp_menu_tree
2. Factories: default
3. REL_ATTR: id
4. Common Name: caption
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attributes	Data Type	Related Object	Flags
id	INTEGER		UNIQUE
caption	STRING		REQUIRED
description	STRING		
has_children	INTEGER		
parent_id	INTEGER		
resource	SREL	menu_tree_res	
tree_name	SREL	menu_tree_name	
last_mod_dt	DATE		
last_mod_by	SREL	cnt	

menu_tree_name Object

The object details are as follows:

1. Associated Table: usp_menu_tree_name
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attributes	Data Type	Related Object	Flags
id	INTEGER		UNIQUE
name	STRING		REQUIRED
code	STRING		UNIQUE; REQUIRED

delete_flag	SREL	actbool	REQUIRED
description	STRING		
internal	SREL	bool	REQUIRED
last_mod_dt	DATE		
last_mod_by	SREL	cnt	

menu_tree_res Object

The object details are as follows:

1. Associated Table: usp_menu_tree_res
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: Security
6. REST Operations: CREATE READ UPDATE

Attributes	Data Type	Related Object	Flags
id	INTEGER		UNIQUE
name	STRING		REQUIRED
delete_flag	SREL	actbool	REQUIRED
description	STRING		
resource	STRING		
type	INTEGER		
last_mod_dt	DATE		
last_mod_by	SREL	cnt	

Notification Objects

This article contains the following topics:

Notification

The object details are as follows:

1. Associated Table: Notification
2. Factories: default
3. REL_ATTR: id
4. Common Name: ALT_EMAIL
5. Function Group:
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
Email Address	ALT_EMAIL	STRING		
Contact ID	ANALYST_ID	UUID	ca_contact uuid	
Document ID	DOC_ID	INTEGER		
id	ID	INTEGER		REQUIRED KEY
Last Modified Date	LAST_MOD_DT	LOCAL_TIME		
KT Notification Level	NTF_LEVEL	INTEGER		

notque Object

The object details are as follows:

1. Associated Table: Queued_Notify
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: msg_title
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
cmth_override	cmth_override	INTEGER		
context_persid	context_persid	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
internal	internal	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
msg_ack	msg_ack	STRING		
msg_body	msg_body	STRING		
msg_body_html	msg_body_html	STRING		
msg_title	msg_title	STRING		
notify_level	notify_level	INTEGER		
persistent_id	persid	STRING		
transition_pt	transition_pt	INTEGER		

noturg Object

The object details are as follows:

1. Associated Table: Notification_Urgency
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
enum	enum	INTEGER		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
description	nx_desc	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY

ntfl Object

The object details are as follows:

1. Associated Table: Notify_Object_Attr
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
producer_id	producer_id	LOCAL STRING 20		
persistent_id	persid	STRING 30	persid	
mgs_ntf	mgs_ntf	LREL	mgs dist_ntflist	
delete_flag	del	INTEGER	actbool enum	REQUIRED
sym	sym	STRING 60		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact uuid	
modified_date	last_mod_dt	LOCAL_TIME		
description	description	STRING 240		
object_attr	object_attr	STRING		
object_type	object_type	STRING		
macro_ntf	macro_ntf	LREL	att_ntflist	
att_ntfrlist	att_ntfrlist	LREL	ntfr_ntflist	

ntfm Object

The object details are as follows:

1. Associated Table: Notify_Msg_Tpl
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: sym
5. Function Group: notification_reference
6. REST Operations: CREATE READ UPDATE

Attribute	Data Type	SREL References	Flags
id	INTEGER		UNIQUE REQUIRED KEY
producer_id	LOCAL STRING 20		
persistent_id	STRING 30		
delete_flag	SREL	actbool	REQUIRED
sym	STRING 128		REQUIRED
notify_flag	INTEGER		
notify_level	SREL	noturg	
notify_msg_title	STRING 80		REQUIRED
notify_msg_body	STRING 4000		

Attribute	Data Type	SREL References	Flags
notify_msg_body_html	STRING 32768		
notify_msg_body_html_real	LOCAL STRING 0		
obj_type	SREL	ntfm_prod_list.sym	REQUIRED
last_mod_dt			
last_mod_by	SREL	cnt	
tenant	SREL	tenant.id	

ntfr Object

The object details are as follows:

1. Associated Table: Notify_Rule
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: notification _reference
6. REST Operations: CREATE READ UPDATE

Attribute	Data Type	SREL References	Flags
id	INTEGER		UNIQUE REQUIRED KEY
producer_id	LOCAL STRING 20		
persistent_id	STRING 30		
delete_flag	SREL	actbool	REQUIRED
sym	STRING 128		REQUIRED
description	STRING 500		
condition	SREL	macro.persistent_id	
obj_type	SREL	ntfr_prod_list	REQUIRED
last_mod_dt	DATE		
last_mod_by	SREL	cnt	
default_rule	INTEGER		
cr_notify_info	SREL	ntfm.persistent_id	
chg_notify_info	SREL	ntfm.persistent_id	
iss_notify_info	SREL	ntfm.persistent_id	
mgs_notify_info	SREL	ntfm.persistent_id	
kd_notify_info	SREL	ntfm.persistent_id	
kd_comment_notify_info	SREL	ntfm.persistent_id	

Attribute	Data Type	SREL References	Flags
krc_notify_info	SREL	ntfm.persistent_id	
sa_notify_info	SREL	ntfm.persistent_id	
cnt_notify_info	SREL	ntfm.persistent_id	
ci_notify_info	SREL	ntfm.persistent_id	
ntfr_ntflist	LREL	ntfl att_ntfrlist	
ntfr_cntlist	LREL	cnt:PDM att_ntfrlist	
ntfr_ctplist	LREL	ctp:PDM att_ntfrlist	
ntfr_macrolist	LREL	marco att_ntfrlist	
tenant	SREL	tenant.id	

Problem Category

This article contains the following topics:

pcat Object

The object details are as follows:

1. Associated Table: Prob_Category
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
producer_id		STRING 20		
persistent_id	persid	STRING 30		
delete_flag		SREL	actbool.enum	REQUIRED
sym	sym	STRING 1000		REQUIRED S_KEY
last_mod_dt	last_mod_dt	LOCAL_TIME		
last_mod_by		SREL	cnt.id	
description	description			

Attribute	DB Field	Data Type	SREL References	Flags
		STRING 500		
organization		SREL	org.id	
assignee	assignee	SREL	agt.id	
group	group_id	UUID	group.id	
properties		BREL	cr_prptpl.owning_are	
survey		SREL	svy_tpl.id	
auto_assign	auto_assign	INTEGER		
service_type		SREL	sdsc.code	
category_urgency		SREL	urg.enum	
owning_contract		SREL	svc_contract.id	
cr_flag	cr_flag	INTEGER		
in_flag	in_flag	INTEGER		
pr_flag	pr_flag	INTEGER		
suggest_knowledge	suggest_knowledge	INTEGER		
assignable_ci_attr	assignable_ci_attr	STRING 60		
service_grps		BREL	lrel_svc_grps_svc_pcat.pcat	
service_locs		BREL	lrel_svc_locs_svc_pcat.pcat	
service_schedules		BREL	lrel_svc_schedules_pcat_svc.pcat	
ss_include		SREL	bool.enum	REQUIRED On new default: 0
ss_sym	ss_sym	STRING 128		
flow_flag	flow_flag	INTEGER		

pcat_loc Object

The object details are as follows:

1. Associated Table: Pcat_Loc
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: lpid
5. Function Group:

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
lattr	l_attr	STRING		
lpid	l_persid	STRING		
lseq	l_sql	INTEGER		
rattr	r_attr	STRING		
rpid	r_persid	STRING		
rseq	r_sql	INTEGER		

Priority

This article contains the following topics:

pri Object

The object details are as follows:

1. Associated Table: Priority
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
enum	enum	INTEGER		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
description	nx_desc	STRING		
service_type	service_type	STRING	srv_desc code	
sym	sym	STRING		UNIQUE REQUIRED S_KEY

pri_cal Object

The object details are as follows:

1. Associated Table: usp_pri_cal
2. REL_ATTR: id
3. Common Name: name
4. Function Group: admin
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
producer_id		LOCAL_STRING 20		
persistent_id	persid	STRING 60		
delete_flag	del	SREL	actbool.enum	REQUIRED
name	name	STRING 80		REQUIRED
description	description	STRING 240		
in_flag	in_flag	SREL	bool.enum	
pr_flag	pr_flag	SREL	bool.enum	
imp_def	imp_flag	SREL	imp.enum	
urg_def	urg_def	SREL	urg.enum	
ci_imp	ci_imp	SREL	bool.enum	
cat_urg	bk_window	SREL	bool.enum	
bk_window	cnt_vip	SREL		
cnt_vip	cnt_vip	SREL		
pri_5_4	pri_5_4	SREL	pri_enum	
pri_5_3	pri_5_3	SREL	pri_enum	
pri_5_2	pri_5_2	SREL	pri_enum	
pri_5_1	pri_5_1	SREL	pri_enum	
pri_5_0	pri_5_0	SREL	pri_enum	
pri_5_x	pri_5_x	SREL	pri_enum	
pri_4_4	pri_4_4	SREL	pri_enum	
pri_4_3	pri_4_3	SREL	pri_enum	
pri_4_2	pri_4_2	SREL	pri_enum	
pri_4_1	pri_4_1	SREL	pri_enum	
pri_4_0	pri_4_0	SREL	pri_enum	
pri_4_x	pri_4_x	SREL	pri_enum	

Attribute	DB Field	Data Type	SREL References	Flags
pri_3_4	pri_3_4	SREL	pri_enum	
pri_3_3	pri_3_3	SREL	pri_enum	
pri_3_2	pri_3_2	SREL	pri_enum	
pri_3_1	pri_3_1	SREL	pri_enum	
pri_3_0	pri_3_0	SREL	pri_enum	
pri_3_x	pri_3_x	SREL	pri_enum	
pri_2_4	pri_2_4	SREL	pri_enum	
pri_2_3	pri_2_3	SREL	pri_enum	
pri_2_2	pri_2_2	SREL	pri_enum	
pri_2_1	pri_2_1	SREL	pri_enum	
pri_2_0	pri_2_0	SREL	pri_enum	
pri_2_x	pri_2_x	SREL	pri_enum	
pri_1_4	pri_1_4	SREL	pri_enum	
pri_1_3	pri_1_3	SREL	pri_enum	
pri_1_2	pri_1_2	SREL	pri_enum	
pri_1_1	pri_1_1	SREL	pri_enum	
pri_1_0	pri_1_0	SREL	pri_enum	
pri_1_x	pri_1_x	SREL	pri_enum	
pri_0_4	pri_0_4	SREL	pri_enum	
pri_0_3	pri_0_3	SREL	pri_enum	
pri_0_2	pri_0_2	SREL	pri_enum	
pri_0_1	pri_0_1	SREL	pri_enum	
pri_0_0	pri_0_0			
pri_0_x	pri_0_x	SREL	pri_enum	
pri_x_4	pri_x_4	SREL	pri_enum	
pri_x_3	pri_x_3	SREL	pri_enum	
pri_x_2	pri_x_2	SREL	pri_enum	
pri_x_1	pri_x_1	SREL	pri_enum	
pri_x_0	pri_x_0	SREL	pri_enum	
pri_x_x	pri_x_x	SREL	pri_enum	
cap_reason	cap_reason	SREL	bool.enum	
template_flag	template_flag	SREL	bool.enum	
last_mod_dt	last_mod_dt	LOCAL_TIME		
last_mod_by	last_mod_by	SREL	cnt.id	
tenant	tenant	UUID	ca_tenant	

Property Objects

This article contains the following topics:

prp Object

The object details are as follows:

1. Associated Table: Property
2. Factories: default
3. REL_ATTR: id
4. Common Name: value
5. Function Group: change_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
error_msg	error_msg	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
label	label	STRING		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
object_id	object_id	INTEGER	chg id	REQUIRED
object_type	object_type	STRING		REQUIRED
owning_macro	owning_macro	BOP_REF_STR	macro	REQUIRED
persistent_id	persid	STRING		
property	property	INTEGER	prptpl id	
required	required	INTEGER	bool_tab enum	
sample	sample	STRING		
sequence	sequence	INTEGER		REQUIRED
value_description	value_description	STRING		
validation_rule	validation_rule	BOP_REF_STR	prpval_rule	REQUIRED
validation_type	validation_type	BOP_REF_STR	prpval_type	REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
value	value	STRING		

prptpl Object

The object details are as follows:

1. Associated Table: Property_Template
2. Factories: default
3. REL_ATTR: id
4. Common Name: label
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
code	code	STRING		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
label	label	STRING		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact uuid	
modified_date	last_mod_dt	LOCAL_TIME		
object_attrname	object_attrname	STRING		REQUIRED
object_attrval	object_attrval	INTEGER		
object_type	object_type	STRING		REQUIRED
persistent_id	persid	STRING		
producer_id		LOCAL STRING 20		
required	required	INTEGER		REQUIRED
required_sym	required_sym	SREL	bool.enum	
sample	sample	STRING		
sequence	sequence	INTEGER		REQUIRED
validation_rule	validation_rule	BOP_REF_STR	prpval_rule	REQUIRED

prpval Object

The object details are as follows:

1. Associated Table: Property_Value
2. REL_ATTR: id

3. Common Name: value
4. Function Group: admin
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
producer_id		LOCAL_STRING 20		
persistent_id	persid			
delete_flag	del	SREL	actbool.enum	REQUIRED
description	description	STRING 240		
owning_rule	owning_rule	SREL	prpval_rule.id	
value	value	STRING 240		REQUIRED
is_default	is_default	INTEGER		
modified_date	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id	

prpval_rule Object

The object details are as follows:

1. Associated Table: Property_Validation_Rule
2. REL_ATTR: id
3. Common Name: sym
4. Function Group: admin
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
producer_id		LOCAL_STRING 20		
persistent_id	persid	STRING 30		
delete_flag	del	SREL	actbool.enum	REQUIRED
sym	sym	STRING 60		REQUIRED
description	description	STRING 240		
validation_type	validation_type	SREL	prpval_type.id	
values		BREL	prpval.owning_rule	
modified_date	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id	

prpval_type Object

The object details are as follows:

1. Associated Table: Property_Validation_Type
2. REL_ATTR: id
3. Common Name: sym
4. Function Group: admin
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
producer_id		LOCAL_STRING 20		
persistent_id	persid			
delete_flag	del	SREL	actbool.enum	REQUIRED
sym	sym	STRING 60		REQUIRED
description	description	STRING 240		
modified_date	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id	

Reporting Method

This topic contains the following information:

rptm Object

The object details are as follows:

1. Associated Table: Rpt_Meth
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		

default_page_length	def_pg_len	STRING		
default_out	default_out	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
is_default	is_default	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
script	script	STRING		
sym	sym	STRING		REQUIRED

rptmeth Object

The object details are as follows:

1. Associated Table: Reporting_Method
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
sym	sym	STRING		UNIQUE REQUIRED S_KEY

Request

This topic contains the following information:

- crsol Object (see page 4594)
- crsq Object (see page 4595)

cr Object

The object details are as follows:

1. Associated Table: Call_Req
2. Factories: default
3. REL_ATTR: persistent_id
4. Common Name: ref_num
5. Function Group: call_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
active	active_flag	INTEGER	bool_tab enum	REQUIRED
active_prev	LOCAL	SREL	bool.enum	
affected_ resource	affected_rc	UUID	ca_owned_ resource uuid	
assignee	assignee	UUID		
assignee_prev	LOCAL	SREL	agt.id (http://agt.id)	
call_back_date	call_back_date	LOCAL_ TIME		
call_back_flag	call_back_flag	INTEGER		
category	category	STRING	prob_ctg persid	
category_prev	LOCAL	SREL	pcat.persistent_id	
caused_by_chg	caused_by_chg	SREL	chg.id (http://chg.id)	
change	change	INTEGER	chg id	
charge_back_id	charge_back_ id	STRING		
close_date	close_date	LOCAL_ TIME		
cr_tticket	cr_tticket	INTEGER		
created_via	created_via	INTEGER	interface id	
customer	customer	UUID	ca_contact uuid	REQUIRED
event_token	event_token	STRING		
external_system_tick et		STRING (4000)		
extern_ref	extern_ref	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
group	group_id	UUID		
group_prev	LOCAL	SREL	grp.id (http://grp.id)	
id	id	INTEGER		UNIQUE REQUIRED KEY
impact	impact	INTEGER	impact enum	
impact_prev	LOCAL	SREL	imp.enum	
incident_priority	incident_priority	INTEGER		
incorrectly_assigned		SREL	actbool	
last_act_id	last_act_id	STRING		
last_mod_dt	last_mod_dt	LOCAL_TIME		
log_agent	log_agent	UUID	ca_contact uuid	REQUIRED
macro_ predicted_ violation	macro_predict_ viol	INTEGER		
major_incident		SREL	actbool	
open_date	open_date	LOCAL_ TIME	org	
orig_user_admin_org		SREL	org	
orig_user_cost_center		SREL	cost_cntr	
orig_user_dept		SREL	dept	
orig_user_organization		SREL	org	
outage_detail_what		STRING (4000)		
outage_detail_who		STRING (4000)		
outage_detail_why		STRING (4000)		
outage_end_time	outage_end_time	LOCAL_TIME		
outage_reason		SREL	outage_reason	
outage_start _time	outage_start _time	LOCAL_TIME		
outage_type		SREL	outage_type	
parent	parent	STRING	call_req persid	
pct_service_restored		INTEGER		
persistent_id	persid	STRING		
predicted_sla_violation	predicted_sla_viol	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
priority	priority	INTEGER	pri enum	REQUIRED
priority_prev	LOCAL	SREL	pri.enum	
problem	problem	STRING		
ref_num	ref_num	STRING		UNIQUE REQUIRED S_KEY
remote_control_used		SREL	actbool	
requested_by		SREL	cnt	
resolvable_at_lower		SREL	actbool	
resolve_date	resolve_date	LOCAL_ TIME		
return_to_service		SREL	actbool	
rootcause	rootcause	INTEGER	rootcause id	
extern_token	sched_token	STRING		
severity	severity	INTEGER	sevrty enum	
severity_prev	LOCAL	SREL	sev.enum	
sla_violation	sla_violation	INTEGER		
base_template	solution	STRING	call_req persid	
status	status	STRING	cr_stat code	
status_prev	LOCAL	SREL	crs.code	
string1	string1	STRING		
string2	string2	STRING		
string3	string3	STRING		
string4	string4	STRING		
string5	string5	STRING		
string6	string6	STRING		
children		QREL	cr	
sla_events		QREL	tev	
attached_slas		BREL	attached_sla. _mapped_cr	
add_sla_persids	add_sla_persids	STRING		
site_sla_attrs	site_sla_attrs	STRING		
audit_userid	audit_userid	SREL	cnt.id (http://cnt.id)	
fldchange_log	fldchange_log	STRING		
affected_service	affected_service	SREL	nr	
init_urg		LOCAL INTEGER		
init_imp		LOCAL INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
cap_reason		LOCAL STRING		
auto_urg		LOCAL INTEGER		
auto_imp		LOCAL INTEGER		
man_urg		LOCAL INTEGER		
man_imp		LOCAL INTEGER		
summary	summary	STRING		
support_lev	support_lev	STRING	srv_desc code	
symptom_code		SREL	symptom_code	
template_name	template_name	STRING	cr_template template_name	
time_spent_ sum	time_spent_ sum	DURATION		
type	type	STRING	crt code	
urgency	urgency	INTEGER	urgncy enum	
urgency_prev	LOCAL	SREL	urg.enum	
target_times	target_times	BREL	tgt_time_mapped_cr	
target_start_last	target_start_last	DATE		
target_hold_last	target_hold_last	DATE		
target_hold_count	target_hold_count	INTEGER		
target_resolved_last	target_resolved_last	DATE		
target_resolved_count	target_resolved_count	INTEGER		
target_closed_last	target_closed_last	DATE		
target_closed_count	target_closed_count	INTEGER		
close_date_prev	close_date_prev	LOCAL DATE		
resolve_date_prev	resolve_date_prev	LOCAL DATE		
target_hold_count_prev	target_hold_count_prev	INTEGER		
target_resolved_count_prev	target_resolved_count_prev	LOCAL INTEGER		
target_closed_count_prev	target_closed_count_prev	LOCAL INTEGER	tgt_time_mapped_iss	

cr_prp Object

The object details are as follows:

1. Associated Table: Req_Property
2. Factories: default
3. REL_ATTR: id
4. Common Name: label
5. Function Group: call_mgr
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	nvarchar(240)		
error_msg	error_msg	STRING		
id	id	INTEGER		Primary key of this table.
label	label	nvarchar(80)		REQUIRED
last_mod_by	last_mod_by	byte(16)	ca_contact uuid	
last_mod_dt	last_mod_dt	INTEGER		
owning_cr	owning_cr	nvarchar 30	call_req persid	REQUIRED
owning_macro	owning_macro	BOP_REF_STR	macro	REQUIRED
persistent_id	persid	STRING		
required	required	INTEGER		REQUIRED
sample	sample	nvarchar(240)		
sequence	sequence	INTEGER		REQUIRED
value_description	value_description	STRING		
validation_rule	validation_rule	BOP_REF_STR	prpval_rule	REQUIRED
validation_type	validation_type	BOP_REF_STR	prpval_type	REQUIRED
value	value	nvarchar(240)		

cr_prptpl Object

The object details are as follows:

1. Associated Table: Req_Property_Template
2. Factories: default
3. REL_ATTR: id

4. Common Name: label
5. Function Group: call_mgr_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
code	code	STRING		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
label	label	STRING		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
owning_area	owning_area	STRING	prob_ctg persid	REQUIRED
persistent_id	persid	STRING		
producer_id		LOCAL STRING 20		
required	required	INTEGER		REQUIRED
sample	sample	STRING		
sequence	sequence	INTEGER		REQUIRED
validation_rule	validation_rule	BOP_REF_STR	prpval_rule	REQUIRED

cr_trans Object

The object details are as follows:

1. Associated Tables: cr_trans
2. Factories: default
3. REL_ATTR: id
4. Common Name: condition_error

Function Group: call_mgr_reference

REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
status	status	STRING	crs	Specifies the current ticket status.
new_status	new status	STRING	crs	Specifies the new ticket status.
t_type		INTEGER		Specifies the transition type.

Attribute	DB Field	Data Type	SREL References	Flags
			transition type	
is default		INTEGER		Default transition that appears when the Status field is empty. On new default: 0
must_comment		INTEGER		Comment required when using a transition. On new default: 0
delete_flag	del		actbool	Required. On new default: 0
condition			macro	Site condition macro to approve transition.
condition_error		STRING		Error message for site condition.
description		STRING		Description of this transition.
last_mod_by			cnt	On new default user; on CI set user
last_mod_dt		DATE		On CI set user now

cr_tpl Object

The object details are as follows:

1. Associated Table: Cr_Template
2. Factories: default
3. REL_ATTR: template_name
4. Common Name: template_name
5. Function Group: call_mgr_template
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
quick_tmpl_type	quick_tmpl_type	INTEGER	quick_tpl_types enum	REQUIRED
template	template	STRING	call_req persid	

Attribute	DB Field	Data Type	SREL References	Flags
template_class	template_class	STRING		
template_name	template_name	STRING		UNIQUE REQUIRED S_KEY

crs Object

The object details are as follows:

1. Associated Table: Cr_Status
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: call_mgr_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
active	active	INTEGER		
code	code	STRING		UNIQUE REQUIRED S_KEY
cr_flag	cr_flag	INTEGER		
delete_flag	del	INTEGER	actbool enum	REQUIRED
hold	hold	INTEGER		
id	id	INTEGER		UNIQUE REQUIRED KEY
in_flag	in_flag	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
pr_flag	pr_flag	INTEGER		
resolved	resolved	INTEGER		
sym	sym	STRING		REQUIRED

crsol Object

The object details are as follows:

1. Associated Table: Call_Solution
2. Factories: default

3. REL_ATTR: persistent_id
4. Common Name: sym
5. Function Group: call_mgr_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
cr_count	cr_count	INTEGER		
cr_flag	cr_flag	INTEGER		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
in_flag	in_flag	INTEGER		
last_mod_dt	last_mod_dt	LOCAL_TIME		
desc	nx_desc	STRING		
persistent_id	persid	STRING		
pr_flag	pr_flag	INTEGER		
solution_approved	sapproved	INTEGER	bool_tab enum	
solution_name	sname	STRING		
solution	solution	STRING		
sym	sym	STRING		REQUIRED S_KEY
tcode	tcode	INTEGER		

crsq Object

The object details are as follows:

1. Associated Table: Cr_Stored_Queries
2. Factories: default, sqchg, sqcr, sqiss
3. REL_ATTR: code
4. Common Name: label
5. Function Group: stored_queries
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
code	code	STRING		UNIQUE REQUIRED S_KEY

Attribute	DB Field	Data Type	SREL References	Flags
count_url	count_url	STRING		
where_clause	criteria	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
label	label	STRING		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
obj_type	obj_type	STRING		
persistent_id	persid	STRING		

Risk

This article contains the following topics:

risk_level Object

The object details are as follows:

1. Rel Attr: value
2. Function Group: change_reference
3. Common Name: sym
4. Associated Table: usp_risk_level
5. Index Key: enum, sym
6. Factories: risk_level
7. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
delete_flag	del	INTEGER		
sym	sym	STRING 60		UNIQUE NOT_NULL S_KEY

Attribute	DB Field	Data Type	SREL References	Flags
value	enum	INTEGER		
description	desc	STRING 40		
last_mod_dt	last_mod_dt	LOCAL_TIME		
last_mod_by	last_mod_by	UUID	ca_contact	

risk_range Object

The object details are as follows:

1. Rel Attr: id
2. Function Group: change_reference
3. Associated Table: usp_risk_range
4. Factories: risk_range
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE KEY
persistent_id	persid	BOP_REF_STR		Persistent id
delete_flag	del	INTEGER		Active: 0 Inactive: 1
risk_lvl	risk_lvl	INTEGER	risk_level	Reference to Risk Level
max_val	max_val	INTEGER		Maximum value of Risk Level
min_val	min_val	INTEGER		Minimum value of Risk Level
owning_survey	owning_survey	INTEGER	risk_svy_ tpl	Reference to owning Risk Survey Template
last_mod_dt		LOCAL_TIME		Last modified by
last_mod_by		UUID	ca_contact	Reference to Contact information
tenant		UUID	ca_tenant	Reference to Tenant information

risk_svy Object

The object details are as follows:

1. Rel Attr: id
2. Common Name: description
3. Function Group: change_reference

4. Associated Table: usp_risk_svy
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE KEY
persistent_id	persid	STRING 30		
delete_flag	del	SREL		REQUIRED
description	description	STRING 400		
sym	sym	STRING 60		REQUIRED
include_comment	include_comment	INTEGER		REQUIRED
comment_label	comment_label	STRING 80		
comment	comment	STRING 200		
chg_id	chg_id	SREL	chg	
survey_template	survey_template	SREL		
total_weightage	total_weightage	INTEGER		
last_mod_dt	last_mod_dt	DATE		Last modified by
last_mod_by	last_mod_by	SREL	cnt.id	
questions		QREL	risk_svy_ question	

risk_svy_answer Object

The object details are as follows:

1. Rel Attr: id
2. Common Name: text
3. Function Group: change_reference
4. Reference Table: usp_risk_svy_answer
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		
persistent_id	persid	STRING 30		
delete_flag	del	SREL	actbool.enum	
text	txt	STRING 400		
sequence	sequence	INTEGER		REQUIRED
weightage	weightage	INTEGER		
selected	selected	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
owning_survey_ question	owning_survey_ question	SREL	risk_svy_ question.id	REQUIRED
last_mod_dt	last_mod_dt	LOCAL_TIME		
last_mod_by	last_mod_by	UUID	ca_contact	
tenant		UUID	ca_tenant	

risk_svy_atpl Object

The object details are as follows:

1. Rel Attr: id
2. Common Name: text
3. Function Group: change_reference
4. Reference Table: usp_risk_svy_atpl
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE KEY
persistent_id	persid	BOP_REF_ STR		Persistent id
delete_flag	del	SREL	act_bool. enum	
txt	txt	STRING 400		Answer Text
sequence	sequence	INTEGER		Display order
weightage	weightage	INTEGER		Weightage of answer
owning_survey_ question	owning_survey_q uestion	INTEGER	risk_svy_qtp l	Reference to owning Risk Survey question template
last_mod_dt	last_mod_dt	LOCAL_TI ME		Last modified by
last_mod_by	last_mod_by	UUID	ca_contact	
tenant		UUID	ca_tenant	Reference to Tenant information

risk_svy_question Object

The object details are as follows:

1. Rel Attr: id

2. Common Name: text
3. Function Group: change_reference
4. Reference Table: usp_risk_svy_question
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		
persistent_id	persid			
delete_flag	del	SREL	actbool.enum	
text	txt	STRING 400		
sequence	sequence	INTEGER		REQUIRED
include_ qcomment	include_ qcomment	INTEGER		
qcomment_ label	qcomment_ label	STRING 80		
qcomment	qcomment	STRING 2000		
mult_resp_flag	mult_resp_flag	INTEGER		
owning_ survey	owning_survey	SREL	risk_svy.id	REQUIRED
last_mod_dt	last_mod_dt	LOCAL_TIME		
last_mod_by	last_mod_by	UUID	ca_contact	
answers		QREL	risk_svy_answer	
tenant		UUID	ca_tenant	

risk_svy_qtpl Object

The object details are as follows:

1. Rel Attr: id
2. Common Name: text
3. Function Group: change_reference
4. Reference Table: usp_risk_svy_qtpl
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE KEY
persistent_id	persid	BOP_REF_STR		Persistent id
delete_flag	del	SREL		

Attribute	DB Field	Data Type	SREL References	Flags
			actbool. enum	
text	txt	STRING 400		Question Text
sequence	sequence	INTEGER		Display order
include_qcomment	include_qcomment	INTEGER		Set to 1 to include comment box for this question.
qcomment_label	qcomment_label	STRING 80		Label for Comment field
mult_resp_flag	mult_resp_flag	INTEGER		0: Choose 1 response (radio) 1: Choose "n" (checkboxes)
owning_survey	owning_survey	INTEGER	risk_svy_tpl	Reference to owning Risk Survey template
last_mod_dt	last_mod_dt	LOCAL_TIME		Last modified by
last_mod_by	last_mod_by	UUID	ca_contact	Reference to Contact information
tenant		UUID	ca_tenant	Reference to Tenant information

risk_svy_tpl Object

The object details are as follows:

1. Rel Attr: id
2. Common Name: sym
3. Function Group: change_reference
4. Reference Table: usp_risk_svy_tpl
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
persistent_id	persid	BOP_REF_STR		
delete_flag	del	SREL	actbool.enum	
description	description	STRING 400		
sym	sym	STRING 60		UNIQUE S_KEY
include_comment	include_comment	INTEGER		
comment_label	comment_label	STRING 80		
last_mod_dt	last_mod_dt	LOCAL_TIME		

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_by	last_mod_by	UUID	ca_contact	
question_ templates		QREL	risk_svy_qtpl	
assocCategories		BREL	risk_survey	
assocRiskRanges		QREL	risk_range	
tenant		UUID	ca_tenant	

Role

This article contains the following topics:

role Object

The object details are as follows:

1. Associated Table: usp_role
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attributes	Data Type	Related Object	Flags
id	INTEGER		UNIQUE
producer_id	LOCAL STRING 20		
persistent_id	LOCAL STRING 60		
name	STRING		REQUIRED
code	STRING		REQUIRED; UNIQUE
delete_flag	SREL	actbool	REQUIRED
default_flag	INTEGER		
description	STRING		
interface_type	INTEGER		
pref_doc	INTEGER		REQUIRED
form_group	SREL	fmgrp	

help_view	SREL	help_set	
initial_form	STRING		REQUIRED
grant_level	SREL	acc_lvls	REQUIRED
view_internal	INTEGER		
data_partition	SREL	dmn	
override_cnt_datapart	INTEGER		REQUIRED
update_global	INTEGER		
tenant_access	INTEGER		
single_tenant	SREL	tenant	
tenant_group	SREL	tenant_group	
call_mgr	INTEGER		
change_mgr	INTEGER		
issue_mgr	INTEGER		
inventory	INTEGER		
references	INTEGER		
notify	INTEGER		
admin	INTEGER		
security	INTEGER		
sd_admin	INTEGER		
sd_analyst	INTEGER		
sd_emloyee	INTEGER		
sd_customer	INTEGER		
kt_admin	INTEGER		
kt_manager	INTEGER		
kt_engineer	INTEGER		
kt_analyst	INTEGER		
kt_customer	INTEGER		
tn_admin	INTEGER		
kt_type	INTEGER		
kd	INTEGER		
kcat	INTEGER		
kd_query_id	SREL	crsq	
kd_query_description	STRING 255		
wsp	INTEGER		
wsp_editForm	INTEGER		
wsp_publishForm	INTEGER		

Attributes	Data Type	Related Object	Flags
wsp_updPreview	INTEGER		
wsp_modifySchema	INTEGER		
wsp_publishSchema	INTEGER		
Tabs	BREL	role_tab	
web_forms	BREL	role_web_form	
go_forms	BREL	role_go_form	
last_mod_dt	DATE		
last_mod_by	SREL	cnt	

role_web_form Object

The object details are as follows:

1. Associated Table: usp_role_web_form
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attributes	Data Type	Related Object	Flags
id	INTEGER		UNIQUE
role_obj	SREL	role	
web_form_obj	SREL	web_form	
last_mod_dt	DATE		

role_go_form Object

The object details are as follows:

1. Associated Table: usp_role_go_form
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. Function Group: security
6. REST Operations: CREATE READ UPDATE

Attributes	Data Type	Related Object	Flags
id	INTEGER		UNIQUE
role_obj	SREL	role	
web_form_obj	SREL	web_form	
menu_bar_obj	SREL	menu_bar	
is_default	INTEGER		
last_mod_dt	DATE		

role_tab Object

The object details are as follows:

1. Associated Table: usp_role_tab
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. Function Group: Security
6. REST Operations: CREATE READ UPDATE

Attributes	Data Type	Related Object	Flags
id	INTEGER		UNIQUE
sequence	INTEGER		
role_obj	SREL	role	
tab_obj	SREL	tab	
last_mod_dt	DATE		

Support Automation Objects

This article contains the following topics:

sa_art_tool_avail Object

The object details are as follows:

- sa_system_message Object (https://support.ca.com/cadocs/0/CA%20Service%20Desk%20Manager%2012%209-ENU/Bookshelf_Files/HTML/CA_SDM_Tech_Ref_ENU/1207342.html)

  1. Associated Table: sa_art_tool_avail

2. Factories: default
3. REL_ATTR: id
4. Common Name: availBits
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
roleID	roleID	SREL	sa_role	
availBits	availBits	STRING 30		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_bin_temp Object

The object details are as follows:

1. Associated Table: sa_bin_temp
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		
data	data	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_branding Object

The object details are as follows:

1. Associated Table: sa_branding
2. Factories: default
3. REL_ATTR: id

4. Common Name: stylesheetURL
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
localizationID	localizationID	SREL	sa_localization	REQUIRED
stylesheetURL	stylesheetURL	STRING 512		
header	header	STRING 32768		
footer	footer	STRING 32768		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_alert_config_param Object

The object details are as follows:

1. Associated Table: sa_alert_config_param
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		
paramName	paramName	STRING 255		REQUIRED
paramValue	paramValue	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_comm_temp Object

The object details are as follows:

1. Associated Table: sa_comm_temp
2. Factories: default
3. REL_ATTR: id
4. Common Name: id

5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
data	data	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_cr_template Object

The object details are as follows:

1. Associated Table: sa_cr_template
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
tpl	tpl	SREL	Cr_Template	REQUIRED
is_default	is_default	SREL	bool.enum	
isActive	isActive	SREL	actrbool.enum	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_custom_category Object

The object details are as follows:

1. Associated Table: sa_custom_category
2. Factories: default
3. REL_ATTR: id
4. Common Name: categoryName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
categoryName	categoryName	STRING 100		REQUIRED
isActive	isActive	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_data_routing_server Object

The object details are as follows:

1. Associated Table: sa_data_routing_server
2. Factories: default
3. REL_ATTR: id
4. Common Name: label
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
label	label	STRING 100		REQUIRED
host	host	STRING 100		REQUIRED
port	port	INTEGER		REQUIRED
cssURL	cssURL	STRING 150		
enabled	enabled	SREL	actrbool.enum	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_datapool_channel Object

The object details are as follows:

1. Associated Table: sa_datapool_channel
2. Factories: default
3. REL_ATTR: channelID
4. Common Name: name
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
name	name	STRING 250		
persistent	persistent	INTEGER		REQUIRED
channelID	channelID	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_datapool_channel_user Object

The object details are as follows:

1. Associated Table: sa_datapool_channel_user
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
channelID	channelID	SREL	sa_datapool_ channel	REQUIRED
sessionID	sessionID	SREL	sa_login_ session	REQUIRED
snoop	snoop	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_debug_log Object

The object details are as follows:

1. Associated Table: sa_debug_log
2. Factories: default
3. REL_ATTR: id
4. Common Name: debugMessage
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
epoch	epoch	LOCAL_TIME		
debugLevel	debugLevel	INTEGER		
debugMessage	debugMessage	STRING 2048		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_default_credential Object

The object details are as follows:

1. Associated Table: sa_default_credential
2. Factories: default
3. REL_ATTR: id
4. Common Name: label
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
label	label	STRING 100		
Domain	Domain	STRING 255		
Login	Login	STRING 255		REQUIRED
Pwd	Pwd	STRING 255		REQUIRED
PwdPlain	PwdPlain	LOCAL STRING		REQUIRED
PwdConf	PwdConf	LOCAL STRING		REQUIRED
active	active	SREL	actrbool.enum	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_display_template_loc Object

The object details are as follows:

1. Associated Table: sa_display_template_loc
2. Factories: default
3. REL_ATTR: id

4. Common Name: displayTemplate
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
localizationID	localizationID	SREL	sa_localization	REQUIRED
eventType	eventType	SREL	sa_event_type	REQUIRED
displayTemplate	displayTemplate	STRING 510		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_event_type_param Object

The object details are as follows:

1. Associated Table: sa_event_type_param
2. Factories: default
3. REL_ATTR: id
4. Common Name: paramName

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
paramName	paramName	STRING 255		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_field Object

The object details are as follows:

1. Associated Table: sa_field
2. Factories: default
3. REL_ATTR: id
4. Common Name: displayName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
fieldType	fieldType	SREL	sa_field_type	REQUIRED

fieldName	fieldName	STRING 50		REQUIRED
fieldOrder	fieldOrder	INTEGER		REQUIRED
mandatory	mandatory	INTEGER		
active	active	SREL	actrbool.enum	
displayName	displayName	STRING 150		
guestMandatory	guestMandatory	SREL	bool.enum	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_field_type Object

The object details are as follows:

1. Associated Table: sa_field_type
2. Factories: default
3. REL_ATTR: fieldType
4. Common Name: fieldTypeDescription
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
fieldType	fieldType	INTEGER		REQUIRED
fieldType Description	fieldType Description	STRING 255		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_flow_control_rule Object

The object details are as follows:

1. Associated Table: sa_flow_control_rule
2. Factories: default
3. REL_ATTR: id
4. Common Name: pageName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
pageName	pageName	STRING 100		REQUIRED
state	state	STRING 100		REQUIRED
directedURL	directedURL	STRING 500		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_function_arg Object

The object details are as follows:

1. Associated Table: sa_function_arg
2. Factories: default
3. REL_ATTR: id
4. Common Name: arg_name
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
functionID	functionID	SREL	sa_lib_function	REQUIRED
arg_name	arg_name	STRING 75		REQUIRED
description	description	STRING 255		
index_value	index_value	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_hour_operation_mode Object

The object details are as follows:

1. Associated Table: sa_hour_operation_mode
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sym	sym	STRING 20		REQUIRED
enum	enum	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_iss_template Object

The object details are as follows:

1. Associated Table: sa_iss_template
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
tpl	tpl	SREL	Iss_Template	REQUIRED
is_default	is_default	SREL	bool.enum	
isActive	isActive	SREL	actrbool.enum	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_keyword Object

The object details are as follows:

1. Associated Table: sa_keyword
2. Factories: default
3. REL_ATTR: id
4. Common Name: keyname
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY

keyname	keyname	STRING 100	
last_mod_by	last_mod_by	UUID	ca_contact
last_mod_dt	last_mod_dt	LOCAL_TIME	

sa_keyword_queue_join Object

The object details are as follows:

1. Associated Table: sa_keyword_queue_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
keywordID	keywordID	SREL	sa_keyword	REQUIRED
queueID	queueID	SREL	sa_queue	REQUIRED
weight	weight	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_large_data_record Object

The object details are as follows:

1. Associated Table: sa_large_data_record
2. Factories: default
3. REL_ATTR: recordID
4. Common Name: originalTableName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
recordID	recordID	INTEGER		REQUIRED
recordOrder	recordOrder	INTEGER		REQUIRED
originalTableName	originalTableName			

Attribute	DB Field	Data Type	SREL References	Flags
data	data	STRING 32768		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_lib_function Object

The object details are as follows:

1. Associated Table: sa_lib_function
2. Factories: default
3. REL_ATTR: id
4. Common Name: functionName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
libID	libID	SREL	sa_scriptlib	REQUIRED
functionName	functionName	STRING 128		REQUIRED
libFunction	libFunction	INTEGER		REQUIRED
funcDesc	funcDesc	STRING 1024		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_localization Object

The object details are as follows:

1. Associated Table: sa_localization
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
localizationID	localizationID	SREL	sa_localization	REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
enabled	enabled	SREL	bool.enum	
name	name	STRING 100		
is_default	is_default	SREL	bool.enum	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_login_session Object

The object details are as follows:

1. Associated Table: sa_login_session
2. Factories: default
3. REL_ATTR: id
4. Common Name: jvm
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
userID	userID	SREL	cnt	
startEpoch	startEpoch	LOCAL_TIME		
endEpoch	endEpoch	LOCAL_TIME		
waitTime	waitTime	INTEGER		
supportLength	supportLength	INTEGER		
CanDownload ScriptApplets	CanDownload ScriptApplets	INTEGER		
CanDownloadDlls	CanDownloadDlls	INTEGER		
CanRunApplet Comms	CanRunApplet Comms	INTEGER		
CanDownloadExecs	CanDownloadExecs	INTEGER		
jvm	jvm	STRING 150		
NoPrompt	NoPrompt	INTEGER		
ClientIsEXE	ClientIsEXE	INTEGER		
Timezone	Timezone	INTEGER		
availableTime	availableTime	LOCAL_TIME		
unavailableTime	unavailableTime			

Attribute	DB Field	Data Type	SREL References	Flags
		LOCAL_TIME		
browser	browser	STRING 150		
DirectSessionCode	DirectSessionCode	STRING 100		
Question	Question	STRING 1024		
initialQueueID	initialQueueID	SREL	sa_queue	
QueuedEpoch	QueuedEpoch	LOCAL_TIME		
QueuedTime	QueuedTime	STRING 50		
OnHoldEpoch	OnHoldEpoch	LOCAL_TIME		
OnHoldTime	OnHoldTime	STRING 50		
HandledEpoch	HandledEpoch	LOCAL_TIME		
HandledTime	HandledTime	STRING 50		
GroupID	GroupID	SREL	sa_group	
AbandonFlag	AbandonFlag	INTEGER		
IsCurrent	IsCurrent	INTEGER		
SelfServe	SelfServe	INTEGER		
localizationID	localizationID	SREL	sa_localization	
profileOverride	profileOverride	INTEGER		
Accessibility ExtEnabled	Accessibility ExtEnabled	INTEGER		
IsWebClient	IsWebClient	INTEGER		
CategoryID	CategoryID	SREL	sa_custom_category	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_rejoin_code_mapping Object

The object details are as follows:

1. Associated Table: sa_rejoin_code_mapping
2. Factories: default
3. REL_ATTR: id

4. Common Name: rejoinCode
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
rejoinCode	rejoinCode	STRING 10		
rejoinString	rejoinString	STRING 100		
creationDate	creationDate	LOCAL_TIME		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_rule_conduit_rule Object

The object details are as follows:

1. Associated Table: sa_rule_conduit_rule
2. Factories: default
3. REL_ATTR: id
4. Common Name: functionName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
functionName	functionName	STRING 100		REQUIRED
className	className	STRING 100		
methodName	methodName	STRING 100		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_named_user_license Object

The object details are as follows:

1. Associated Table: sa_named_user_license
2. Factories: default
3. REL_ATTR: id

4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
userID	userID	SREL	cnt	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_patch_history Object

The object details are as follows:

1. Associated Table: sa_patch_history
2. Factories: default
3. REL_ATTR: id
4. Common Name: patch_name
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
patch_name	patch_name	STRING 100		REQUIRED
release_base	release_base	STRING 50		REQUIRED
build_version	build_version	STRING 50		
epoch	epoch	LOCAL_TIME		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_portal_component Object

The object details are as follows:

1. Associated Table: sa_portal_component
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
name	name	STRING 50		REQUIRED
URL	URL	STRING 255		REQUIRED
beforeLogin	beforeLogin	INTEGER		
afterLogin	afterLogin	INTEGER		
beforeProbDef	beforeProbDef	INTEGER		
afterProbDef	afterProbDef	INTEGER		
displayColumn	displayColumn	INTEGER		
displayIndex	displayIndex	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_property Object

The object details are as follows:

1. Associated Table: sa_property
2. Factories: default
3. REL_ATTR: id
4. Common Name: propertyName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
propertyName	propertyName	STRING 30		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_sd_user_map Object

The object details are as follows:

1. Associated Table: sa_sd_user_map
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
SDUUID	SDUUID	UUID		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_sdconfig Object

The object details are as follows:

1. Associated Table: sa_sdconfig
2. Factories: default
3. REL_ATTR: id
4. Common Name: propertyKey
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
propertyKey	propertyKey	STRING 50		REQUIRED
propertyValue	propertyValue	STRING 512		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_sdgroup_map Object

The object details are as follows:

1. Associated Table: sa_sdgroup_map
2. Factories: default
3. REL_ATTR: id
4. Common Name: SDTicketID
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_group	REQUIRED
SDTicketID	SDTicketIT	STRING 50		REQUIRED

SDRefNum	SDRefNum	STRING 50		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_sdsession_ticket_map Object

The object details are as follows:

1. Associated Table: sa_sdsession_ticket_map
2. Factories: default
3. REL_ATTR: id
4. Common Name: SDTicketID
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sessionID	sessionID	SREL	sa_login_session	REQUIRED
SDTicketID	SDTicketID	STRING 50		REQUIRED
SDRefNum	SDRefNum	STRING 50		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_sound Object

The object details are as follows:

1. Associated Table: sa_sound
2. Factories: default
3. REL_ATTR: id
4. Common Name: soundName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
soundName	soundName	STRING 255		

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_sup_desk_hour_config Object

The object details are as follows:

1. Associated Table: sa_sup_desk_hour_config
2. Factories: default
3. REL_ATTR: id
4. Common Name: label
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
label	label	STRING 100		
active	active	SREL	actrbool.enum	
useHours	useHours	SREL	sa_hour_operation_ mode	
workshift	workshift	SREL	Bop_Workshift	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_system_message Object

The object details are as follows:

1. Associated Table: sa_system_message
2. Factories: default
3. REL_ATTR: id
4. Common Name: messageTag
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
messageTag	messageTag	STRING 100		REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
localizationID	localizationID	SREL	sa_localization	REQUIRED
messageText	messageText	STRING 1024		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_system_property Object

The object details are as follows:

1. Associated Table: sa_system_property
2. Factories: default
3. REL_ATTR: id
4. Common Name: propertyKey
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
propertyKey	propertyKey	STRING 300		REQUIRED
propertyValue	propertyValue	STRING 32768		
property Description	property Description	STRING 32768		
isGlobal	isGloabl	SREL	bool.enum	
obsolete	obsolete	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_triage_script Object

The object details are as follows:

1. Associated Table: sa_triage_script
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
queueID	queueID	SREL	sa_queue	REQUIRED
scriptID	scriptID	SREL	sa_script	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_version Object

The object details are as follows:

1. Associated Table: sa_version
2. Factories: default
3. REL_ATTR: id
4. Common Name: DBVersion
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		
DBVersion	DBVersion	STRING 100		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_virtual_session Object

The object details are as follows:

1. Associated Table: sa_virtual_session
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
queueID	queueID	SREL	sa_queue	
userID	userID	SREL	ca_contact	

Attribute	DB Field	Data Type	SREL References	Flags
sessionID	sessionID	SREL	sa_login_session	
queuedEpoch	queuedEpoch	LOCAL_TIME		
handledEpoch	handledEpoch	LOCAL_TIME		
endEpoch	endEpoch	LOCAL_TIME		
waitTime	waitTime	INTEGER		
handledTime	handledTime	INTEGER		
abandonFlag	abandonFlag	INTEGER		
firstFlag	firstFlag	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_wait_component Object

The object details are as follows:

1. Associated Table: sa_wait_component
2. Factories: default
3. REL_ATTR: id
4. Common Name: waitURL
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
queueID	queueID	SREL	sa_queue	
waitURL	waitURL	STRING 300		
isExternal	isExternal	SREL	bool.enum	
pageType	pageType	SREL	sa_wait_ component_type	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_wait_component_type Object

The object details are as follows:

1. Associated Table: sa_wait_component_type
2. Factories: default

3. REL_ATTR: enum
4. Common Name: sym
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
enum	enum	INTEGER		
sym	sym	STRING 50		
is_optional	is_optional	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sapolicy Object

The object details are as follows:

1. Associated Table: SA_Policy
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
attachment	access_atmnt	INTEGER		
data_query	access_data	INTEGER		
knowledge_op	access_knowledge	INTEGER		
object_insertion	access_object_ins	INTEGER		
object_update	access_object_upd	INTEGER		
ticket_insertion	access_ticket_ins	INTEGER		
allow_impersonate	allow_impersonate	INTEGER	actbool enum	REQUIRED
code	code	STRING		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
ext_appl	ext_appl	INTEGER		
id	id	INTEGER		UNIQUE REQUIRED KEY
is_default	is_default	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
proxy_contact	proxy_contact	UUID	ca_contact uuid	
public_key	pub_key	STRING		
state	state	INTEGER		
sym	sym	STRING		REQUIRED

saprobtyp Object

The object details are as follows:

1. Associated Table: SA_Prob_Type
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
code	code	STRING		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
action	dup_action	INTEGER		
search_interval	dup_interval	DURATION		
id	id	INTEGER		UNIQUE REQUIRED KEY
is_default	is_default	INTEGER		
is_internal	is_internal	INTEGER	actbool enum	
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
owning_policy	owning_policy	INTEGER	sapolicy id	
persistent_id	persid	STRING		
program_output	ret_app_1	STRING		
user_output	ret_usr_1	STRING		
sym	sym	STRING		REQUIRED
template_factory	ticket_tmpl_fac	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
template_id	ticket_tmpl_id	INTEGER		
template_sym	ticket_tmpl_name	STRING		

Support Automation Disclaimer

This article contains the following topics:

sa_disclaimer Object

The object details are as follows:

1. Associated Table: sa_disclaimer
2. Factories: default
3. REL_ATTR: id
4. Common Name: disclaimerName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
disclaimerName	disclaimerName	STRING 30		REQUIRED
disclaimerText	disclaimerText	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_disclaimer_accept_log Object

The object details are as follows:

1. Associated Table: sa_disclaimer_accept_log
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
selfServe SessionID	selfServe SessionID	SREL	sa_self_serve_ session	REQUIRED
scriptID	scriptID	SREL	sa_script	REQUIRED
disclaimerID	disclaimerID	INTEGER		REQUIRED
accepted	accepted	INTEGER		REQUIRED
epoch	epoch	LOCAL_TIME		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_disclaimer_history Object

The object details are as follows:

1. Associated Table: sa_disclaimer_history
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sessionID	sessionID	SREL	sa_login_session	REQUIRED
disclaimerID	disclaimerID	SREL	sa_disclaimer	REQUIRED
response	response	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_disclaimer_localized Object

The object details are as follows:

1. Associated Table: sa_disclaimer_localized
2. Factories: default
3. REL_ATTR: id

4. Common Name: textLocal
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
disclaimerID	disclaimerID	SREL	sa_disclaimer	REQUIRED
localizationID	localizationID	SREL	sa_localization	REQUIRED
disclaimerText	disclaimerText	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Support Automation Security

This article contains the following topics:

sa_security_group Object

The object details are as follows:

1. Associated Table: sa_security_group
2. Factories: default
3. REL_ATTR: id
4. Common Name: groupName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupName	groupName	STRING 50		REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING 512		
rank	rank	INTEGER		REQUIRED
localizationID	localizationID	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_security_group_dir Object

The object details are as follows:

1. Associated Table: sa_security_group_dir
2. Factories: default
3. REL_ATTR: id
4. Common Name: directoryREST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_security_ group	REQUIRED
directory	directory	STRING 150		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_security_group_function Object

The object details are as follows:

1. Associated Table: sa_security_group_function
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_security_ group	REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
functionID	functionID	SREL	sa_security_ tool_function	REQUIRED
value	value	SREL	rev_bool.enum	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_security_group_loc Object

The object details are as follows:

1. Associated Table: sa_security_group_loc
2. Factories: default
3. REL_ATTR: id
4. Common Name: groupName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_security_ group	REQUIRED
localizationID	localizationID	SREL	sa_localization	REQUIRED
groupName	groupName	STRING 50		
description	description	STRING 512		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_security_grp_role_join Object

The object details are as follows:

1. Associated Table: sa_security_grp_role_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
roleID	roldIE	SREL	sa_role	REQUIRED
groupID	groupID	SREL	sa_security_ group	REQUIRED
isDefault	isDefault	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_security_login_function Object

The object details are as follows:

1. Associated Table: sa_security_login_function
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sessionID	sessionID	SREL	sa_login_session	REQUIRED
functionID	functionID	SREL	sa_security_ tool_function	REQUIRED
value	value	INTEGER		REQUIRED
localizationID	localizationID	SREL	sa_localization	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_security_request_order Object

The object details are as follows:

1. Associated Table: sa_security_request_order
2. Factories: default
3. REL_ATTR: id

4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
toolID	toolID	SREL	sa_tool	REQUIRED
functionID	functionID	SREL	sa_security_ tool_function	REQUIRED
orderbit	orderbit	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_security_text_localized Object

The object details are as follows:

1. Associated Table: sa_security_text_localized
2. Factories: default
3. REL_ATTR: id
4. Common Name: TextValue
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
TextID	textID	INTEGER		REQUIRED
localizationID	localizationID	SREL	sa_localization	REQUIRED
TextValue	TextValue	STRING 100		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_security_tool_function Object

The object details are as follows:

1. Associated Table: sa_security_tool_function
2. Factories: default
3. REL_ATTR: id

4. Common Name: functionName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
toolID	toolID	SREL	sa_tool	REQUIRED
functionName	functionName	STRING 50		
canPrompt	canPrompt	SREL	bool.enum	REQUIRED
localizationID	localizationID	SREL	sa_localization	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_security_tool_localized Object

The object details are as follows:

1. Associated Table: sa_security_tool_localized
2. Factories: default
3. REL_ATTR: id
4. Common Name: functionName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
functionID	functionID	SREL	sa_security_ tool_function	REQUIRED
localizationID	localizationID	SREL	sa_localization	
functionName	functionName	STRING 100		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_security_user_directory Object

The object details are as follows:

1. Associated Table: sa_security_user_directory
2. Factories: default
3. REL_ATTR: id
4. Common Name: directory

5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sessionID	sessionID	SREL	sa_login_session	REQUIRED
directory	directory	STRING 150		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Support Automation Self Service

This article contains the following topics:

sa_self_serve_event_join Object

The object details are as follows:

1. Associated Table: sa_self_serve_event_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
selfServe SessionID	selfServe SessionID	SREL	sa_self_serve_ session	REQUIRED
eventID	eventID	SREL	sa_event_history	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_self_serve_keyword Object

The object details are as follows:

1. Associated Table: sa_self_serve_keyword

2. Factories: default
3. REL_ATTR: id
4. Common Name: keyword
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
selfServe SessionID	selfServe SessionID	SREL	sa_self_serve_ session	REQUIRED
keyword	keyword	STRING 255		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_self_serve_login_field Object

The object details are as follows:

1. Associated Table: sa_self_serve_login_field
2. Factories: default
3. REL_ATTR: id
4. Common Name: value
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
selfServe SessionID	selfServe SessionID	SREL	sa_self_serve_ session	REQUIRED
fieldID	fieldID	SREL	sa_field	REQUIRED
value	value	STRING 500		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_self_serve_session Object

The object details are as follows:

1. Associated Table: sa_self_serve_session
2. Factories: default

3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sessionID	sessionID	SREL	sa_login_session	
userID	userID	SREL	cnt	REQUIRED
queueID	queueID	SREL	sa_queue	
categoryID	categoryID	SREL	sa_custom_ category	
createdEpoch	createdEpoch	LOCAL_TIME		
lastScript Epoch	lastScript Epoch	LOCAL_TIME		
scriptCount	scriptCount	INTEGER		REQUIRED
endEpoch	endEpoch	LOCAL_TIME		
Timezone	Timezone	INTEGER		
localizationID	localizationID	SREL	sa_localization	
associated SessionID	associated SessionID	SREL	sa_login_session	
isscat_rel	isscat_rel	SREL	isscat.code	
pcat_rel	pcat_rel	SREL	pcat.persistent_id	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Support Automation Static Content

This article contains the following topics:

sa_static_content Object

The object details are as follows:

1. Associated Table: sa_static_content
2. Factories: default
3. REL_ATTR: id

4. Common Name: GUID
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
GUID	GUID	STRING 255		
itemName	itemName	STRING 255		
itemDesc	itemDesc	STRING 255		
itemMimeType	itemMimeType	STRING 50		
version	version	INTEGER		
isLocked	isLocked	INTEGER		
itemContents	itemContents	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_static_cont_script_join Object

The object details are as follows:

1. Associated Table: sa_static_cont_script_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
scriptID	scriptID	SREL	sa_script	REQUIRED
itemID	itemID	SREL	sa_static_content	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Service Desk

This article contains the following topics:

sdsc Object

The object details are as follows:

1. Associated Table: Service_Desc
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: service_level
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
code	code	STRING		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
owning_contract	owning_contract	INTEGER	svc_contract id	
persistent_id	persid	STRING		
rank	rank	INTEGER		
schedule	schedule	STRING	bpwshft persid	
sym	sym	STRING		REQUIRED S_KEY
violation_cost	violation_cost	INTEGER		
tgttpls	tgttpls	BREL	tgt_tgttpls_srvtypes sdsc	

sdsc_map Object

The object details are as follows:

1. Associated Table: SLA_Contract_Map
2. Factories: default
3. REL_ATTR: id
4. Common Name: map_persid
5. Function Group: service_level

6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
map_contract	map_contract	INTEGER	svc_contract id	REQUIRED
map_persid	map_persid	STRING		
map_sdsc	map_sdsc	STRING	srv_desc code	
persistent_id	persid	STRING		

Session Objects

This topic contains the following information:

session_log Object

The object details are as follows:

1. Associated Table: session_log
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
contact	contact	UUID	ca_contact uuid	
id	id	INTEGER		UNIQUE REQUIRED KEY
login_time	login_time	LOCAL_TIME		
logout_time	logout_time	LOCAL_TIME		
policy	policy	INTEGER	sapolicy id	
session_id	session_id	INTEGER		
session_type	session_type	INTEGER	session_type id	
status	status	INTEGER		

session_type Object

The object details are as follows:

1. Associated Table: session_type
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
sym	sym	STRING		REQUIRED S_KEY

Server Objects

This article contains the following topics:

srvr_aliases Object

The object details are as follows:

1. Associated Table: Server_Aliases
2. Factories: default
3. REL_ATTR: id
4. Common Name: alias_name
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
alias_name	alias_name	STRING		REQUIRED
delete_flag	del	INTEGER	actbool enum	REQUIRED
host_addr	host_addr	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
zone_id	zone_id	INTEGER	srvr_zones id	REQUIRED

srvr_zones Object

The object details are as follows:

1. Associated Table: Server_Zones
2. Factories: default
3. REL_ATTR: id
4. Common Name: zone_name
5. Function Group: reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
is_default	is_default	INTEGER	bool_tab enum	
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
zone_name	zone_name	STRING		REQUIRED

Survey Objects

This article contains the following topics:

svy_qtpl Object

The object details are as follows:

1. Associated Table: Survey_Question_Template
2. Factories: default
3. REL_ATTR: id
4. Common Name: text
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
include_qcomment	include_qcomment	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
mult_resp_flag	mult_resp_flag	INTEGER		
owning_survey	owning_survey	INTEGER	survey_tpl id	
persistent_id	persid	STRING		
qcomment_label	qcomment_label	STRING		
resp_required	resp_required	INTEGER		
sequence	sequence	INTEGER		REQUIRED
text	txt	STRING		

svy_ques Object

The object details are as follows:

1. Associated Table: Survey_Question
2. Factories: default
3. REL_ATTR: id

4. Common Name: text
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
include_qcomment	include_qcomment	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
mult_resp_flag	mult_resp_flag	INTEGER		
owning_survey	owning_survey	INTEGER	survey id	
persistent_id	persid	STRING		
qcomment	qcomment	STRING		
qcomment_label	qcomment_label	STRING		
resp_required	resp_required	INTEGER		
response	response	INTEGER		REQUIRED
sequence	sequence	INTEGER		REQUIRED
text	txt	STRING		

svy_tpl Object

The object details are as follows:

1. Associated Table: Survey_Template
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
comment_label	comment_label	STRING		
Survey Completion Message	conclude_text	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
cycle_counter	cycle_counter	INTEGER		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
include_comment	include_comment	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
Submit Cycle	submit_cycle	INTEGER		
Survey Name	sym	STRING		UNIQUE REQUIRED S_KEY
tracking_flag	tracking_flag	INTEGER		
Survey Introduction	description	STRING		

svystat Object

The object details are as follows:

1. Associated Table: Survey_Stats
2. Factories: default
3. REL_ATTR: id
4. Common Name:
5. Function Group: admin

Attribute	DB Field	Data Type	SREL References	Flags
cyc_counter	cyc_counter	INTEGER		
cycle	cycle	INTEGER		
delete_flag	del	INTEGER	actbool enum	REQUIRED
eval_counter	eval_counter	INTEGER		
id	id	INTEGER		UNIQUE REQUIRED KEY
persistent_id	persid	STRING		
sub_counter	sub_counter	INTEGER		
tplid	tplid	INTEGER	survey_tpl id	

svy_atpl Object

The object details are as follows:

1. Associated Table: Survey_Answer_Template
2. Factories: default
3. REL_ATTR: id
4. Common Name: text
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
owning_ survey_ question	own_srvy_question	INTEGER	survey_qtpl id	
persistent_id	persid	STRING		
sequence	sequence	INTEGER		REQUIRED
text	txt	STRING		

svy_ans Object

The object details are as follows:

1. Associated Table: Survey_Answer
2. Factories: default
3. REL_ATTR: id
4. Common Name: text
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
				UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
owning_survey_question	own_srvy_question	INTEGER	survey_question id	
persistent_id	persid	STRING		
selected	selected	INTEGER		
sequence	sequence	INTEGER		REQUIRED
text	txt	STRING		

svytrk Object

The object details are as follows:

1. Associated Table: Survey_Tracking
2. Factories: default
3. REL_ATTR: id
4. Common Name: object_type
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
cntid	cntid	UUID	ca_contact uuid	
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
notif_dt	notif_dt	LOCAL_TIME		
object_id	object_id	INTEGER		
object_type	object_type	STRING		
persistent_id	persid	STRING		
recv_dt	recv_dt	LOCAL_TIME		
status	status	INTEGER		
tplid	tplid	INTEGER	survey_tpl id	

tgt_tgttpls_srvtypes Object

The object details are as follows:

1. Associated Table: target_tgttpls_srvtypes

2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: service_level
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	SREL	actbool.enum	REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id (http://cnt.id)	
tgt_time_tpl	tgt_time_tpl	SREL	tgt_time_tpl	REQUIRED
sdsc	sdsc	SREL	sdsc.code	REQUIRED
target_duration	target_duration	DURATION		REQUIRED

sa_survey Object

The object details are as follows:

1. Associated Table: sa_survey
2. Factories: default
3. REL_ATTR: id
4. Common Name: surveyName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
surveyName	surveyName	STRING 32		REQUIRED
question	question	STRING 512		REQUIRED
responseType	responseType	INTEGER		REQUIRED
isDeleted	isDeleted	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_survey_localized Object

The object details are as follows:

1. Associated Table: sa_survey_localized

2. Factories: default
3. REL_ATTR: id
4. Common Name: question
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
surveyID	surveyID	SREL	sa_survey	REQUIRED
localizationID	localizationID	SREL	sa_localization	REQUIRED
question	question	STRING 512		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_survey_result Object

The object details are as follows:

1. Associated Table: sa_survey_result
2. Factories: default
3. REL_ATTR: id
4. Common Name: SurveyComment
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
surveyID	surveyID	SREL	sa_survey	REQUIRED
selfServe SessionID	selfServe SessionID	SREL	sa_self_serve_ session	REQUIRED
scriptID	scriptID	SREL	sa_script	
response	response	INTEGER		
completion	completion	INTEGER		REQUIRED
SurveyComment	SurveyComment	STRING 512		
surveyEpoch	surveyEpoch	LOCAL_TIME		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

mgs Object

The object details are as follows:

1. Associated Table: Managed_Survey
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
open_date	create_date	LOCAL_TIME		
active	del	INTEGER	bool_tab enum	REQUIRED
close_date	end_date	LOCAL_TIME		
group	group_id	UUID		
id	id	INTEGER		UNIQUE REQUIRED KEY
initial_method	initial_method	INTEGER	ct_mth id	
initial_msgbody	initial_msgbody	STRING		
initial_msgtitle	initial_msgtitle	STRING		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
assignee	owner	UUID	ca_contact uuid	
persistent_id	persid	STRING		
reminder_method	reminder_method	INTEGER	ct_mth id	
reminder_ msgbody	reminder_ msgbody	STRING		
reminder_msgtitle	reminder_msgtitle	STRING		
start_dt	start_date	LOCAL_TIME		
status	status	STRING	mgsstat code	
sym	sym	STRING		UNIQUE REQUIRED S_KEY
tplid	tplid	INTEGER	survey_tpl id	

survey Object

The object details are as follows:

1. Associated Table: Survey

2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
comment_label	comment_label	STRING		
conclude_text	conclude_text	STRING		
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
include_comment	include_comment	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
comment	nx_comment	STRING		
object_id	object_id	INTEGER		
object_type	object_type	STRING		
persistent_id	persid	STRING		
sym	sym	STRING		S_KEY

Support

This topic contains the following information:

sa_group Object

The object details are as follows:

1. Associated Table: sa_group
2. Factories: default
3. REL_ATTR: id
4. Common Name: groupName

5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupName	groupName	STRING 100		
startEpoch	startEpoch	LOCAL_TIME		
endEpoch	endEpoch	LOCAL_TIME		
isCurrent	isCurrent	INTEGER		
owner SessionID	owner SessionID	SREL	sa_login_session	
status	status	INTEGER		
escalation Date	escalation Date	LOCAL_TIME		
creatorUser ID	creatorUser ID	SREL	cnt	
originalGroup ID	originalGroup ID	SREL	sa_group	
categoryID	categoryID	SREL	sa_custom_ category	
groupType	groupType	INTEGER		
sd_obj_type	sd_obj_type	STRING 10		
sd_obj_id	sd_obj_id	INTEGER		
cr_rel	cr_rel	SREL	cr.persistent_id	
iss_rel	iss_rel	SREL	iss.persistent_id	
user_route_ rel	user_route_ rel	SREL	sa_user_route.id (http://sa_user_route.id/)	
isscat_rel	isscat_rel	SREL	isscat.code	
pcat_rel	pcat_rel	SREL	pcat.persistent_id	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_group_current_user Object

The object details are as follows:

1. Associated Table: sa_group_current_user
2. Factories: default
3. REL_ATTR: id

4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_group	REQUIRED
sessionID	sessionID	SREL	sa_login_ session	REQUIRED
directedURL	directedURL	STRING 500		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_group_event_join Object

The object details are as follows:

1. Associated Table: sa_group_event_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_group	REQUIRED
eventID	eventID	SREL	sa_event_history	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_group_history Object

The object details are as follows:

1. Associated Table: sa_group_history
2. Factories: default
3. REL_ATTR: id
4. Common Name: id

5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_group	REQUIRED
startEpoch	startEpoch	LOCAL_TIME		REQUIRED
endEpoch	endEpoch	LOCAL_TIME		REQUIRED
sessionID	sessionID	SREL	sa_login_session	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_group_tool_invocation Object

The object details are as follows:

1. Associated Table: sa_group_tool_invocation
2. Factories: default
3. REL_ATTR: id
4. Common Name: toolStartTime
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_group	REQUIRED
toolID	toolID	SREL	sa_tool	REQUIRED
toolInstanceID	toolInstanceID	SREL	sa_tool_ instance	REQUIRED
toolStartEpoch	toolStartEpoch	LOCAL_TIME		REQUIRED
toolStartTime	toolStartTime	STRING 50		
toolInstance LogID	toolInstance LogID	SREL	sa_tool_ instance_log	
extraData	extraData	STRING 100		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Support Automation Agent

This topic contains the following information:

sa_agent_availability Object

The object details are as follows:

1. Associated Table: sa_agent_availability
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
agentID	agentID	SREL	cnt	REQUIRED
queueID	queueID	SREL	sa_queue	REQUIRED
status	status	INTEGER		
availEpoch	availEpoch	LOCAL_TIME		
clientSessionID	clientSessionID	SREL	sa_login_ session	
matchEpoch	matchEpoch	LOCAL_TIME		
groupID	groupID	INTEGER	ca_contact	NOT_NULL
incidentCount	incidentCount	INTEGER		
last_mod_by	last_mod_by	UUID	cnt	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_agent_consult_history Object

The object details are as follows:

1. Associated Table: sa_agent_consult_history
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		
userID	userID	SREL	cnt	REQUIRED
epoch	epoch	LOCAL_TIME		REQUIRED
groupID	groupID	SREL	sa_group	
type	type	INTEGER		
targetID	targetID	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_agent_present_history Object

The object details are as follows:

1. Associated Table: sa_agent_present_history
2. Factories: default
3. REL_ATTR: id
4. Common Name: eventTime
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		
agentSessionID	agentSessionID			REQUIRED
eventType	eventType	INTEGER		REQUIRED
eventEpoch	eventEpoch	LOCAL_TIME		REQUIRED
agentUserID	agentUserID	SREL	cnt	
eventTime	eventTime	STRING 50		
presentedItem Type	presentedItem Type	INTEGER		
presentedItemID	presentedItemID	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_agent_status_history Object

The object details are as follows:

1. Associated Table: sa_agent_status_history
2. Factories: default
3. REL_ATTR: id
4. Common Name: statusChangeTime
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		
agentSessionID	agentSessionID	SREL	sa_login_session	REQUIRED
newStatus	newStatus	INTEGER		REQUIRED
statusChange Epoch	statusChange Epoch	LOCAL_TIME		REQUIRED
statusChange Time	statusChange Time	STRING 50		
nextStatus ChangeEpoch	nextStatus ChangeEpoch	LOCAL_TIME		
nextStatus ChangeTime	nextStatus ChangeTime	STRING 50		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Support Automation Chat

This topic contains the following information:

sa_chat_preset Object

The object details are as follows:

1. Associated Table: sa_chat_preset
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
responseName	responseName	STRING 128		NOT_NULL
responseText	responseText	INTEGER		
responseTitle	responseTitle	STRING 128		
responseType	responseType	INTEGER	sa_chat_preset_ type	
categoryID	categoryID	INTEGER	sa_chat_preset_ category	NOT_NULL
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_chat_preset_agent_cat Object

The object details are as follows:

1. Associated Table: sa_chat_preset_agent_cat
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		
userID	userID	SREL	cnt	REQUIRED
groupID	groupID	SREL	sa_group	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_chat_preset_cat_loc Object

The object details are as follows:

1. Associated Table: sa_chat_preset_cat_loc
2. Factories: default
3. REL_ATTR: id
4. Common Name: name

5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_chat_preset_category	REQUIRED
localizationID	localizationID	SREL	sa_localization	REQUIRED
targetID	targetID	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenantq	UUID	ca_tenant	

sa_chat_preset_category Object

The object details are as follows:

1. Associated Table: sa_chat_preset_category
2. Factories: default
3. REL_ATTR: id
4. Common Name: groupName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		
userID	userID	SREL	cnt	REQUIRED
groupName	groupName	STRING 128		
lastUpdateDate	lastUpdateDate	LOCAL_TIME		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_chat_preset_localized Object

The object details are as follows:

1. Associated Table: sa_chat_preset_localized
2. Factories: default
3. REL_ATTR: id
4. Common Name: responseName

5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
responseID	responseID	SREL	sa_chat_preset	REQUIRED
localizationID	localizationID	SREL	sa_localization	REQUIRED
responseName	responseName	STRING		
responseText	responseText	INTEGER		
responseTitle	responseTitle	STRING		
responseLocal	responseLocal	LOCAL STRING		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_chat_preset_type Object

The object details are as follows:

1. Associated Table: sa_chat_preset_type
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		
enum	enum	INTEGER		NOT_NULL
sym	sym	STRING 20		NOT_NULL
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

Support Automation Direct

This topic contains the following information:

sa_division_login_script Object

The object details are as follows:

1. Associated Table: sa_division_login_script
2. Factories: default
3. REL_ATTR: id
4. Common Name: scriptName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
scriptText	scriptText	INTEGER		
scriptName	scriptName	STRING 128		
scriptDescription	scriptDescription	STRING 32768		
scriptLanguage	scriptLanguage	STRING 24		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_division_role_join Object

The object details are as follows:

1. Associated Table: sa_division_role_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
roleID	roleID	SREL	sa_role	REQUIRED
sessionID	sessionID	SREL	sa_login_ session	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_division_tool_join Object

The object details are as follows:

1. Associated Table: sa_division_tool_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
toolID	toolID	SREL	sa_tool	REQUIRED
enabled	enabled	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Support Automation Direct Session

This topic contains the following information:

sa_direct_session Object

The object details are as follows:

1. Associated Table: sa_direct_session
2. Factories: default
3. REL_ATTR: id
4. Common Name: code
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
code	code	STRING 100		REQUIRED
groupID	groupID	SREL	sa_group	
expired	expired	LOCAL_TIME		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

Attribute	DB Field	Data Type	SREL References	Flags
tenant	tenant	UUID	ca_tenant	

sa_direct_session_page Object

The object details are as follows:

1. Associated Table: sa_direct_session_page
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
stage	stage	INTEGER		REQUIRED
epoch	epoch	LOCAL_TIME		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_direct_session_preset Object

The object details are as follows:

1. Associated Table: sa_direct_session_preset
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
responseID	responseID	SREL	sa_chat_preset	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Support Automation Events

This topic contains the following information:

sa_event_history Object

The object details are as follows:

1. Associated Table: sa_event_history
2. Factories: default
3. REL_ATTR: id
4. Common Name: sd_obj_type
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
eventEpoch	eventEpoch	LOCAL_TIME		REQUIRED
eventType	eventType	SREL	sa_event_type	REQUIRED
sd_obj_type	sd_obj_type	STRING 10		
sd_obj_id	sd_obj_id	INTEGER		
cr_rel	cr_rel	SREL	Call_Req	
iss_rel	iss_rel	SREL	Issue	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_event_history_param Object

The object details are as follows:

1. Associated Table: sa_event_history_param
2. Factories: default
3. REL_ATTR: id
4. Common Name: paramValue
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
eventID	eventID	SREL	sa_event_ history	REQUIRED
paramID	paramID	SREL	sa_event_type_param	REQUIRED
paramValue	paramValu	STRING 4000		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_event_type Object

The object details are as follows:

1. Associated Table: sa_event_type
2. Factories: default
3. REL_ATTR: id
4. Common Name: displayTemplate
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
displayTemplate	displayTemplate	STRING 255		
eventDescription	eventDescription	STRING 50		
localizationID	localizationID	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

Support Automation Group

This topic contains the following information:

sa_group Object

The object details are as follows:

1. Associated Table: sa_group
2. Factories: default
3. REL_ATTR: id
4. Common Name: groupName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupName	groupName	STRING 100		
startEpoch	startEpoch	LOCAL_TIME		
endEpoch	endEpoch	LOCAL_TIME		
isCurrent	isCurrent	INTEGER		
owner SessionID	owner SessionID	SREL	sa_login_session	
status	status	INTEGER		
escalation Date	escalation Date	LOCAL_TIME		
creatorUser ID	creatorUser ID	SREL	cnt	
originalGroup ID	originalGroup ID	SREL	sa_group	
categoryID	categoryID	SREL	sa_custom_ category	
groupType	groupType	INTEGER		
sd_obj_type	sd_obj_type	STRING 10		
sd_obj_id	sd_obj_id	INTEGER		
cr_rel	cr_rel	SREL	cr.persistent_id	
iss_rel	iss_rel	SREL	iss.persistent_id	
user_route_ rel	user_route_ rel	SREL	sa_user_route.id (http://sa_user_route.id/)	
isscat_rel	isscat_rel	SREL	isscat.code	
pcat_rel	pcat_rel	SREL	pcat.persistent_id	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_group_current_user Object

The object details are as follows:

1. Associated Table: sa_group_current_user
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_group	REQUIRED
sessionID	sessionID	SREL	sa_login_ session	REQUIRED
directedURL	directedURL	STRING 500		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_group_event_join Object

The object details are as follows:

1. Associated Table: sa_group_event_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_group	REQUIRED
eventID	eventID	SREL	sa_event_history	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_group_history Object

The object details are as follows:

1. Associated Table: sa_group_history
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_group	REQUIRED
startEpoch	startEpoch	LOCAL_TIME		REQUIRED
endEpoch	endEpoch	LOCAL_TIME		REQUIRED
sessionID	sessionID	SREL	sa_login_session	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_group_tool_invocation Object

The object details are as follows:

1. Associated Table: sa_group_tool_invocation
2. Factories: default
3. REL_ATTR: id
4. Common Name: toolStartTime
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_group	REQUIRED
toolID	toolID	SREL	sa_tool	REQUIRED
toolInstanceID	toolInstanceID	SREL	sa_tool_ instance	REQUIRED
toolStartEpoch	toolStartEpoch	LOCAL_TIME		REQUIRED
toolStartTime	toolStartTime	STRING 50		

Attribute	DB Field	Data Type	SREL References	Flags
toolInstance LogID	toolInstance LogID	SREL	sa_tool_ instance_log	
extraData	extraData	STRING 100		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Support Automation Guest

This topic contains the following information:

sa_guest_agent_code Object

The object details are as follows:

1. Associated Table: sa_guest_agent_code
2. Factories: default
3. REL_ATTR: id
4. Common Name: agentCode
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
agentCode	agentCode	STRING 5		REQUIRED
groupID	groupID	SREL	sa_group	
createdEpoch	createdEpoch	LOCAL_TIME		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_guest_profile Object

The object details are as follows:

1. Associated Table: sa_guest_profile
2. Factories: default
3. REL_ATTR: id

4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sessionID	sessionID	SREL	sa_login_session	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_guest_user_field Object

The object details are as follows:

1. Associated Table: sa_guest_user_field
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
fieldID	fieldID	SREL	sa_field	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Support Automation Milepost

This topic contains the following information:

sa_milepost Object

The object details are as follows:

1. Associated Table: sa_milepost
2. Factories: default

3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sessionID	sessionID	SREL	sa_login_session	REQUIRED
milepost	milepost	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_milepost_history Object

The object details are as follows:

1. Associated Table: sa_milepost_history
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sessionID	sessionID	SREL	sa_login_session	REQUIRED
milepost	milepost	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Support Automation Queue

This topic contains the following information:

- sa_queue_summary_field Object (see page 4680)
- sa_queue_tool_join Object (see page 4681)

sa_queue_transfer_target Object

The object details are as follows:

1. Associated Table: sa_queue_transfer_target
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
roleID	roleID	SREl	sa_role	REQUIRED
queueID	queueID	SREL	sa_queue	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_queued_group Object

The object details are as follows:

1. Associated Table: sa_queued_group
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
queueID	queueID	SREL	sa_queue	REQUIRED
groupID	groupID	SREL	sa_group	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_queued_user

The object details are as follows:

1. Associated Table: sa_queued_user
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
queueID	queueID	SREL	sa_queue	REQUIRED
sessionID	sessionID	SREL	sa_login_session	REQUIRED
entryEpoch	entryEpoch	LOCAL_TIME		
status	status	INTEGER		
user_route_rel	user_route_rel	SREL	sa_user_route	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_queue Object

The object details are as follows:

1. Associated Table: sa_queue
2. Factories: default
3. REL_ATTR: id
4. Common Name: queueName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
queueName	queueName	STRING 100		REQUIRED
isDefault	isDefault	SREL	bool.enum	
isActive	isActive	SREL	actrbool.enum	
enableAuto Matching	enableAuto Matching	INTEGER		

enableAuto Escalation	enableAuto Escalation	INTEGER		
escalation Timeout	escalation Timeout	INTEGER		
escalation TargetQueue	escalation TargetQueue	SREL	sa_queue	
customer DisplayName	customer DisplayName	STRING 100		REQUIRED
onDeck Priority	onDeck Priority	INTEGER		
categoryID	categoryID	SREL	sa_custom_ category	
responseID	responseID	SREL	sa_chat_preset	
isscat_rel	isscat_rel	SREL	isscat.code	
pcat_rel	pcat_rel	SREL	pcat.persistent_id	
cr_template	cr_template	SREL	cr.persistent_id	
iss_template	iss_template	SREL	iss.persistent_id	
workshift	workshift	SREL	wrkshft.persistent_ id	
is_special	is_special	SREL	bool.enum	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIM E		

sa_queue_hour_setting Object

The object details are as follows:

1. Associated Table: sa_queue_hour_setting
2. Factories: default
3. REL_ATTR: id
4. Common Name: url
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
queueID	queueID	SREL	sa_queue	REQUIRED
url	url	STRING 2048		
isExternal	isExternal	INTEGER		
useHours	useHours	SREL	sa_hour_ operation_mode	
last_mod_by	last_mod_by	UUID	ca_contact	

last_mod_dt	last_mod_dt	LOCAL_TIME	
tenant	tenant	UUID	ca_tenant

sa_queue_localized Object

The object details are as follows:

1. Associated Table: sa_queue_localized
2. Factories: default
3. REL_ATTR: id
4. Common Name: customerDisplayName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
queueID	queueID	SREL	sa_queue	REQUIRED
localizationID	localizationID	SREL	sa_localization	REQUIRED
customer DisplayName	customer DisplayName	STRING 100		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_queue_summary_field Object

The object details are as follows:

1. Associated Table: sa_queue_summary_field
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
fieldID	fieldID	SREL	sa_field	REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
fieldOrder	fieldOrder	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_queue_tool_join Object

The object details are as follows:

1. Associated Table: sa_queue_tool_join
2. Factories: default
3. REL_ATTR: id

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
queueID	queueID	SREL	sa_queue	REQUIRED
toolID	toolID	SREL	sa_tool	
displayOrder	displayOrder	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Support Automation Role

This topic contains the following information:

sa_role Object

The object details are as follows:

1. Associated Table: sa_role
2. Factories: default
3. REL_ATTR: id
4. Common Name: roleName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
roleName	roleName	STRING 100		
isAgent	isAgent	INTEGER		
default SecurityGroup	default SecurityGroup	SREL	sa_security_ group	
joinSession	joinSession	INTEGER		
allowSecLevel Change	allowSecLevel Change	INTEGER		
isActive	isActive	SREL	actrbool.enum	
onDeck	onDeck	INTEGER		
allow_script_ide	allow_script_ide	INTEGER		
sa_client_ launch_node	sa_client_ launch_node	INTEGER		
description	description	STRING 1024		
queues	queues	BREL	sa_role_ queue_join	
target_queues	target_queues	BREL	sa_queue_transfer _target	
security_grps	security_grps	BREL	sa_security_grp_ role_join	
tools_non_art	tools_non_art	BREL	sa_role_tool_non_ art	
assigned_ scripts	assigned_ scripts	BREL	sa_script_role_join	
last_mod_dt	last_mod_dt	LOCAL_TIME		
last_mod_by	last_mod_by	UUID	ca_contact	

sa_role_queue_join Object

The object details are as follows:

1. Associated Table: sa_role_queue_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
roleID	roleID	SREL	sa_role	REQUIRED
queueID	queueID	SREL	sa_queue	REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
isDefault	isDefault	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_role_tool_join Object

The object details are as follows:

1. Associated Table: sa_role_tool_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
roleID	roleID	SREL	sa_role	REQUIRED
toolID	toolID	SREL	sa_tool	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_role_tool_non_art_join Object

The object details are as follows:

1. Associated Table: sa_role_tool_non_art_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
roleID	roleID	SREL	sa_role	REQUIRED
toolID	toolID	SREL	sa_tool_non_art	REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

Support Automation Script

This topic contains the following information:

sa_script Object

The object details are as follows:

1. Associated Table: sa_script
2. Factories: default
3. REL_ATTR: id
4. Common Name: scriptName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
scriptText	scriptText	INTEGER		
scriptName	scriptName	STRING 128		
script Description	script Description	STRING 2000		
isLocked	isLocked	INTEGER		
version	version	INTEGER		
GUID	GUID	STRING 255		
credLogin	credLogin	STRING 50		

Attribute	DB Field	Data Type	SREL References	Flags
credPswd	credPswd	STRING 255		
credPswdPlain	credPswdPlain	LOCAL STRING		
credDomain	credDomain	STRING 50		
impersonate	impersonate	INTEGER		
credentials Type	credentials Type	INTEGER		
disclaimer	disclaimer	SREl	sa_disclaimer	
surveyID	surveyID	SREL	sa_survey	
percentShown	percentShown	INTEGER		
loginRequired	loginRequired	INTEGER		
restrict Functions	restrict Functions	iNTEGER		
scriptTimeout	scriptTimeout	INTEGER		
wsEnabled	wsEnabled	INTEGER		
groupID	groupID	SREL	sa_script_group	REQUIRED
securityFunctions	securityFunctions	BREL	sa_script_ security_join	
assigned_roles	BREL	BREL	sa_script_role_ join	
last_mod_dt	last_mod_dt	LOCAL_TIME		
last_mod_by	last_mod_by	UUID	ca_contact	
tenant	tenant	UUID	ca_tenant	

sa_script_acquired_data Object

The object details are as follows:

1. Associated Table: sa_script_acquired_data
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sessionID	sessionID	SREL	sa_login_session	REQUIRED
scriptID	scriptID	SREL	sa_script	REQUIRED
scriptInstance ID	scriptInstance ID	SREL	sa_script_ execution_log	REQUIRED
epoch	epoch	LOCAL_TIME		REQUIRED
acquiredData	acquiredData	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_script_exec_log_join Object

The object details are as follows:

1. Associated Table: sa_role_tool_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
scriptInstanceID	scriptInstanceID	SREL	sa_script_ execution	REQUIRED
eventID	eventID	SREL	sa_event_ history	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_script_exec_status Object

The object details are as follows:

1. Associated Table: sa_script_exec_status
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
eventID	eventID	SREL	sa_event_history	REQUIRED
scriptID	scriptID	SREL	sa_script	REQUIRED
executedStatus	executedStatus	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

Attribute	DB Field	Data Type	SREL References	Flags
tenant	tenant	UUID	ca_tenant	

sa_script_execution_log Object

The object details are as follows:

1. Associated Table: sa_script_execution_log
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
scriptID	scriptID	SREL	sa_script	REQUIRED
selfServe SessionID	selfServe SessionID	SREl	sa_self_serve_ session	REQUIRED
sessionID	sessionID	SREL	sa_login_session	
executedEpoch	executedEpoch	LOCAL_TIME		REQUIRED
surveyShown	surveyShown	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_script_function_lib Object

The object details are as follows:

1. Associated Table: sa_script_function_lib
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
scriptID	scriptID	SREL	sa_script	REQUIRED
libID	libID	SREL	sa_scriptlib	REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_script_group Object

The object details are as follows:

1. Associated Table: sa_script_group
2. Factories: default
3. REL_ATTR: id
4. Common Name: groupName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupName	groupName	STRING 128		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_script_role_join Object

The object details are as follows:

1. Associated Table: sa_script_role_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
scriptID	scriptID	SREL	sa_script	REQUIRED
roleID	roleID	SREL	sa_role	REQUIRED
autorun	autorun	SREL	bool.enum	

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_script_security_join Object

The object details are as follows:

1. Associated Table: sa_script_security_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
scriptID	scriptID	SREL	sa_script	REQUIRED
functionID	functionID	SREL	sa_security_ tool_function	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_script_user_field Object

The object details are as follows:

1. Associated Table: sa_script_user_field
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
fieldID	fieldID	SREL	sa_field	REQUIRED
scriptID	scriptID	SREL	sa_script	REQUIRED

Attribute	DB Field	Data Type	SREL References	Flags
isProfileField	isProfileField	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_scriptlib Object

The object details are as follows:

1. Associated Table: sa_scriptlib
2. Factories: default
3. REL_ATTR: id
4. Common Name: libName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
libName	libName	STRING 128		REQUIRED
libLang	libLang	SREL	sa_scriptlib_ language	REQUIRED
active	active	INTEGER		REQUIRED
GUID	GUID	STRING 255		
version	version	INTEGER		REQUIRED
isLocked	isLocked	INTEGER		
description	description	STRING 1024		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_scriptlib_language Object

The object details are as follows:

1. Associated Table: sa_scriptlib_language
2. Factories: default
3. REL_ATTR: enum
4. Common Name: sym
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		
sym	sym	STRING 30		REQUIRED
enum	enum	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		

Support Automation Session

This topic contains the following information:

sa_session_event_join Object

The object details are as follows:

1. Associated Table: sa_session_event_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sessionID	sessionID	SREL	sa_login_session	REQUIRED
eventID	eventID	SREL	sa_event_history	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_session_login_field Object

The object details are as follows:

1. Associated Table: sa_session_login_field
2. Factories: default
3. REL_ATTR: id

4. Common Name: value
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sessionID	sessionID	SREL	sa_login_session	REQUIRED
fieldID	fieldID	SREL	sa_field	REQUIRED
value	value	STRING 500		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_session_security_info Object

The object details are as follows:

1. Associated Table: sa_session_security_info
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sessionID	sessionID	SREL	sa_login_session	REQUIRED
folderAccess Bit	folderAccess Bit	INTEGER		
securityLevel ID	securityLevel ID	SREL	sa_security_ group	
hasCustom	hasCustom	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Support Automation Tool

This topic contains the following information:

sa_tool Object

The object details are as follows:

1. Associated Table: sa_tool
2. Factories: default
3. REL_ATTR: id
4. Common Name: toolName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
toolName	toolName	STRING 100		
URL	URL	STRING 255		
suggestion	suggestion	INTEGER		
imageName	imageName	STRING 255		
displayURL	displayURL	STRING 255		
width	width	INTEGER		
height	height	INTEGER		
toolType	toolType	INTEGER		
useViewport	useViewport	INTEGER		
agentDefault	agentDefault	INTEGER		
isAdmin	isAdmin	INTEGER		
isSpecial	isSpecial	INTEGER		
localizationID	localizationID	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_tool_inst_log_evt_join Object

The object details are as follows:

1. Associated Table: sa_tool_inst_log_evt_join

2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
toolInstance LogID	toolInstance LogID	SREL	sa_tool_instance_ log	REQUIRED
eventID	eventID	SREL	sa_event_history	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_tool_instance Object

The object details are as follows:

1. Associated Table: sa_tool_instance
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_group	REQUIRED
toolInstanceID	toolInstanceID	INTEGER		REQUIRED
toolID	toolID	SREL	sa_tool	
toolInstanceLog ID	toolInstanceLog ID	SREL	sa_tool_instance_ log	
lastUpdated	lastUpdated	LOCAL_TIME		
writeLockID	writeLockID	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_tool_instance_log Object

The object details are as follows:

1. Associated Table: sa_tool_instance_log
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
groupID	groupID	SREL	sa_group	
toolID	toolID	SREL	sa_tool	
startEpoch	startEpoch	LOCAL_TIME		
endEpoch	endEpoch	LOCAL_TIME		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_tool_log Object

The object details are as follows:

1. Associated Table: sa_tool_log
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
toolID	toolID	SREL	sa_tool	REQUIRED
logStart	logStart	LOCAL_TIME		
logEnd	logEnd	LOCAL_TIME		
toolData	toolData	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_tool_log_message Object

The object details are as follows:

1. Associated Table: sa_tool_log_message
2. Factories: default
3. REL_ATTR: id
4. Common Name: logMessage
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
toolID	toolID	SREL	sa_tool	REQUIRED
logMessage	logMessage	STRING 300		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_tool_module Object

The object details are as follows:

1. Associated Table: sa_tool_module
2. Factories: default
3. REL_ATTR: id
4. Common Name: moduleLocation
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
toolID	toolID	SREL	sa_tool	REQUIRED
seqID	seqID	INTEGER		REQUIRED
module Location	module Location	STRING 512		
agentModule Name	agentModule Name	STRING 255		REQUIRED
delayLoading	delayLoading	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_tool_name_localized Object

The object details are as follows:

1. Associated Table: sa_tool_name_localized
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
toolID	toolID	SREL	sa_tool	REQUIRED
localizationID	localizationID	SREL	sa_localization	REQUIRED
name	name	STRING 200		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_tool_non_art Object

The object details are as follows:

1. Associated Table: sa_tool_non_art
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
sym	sym	STRING 100		
art_pos	art_pos	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

sa_tool_property Object

The object details are as follows:

1. Associated Table: sa_tool_property

2. Factories: default
3. REL_ATTR: id
4. Common Name: value
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
toolID	toolID	SREL	sa_tool	REQUIRED
propertyID	propertyID	SREL	sa_property	REQUIRED
value	value	STRING 100		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_tool_start_message Object

The object details are as follows:

1. Associated Table: sa_tool_start_message
2. Factories: default
3. REL_ATTR: id
4. Common Name: toolStartMessage
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
toolID	toolID	SREL	sa_tool	REQUIRED
showMessage	showMessage	INTEGER		REQUIRED
toolStart Message	toolStart Message	STRING 200		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_tool_version Object

The object details are as follows:

1. Associated Table: sa_tool_version

2. Factories: default
3. REL_ATTR: id
4. Common Name: moduleName
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
localizationID	localizationID	SREL	sa_localization	REQUIRED
moduleName	moduleName	STRING 100		REQUIRED
moduleVersion	moduleVersion	STRING 30		
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

Support Automation User

This topic contains the following information:

sa_tenant_localization Object

The object details are as follows:

1. Associated Table: sa_tenant_localization
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
localizationID	localizationID	SREL	sa_localization	REQUIRED
enabled	enabled	SREL	bool.enum	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		

Attribute	DB Field	Data Type	SREL References	Flags
tenant	tenant	UUID	ca_tenant	

sa_user_alert_config Object

The object details are as follows:

1. Associated Table: sa_user_alert_config
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
userID	userID	SREL	cnt	REQUIRED
AlertType	AlertType	INTEGER		REQUIRED
AlertTrigger	AlertTrigger	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_user_route Object

The object details are as follows:

1. Associated Table: sa_user_route
2. Factories: default
3. REL_ATTR: id
4. Func Group: sa
5. Common Name: sd_obj_type
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
userID	userID	SREL	cnt	
queue_id	queue_id	SREL	sa_queue	

Attribute	DB Field	Data Type	SREL References	Flags
login_session_id	login_session_ id	SREL	sa_login_session	
launch_type	launch_type	INTEGER		
sd_obj_type	sd_obj_type	STRING 10		
sd_obj_id	sd_obj_id	INTEGER		
cr	cr	SREL	Call_Req	
iss	iss	SREL	Issue	
user_description	user_description	STRING 4000		
sdm_web_addrs	sdm_web_addrs	STRING 255		
isscat_rel	isscat_rel	SREL	Issue_Category	
pcat_rel	pcat_rel	SREL	Prob_Category	
category	category	LOCAL STRING		
priority	priority	SREL	Priority	
properties		BREL	sa_user_route_ prop	
add_property_ persids		LOCAL STRING		
direct_session_ code		LOCAL STRING		
summary		LOCAL STRING		
localizationID		LOCAL SREL	sa_localization	
endUserID	endUserID	LOCAL SREL	cnt	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

sa_user_route_prop Object

The object details are as follows:

1. Associated Table: sa_user_route_prop
2. Factories: default
3. REL_ATTR: id
4. Func Name: sa
5. Common Name: description
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
login_session_id	login_session_id	SREL	sa_login_session	
self_serve_ session_id	self_serve_ session_id	SREL	sa_self_serve_ session	
user_route	user_route	SREL	sa_user_route	
sequence	sequence	INTEGER		REQUIRED
description	description	STRING 1024		
label	label	STRING 256		REQUIRED
value	value	STRING 128		
required	required	INTEGER		
sample	sample	STRING 128		
validation_rule	validation_rule	SREL	prpval_rule	
validation_type	validation_type	SREL	prpval_type	
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIM E		
tenant	tenant	UUID	ca_tenant	

sa_userdrserver_join Object

The object details are as follows:

1. Associated Table: sa_userdrserver_join
2. Factories: default
3. REL_ATTR: id
4. Common Name: id
5. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE NOT_NULL KEY
userID	userID	SREL	cnt	REQUIRED
drServerID	drServerID	SREL	sa_data_routing_ server	REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact	
last_mod_dt	last_mod_dt	LOCAL_TIME		
tenant	tenant	UUID	ca_tenant	

Task Objects

This article contains the following topics:

tskstat Object

The object details are as follows:

1. Associated Table: Task_Status
2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
allow_accumulate	allow_accumulate	INTEGER		REQUIRED
allow_task_update	allow_task_update	INTEGER		REQUIRED
code	code	STRING		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
do_next_task	do_next_task	INTEGER		REQUIRED
hold	hold	INTEGER		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
is_internal	is_internal	INTEGER		REQUIRED
last_mod_by	last_mod_by	UUID	ca_contact uuid	
modified_date	last_mod_dt	LOCAL_TIME		
no_update_msg	no_update_msg	STRING		
persistent_id	persid	STRING		
sym	sym	STRING		REQUIRED
task_complete	task_complete	INTEGER		REQUIRED

tskty Object

The object details are as follows:

1. Associated Table: Task_Type

2. Factories: default
3. REL_ATTR: code
4. Common Name: sym
5. Function Group: workflow_reference
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
code	code	STRING		UNIQUE REQUIRED S_KEY
delete_flag	del	INTEGER	actbool enum	REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
modified_date	last_mod_dt	LOCAL_TIME		
persistent_id	persid	STRING		
sym	sym	STRING		REQUIRED S_KEY

Target Time

This topic contains the following information:

tgt_time Object

The object details are as follows:

1. Associated Table: target_time
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: service_level
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	INTEGER	actbool	REQUIRED
sym	sym	STRING 60		REQUIRED
last_mod_dt	last_mod_dt	DATE		
last_mod_by	last_mod_by	SREL	cnt.id (http://cnt.id)	

Attribute	DB Field	Data Type	SREL References	Flags
target_duration	target_duration	DURATION		REQUIRED
condition	condition	SREL	macro.persistent	
condition_ outcome	condition_ outcome	SREL	true_false.enum	
service_type	service_type	STRING	sdsc.code	REQUIRED
object_type	object_type	STRING	event_prod_list. sym	REQUIRED
object_id	object_id	INTEGER		REQUIRED
set_actual	set_actual	SREL	bool.enum	
reset_actual	reset_actual	SREL	bool.enum	
lock_target	lock_target	SREL	bool.enum	
cost	cost	STRING 255		
target_time	target_time	DATE		
actual_time	actual_time	DATE		
time_left	time_left	DURATION		
work_shift	work_shift	SREL	wrkshft.persistent_id	
_mapped_cr	_mapped_cr	SREL	cr.persistent_id	
_mapped_chg	_mapped_chg	SREL	chg.persistent_id	
_mapped_iss	_mapped_iss	SREL	iss.persistent_id	
target_tpl	target_tpl	SREL	tgt_time_tpl.id (http://tgt_time_tpl.id)	
suppress_log	INTEGER			

tgt_time_tpl Object

The object details are as follows:

1. Associated Table: target_time_tpl
2. Factories: default
3. REL_ATTR: id
4. Common Name: sym
5. Function Group: service_level
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
delete_flag	del	SREL	actbool.enum	REQUIRED
sym	sym	STRING 60		REQUIRED
last_mod_dt	last_mod_dt	DATE		

Attribute	DB Field	Data Type	SREL References	Flags
last_mod_by	last_mod_by	SREL	cnt.id (http://cnt.id)	
target_duration	target_duration	DURATION		REQUIRED
condition	condition	SREL	macro.persistent_id	
condition_outcome	condition_outcome	SREL	true_false.enum	
object_type	object_type	SREL	event_prod_list.sym	REQUIRED
set_actual	set_actual	SREL	bool.enum	
reset_actual	reset_actual	SREL	bool.enum	
cost	cost	STRING 255		
work_shift	work_shift	SREL	wrkshft.persistent_id	
srvtypes	srvtypes	BREL	tgt_tgttpls_srvtypes.tgt_time_tpl	

Tenant Objects

This topic contains the following information:

tenant Object

The object details are as follows:

Associated Table: ca_tenant

Factories: default

REL_ATTR: id

Common Name: name

Function Group: tenant_admin

REST Operations: CREATE READ UPDATE

Attributes	Data Type	SREL References	Flags
id	UUID		
producer_id	STRING 20		
persistent_id	STRING 60		
name	STRING 255		
tenant_ number	STRING 30		
service_provider	INTEGER		
contact	SREL	cnt.id (http://cnt.id)	

Attributes	Data Type	SREL References	Flags
logo	STRING 255		
description	STRING 1024		
phone_number	STRING 255		
fax_number	STRING 255		
alt_phone	STRING 255		
location	SREL	loc.id (http://loc.id)	
delete_flag	SREL	actbool.enum	
version_number	INTEGER		
creation_user	STRING 64		
creation_date	LOCAL_ TIME		
last_update_user	LOCAL_ TIME		
last_update_date	LOCAL_ TIME		
ldap_tenant_group	SREL	ldap_group.id (http://ldap_group.id)	
groups	BREL	tgm_groups. tenant_id	
tenant	SREL	tenant.id (http://tenant.id)	REQUIRED
terms_of_usage	SREL	ca_tou	

tenant_group Object

The object details are as follows:

Associated Table: ca_tenant_group

Factories: default

REL_ATTR: id

Common Name: name

Function Group: admin

REST Operations: CREATE READ UPDATE

Attributes	Data Type	SREL References	Flags
id	UUID		
producer_id	STRING 20		
persistent_id	STRING 60		
name	STRING 255		

Attributes	Data Type	SREL References	Flags
description	STRING 1024		
delete_flag	SREL	actbool.enum	
version_number	INTEGER		
creation_user	STRING 64		
creation_date	LOCAL_ TIME		
last_update_user	STRING 64		
last_update_date	LOCAL_TIME		
members	BREL	tgm_members. tenant_group	

tenant_group_member Object

The object details are as follows:

Associated Table: ca_tenant_group_member

Factories: default

REL_ATTR: persistent_id

Common Name: creation_user

Function Group: admin

REST Operations: CREATE READ UPDATE

Attributes	Data Type	SREL References	Flags
id	UUID		
producer_id	STRING 20		
persistent_id	STRING 60		
tenant_id	SREL	tenant.id (http://tenant.id)	
tenant_group	SREL	tenant_group. id	
creation_date	LOCAL_ TIME		
creation_user	STRING 64		
tenant	SREL	tenant.id (http://tenant.id)	REQUIRED

Web Form

This article contains the following topics:

web_form Object

The object details are as follows:

1. Associated Table: usp_web_form
2. Factories: default
3. REL_ATTR: id
4. Common Name: name
5. Function Group: Security
6. REST Operations: CREATE READ UPDATE

Attribute Name	Data Type	Relationship Object	Flags
id	INTEGER		UNIQUE
name	STRING		REQUIRED
code	STRING		UNIQUE; REQUIRED
delete_flag	SREL	actbool	REQUIRED
description	STRING		
resource	STRING		
wf_type	INTEGER		
dflt_for_obj	STRING		
last_mod_by	SREL	cnt	
last_mod_dt	DATE		

web_form_pref Object

The object details are as follows:

1. Associated Table: usp_web_form_pref
2. Factories: default
3. REL_ATTR: id
4. Common Name: frame_name
5. Function Group: Reference
6. REST Operations: CREATE READ UPDATE

Attribute Name	Data Type	Relationship Object	Flags
id	INTEGER		UNIQUE
contact	SREL	cnt	
web_form_obj	SREL	web_form	
role_tab_obj	SREL	role_tab	
frame_name	STRING		
last_mod_dt	DATE		

Web Screen Painter Objects

This topic contains the following information:

wspcol Object

The object details are as follows:

1. Associated Table: wspcol
2. Factories: default
3. REL_ATTR: id
4. Common Name: column_name
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
addl_info	addl_info	STRING		
column_name	column_name	STRING		REQUIRED
dbms_name	dbms_name	STRING		
display_name	display_name	STRING		
id	id	INTEGER		UNIQUE REQUIRED KEY
is_cluster	is_cluster	INTEGER		
is_descending	is_descending	INTEGER		
is_indexed	is_indexed	INTEGER		
is_local	is_local	INTEGER		
is_REQUIRED	is_REQUIRED	INTEGER		

Attribute	DB Field	Data Type	SREL References	Flags
is_order_by	is_order_by	INTEGER		
is_required	is_required	INTEGER		
is_skey	is_skey	INTEGER		
is_unique	is_unique	INTEGER		
is_write_new	is_write_new	INTEGER		
is_wsp	is_wsp	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
on_ci_set	on_ci_set	STRING		
on_new_default	on_new_default	STRING		
persistent_id	persid	STRING		
schema_name	schema_name	STRING		
status	status	INTEGER		REQUIRED
string_len	string_len	INTEGER		
table_name	table_name	STRING		REQUIRED
type	type	INTEGER		
xrel_table	xrel_table	STRING		

wsptbl Object

The object details are as follows:

1. Associated Table: wsptbl
2. Factories: default
3. REL_ATTR: id
4. Common Name: table_name
5. Function Group: admin
6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
common_name	common_name	STRING		
dbms_name	dbms_name	STRING		
display_group	display_group	STRING		
display_name	display_name	STRING		
function_group	function_group	STRING		

Attribute	DB Field	Data Type	SREL References	Flags
id	id	INTEGER		UNIQUE REQUIRED KEY
is_local	is_local	INTEGER		
is_wsp	is_wsp	INTEGER		
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_TIME		
methods	methods	STRING		
persistent_id	persid	STRING		
rel_attr	rel_attr	STRING		
schema_name	schema_name	STRING		
sort_by	sort_by	STRING		
status	status	INTEGER		REQUIRED
table_name	table_name	STRING		REQUIRED
triggers	triggers	STRING		

Workflow Objects

This topic contains the following information:

wf Object

The object details are as follows:

1. Associated Table: Workflow_Task
2. Factories: default
3. REL_ATTR: id
4. Common Name: description
5. Function Group: change_mgr
6. REST Operations: CREATE READ UPDATE DELETE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
actual_duration	actual_duration	DURATION		
asset	asset	UUID	ca_owned_ resource uuid	
assignee	assignee	UUID	ca_contact uuid	
completion_ date				

Attribute	DB Field	Data Type	SREL References	Flags
	completion_ date	LOCAL_ TIME		
comments	comments	STRING		
cost	cost	INTEGER		
creator	creator	UUID	ca_contact uuid	
date_created	date_created	LOCAL_ TIME		
delete_flag	del	INTEGER	actbool enum	REQUIRED
done_by	done_by	UUID	ca_contact uuid	
est_completion_dat e	est_comp_date	LOCAL_ TIME		
est_cost	est_cost	INTEGER		
est_duration	est_duration	DURATION		
group	group_id	UUID		
group_task	group_task	INTEGER		REQUIRED
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
last_mod_dt	last_mod_dt	LOCAL_ TIME		
chg	object_id	INTEGER	chg id	REQUIRED
object_type	object_type	STRING		REQUIRED
persistent_id	persid	STRING		
sequence	sequence	INTEGER		REQUIRED
start_date	start_date	LOCAL_ TIME		
status	status	STRING	tskstat code	
support_lev	support_lev	STRING	srv_desc code	
task	task	STRING	tskty code	REQUIRED
wf_template	wf_template	INTEGER	wftpl id	

wftpl Object

The object details are as follows:

1. Associated Table: Workflow_Task_Template
2. Factories: default
3. REL_ATTR: id
4. Common Name: id

5. Function Group: workflow_reference

6. REST Operations: CREATE READ UPDATE

Attribute	DB Field	Data Type	SREL References	Flags
description	description	STRING		
assignee	assignee	UUID	ca_contact uuid	
auto_assign	auto_assign	INTEGER		
delete_flag	del	INTEGER	actbool enum	REQUIRED
deleteable	deleteable	INTEGER		REQUIRED
est_cost	est_cost	INTEGER		
est_duration	est_duration	DURATION		
group	group_id	UUID		
id	id	INTEGER		UNIQUE REQUIRED KEY
last_mod_by	last_mod_by	UUID	ca_contact uuid	
modified_date	last_mod_dt	LOCAL_TIME		
object_attrname	object_attrname	STRING		REQUIRED
object_attrval	object_attrval	INTEGER		REQUIRED
object_type	object_type	STRING		REQUIRED
persistent_id	persid	STRING		
sequence	sequence	INTEGER		REQUIRED
service_type	service_type	STRING	srv_desc code	
task	task	STRING	tskty code	REQUIRED

CA Service Catalog Glossary

accounts

Accounts are part of a business unit. Accounts are used to subscribe and request services. Charges are applied at the account level in Service Accounting Component.

action

An *action* is the smallest unit of work in the Rule Management Engine. This task is executed when a rule gets notified. Examples include sending an email, running a script, and running Java code.

Activity Based Costing (ABC)

Activity Based Costing is a costing methodology that is used to trace overhead costs directly to cost objects. The cost objects can be products, processes, services, or customers. This costing methodology helps managers to make the right decisions regarding product mix and competitive strategies.

Activity Based Management (ABM)

Activity Based Management uses Activity Based Cost information to allocate resources more effectively during budgeting and planning processes.

adjustments

Adjustments are credits or debits applied to services, individual charges of a Service Option Group, and SLA violations. These adjustments are either a fixed dollar amount or a percentage. Several types of general and SLA violation adjustments are available.

batch print job

A *batch print job* is a collection of invoices that have been grouped according to the specified credentials. After the collection has been created, it remains unchanged. The invoices can then be printed as a whole or individually at any time.

business unit

The *business unit* is a branch in the organizational structure. This organizational unit has some characteristics of the service provider and all characteristics of a sub-department.

CA Embedded Entitlements Manager (CA EEM)

CA Embedded Entitlements Manager provides enterprises with the ability to manage the identities of their employees, partners, and customers. CA EEM can also provision web services, and applications to the users, and define authentication and authorization policies.

cost allocation

Cost allocation is a method to determine the cost of services that are provided to users of that service. This method does not determine the price of the service, but rather it determines the cost of providing the service.

cost element

A *cost element* is a resource that is used to subdivide costs corresponding to the consumption of a particular service. Cost Element is the amount that is paid for a resource that an activity consumes and included in the activity cost pool. Such information helps validating that the overhead calculated at the beginning of the process is the same as the overhead that is assigned to each individual product using ABC.

cost pool

A *cost pool* is a grouping of all cost elements that are associated with an activity.

Dashboard Library

A *Dashboard Library* is a hierarchical tree structure of name spaces facilitating the sharing of information. The Dashboard Library does not hold actual data. Instead, it stores information about how the data can be accessed.

data collector (DC)

A *data collector* collects data for particular metrics.

data mediation profile

The *data mediation profile* is a definition of the data feed and structure of the external data. Data Mediation Profile also provides features to manipulate and normalize usage event data.

data object

A *data object* defines the data for a chart or table. The data object source can be a SQL database, comma-separated file, or any data source that a Java plug-in can access. Data objects are managed in folders to help categorize them by purpose.

data view

A *data view* formats the data that a data object produces. Data can be presented in tabular or chart format or both. Data views are managed in folders to help categorize them by purpose.

direct costs

Direct costs are those costs that can be easily traced and assigned to activities.

dynamic invoice group

Dynamic invoice groups are invoice groups that contain account lists that are generated dynamically. The invoice groups are generated based on the specified criteria that are stored as a data object.

event filter

An *event filter* can be specified as part of a rule and is used to refine the event. The event filter allows actions that are associated with a rule to be invoked only if certain event conditions are met.

failover

Failover is the process of maintaining an up-to-date copy of a database on an alternate system for backup. The traditional failover architecture is comprised of one system running the application and the other is idle in standby mode. The standby system is ready to take over if the primary system fails. An alternative architecture includes clustering.

invoice group

An *invoice group* is comprised of a set of accounts that can be run together in one instance.

IT Infrastructure Library (ITIL)

ITIL is a set of practices that is used to aid the implementation of a framework for IT Service Management. This customizable framework defines how service management is applied within an organization. ITIL is used across the world as the de-facto standard for best practice in the provision of IT Service.

Although ITIL covers a number of areas, its main focus is on IT Service Management.

Java Runtime Environment (JRE)

Java Runtime Environment or Java Runtime provides the minimum requirements for executing a Java application. JRE consists of the Java Virtual Machine (JVM), core classes, and supporting files. JRE is part of the Java Development Kit (JDK), a set of programming tools for developing Java applications.

Management Database (MDB)

The *Management Database (MDB)* is the CA Management Database schema. The MDB is a common enterprise data repository that integrates CA product suites. The MDB provides a unified database schema for the management data that all CA products store. The CA products can be distributed or

mainframe. Use of the MDB with CA products enables full integration for managing your IT infrastructure. The MDB integrates management data from all IT disciplines and CA products. Customers can extend the MDB Schema to include other IT management data from non-CA software products and tools.

pool worksheets

Pool worksheets are used to trace cost elements to activities to obtain dollar values for each related activity cost pool. Formulas can be used to adjust costs spanning across fiscal periods and sets.

process definition

A *process definition* is a representation of one of your business processes. A process definition is comprised of nodes, events, roles, actors, work, and the criteria for process logic. Running a process definition creates a process instance. You can create multiple process instances of the same process definition.

process instance

A *process instance* represents what is actually happening. By running a process definition, you create a process instance. You can create multiple process instances of the same process definition. Process instances are sometimes called a process definition instance.

proration

Proration is the process of dividing the cost of a subscription over the billing cycle period of an account.

report layout

A *report layout* is used to present multiple report elements as one report. With report layouts, you can design customized reports by using objects such as text, URLs, and multiple data view objects. You can choose sizes, colors, borders/styles, set up snap to grid, and other tools to obtain the desired result. Layouts are managed in folders to help categorize them by purpose.

routing nodes

Routing nodes define the branching of control flow in a Workflow process definition. Choice routing nodes allow one route for the next activity. Parallel routing nodes allow more than one route to be taken.

rule

A *rule* is associated with an event. A rule can have a set of filter conditions that define when the rule is applied. When the filter conditions are satisfied and the rule is enabled, the rule actions are launched.

service

A *service* is a product or an application that your clients can access through a request or a subscription. A service is defined by associating service option groups to the service before it can be subscribed to or requested.

service catalog

A *service catalog* consists of services that a business unit or an entire enterprise publishes. Services are built of one or more service option groups that describe IT services and how to charge for them. The service catalog enables an organization to model its business units and manage the users accounts contained within those units. The service catalog also defines the inclusion, inheritance, dependencies, and associative relationships between each of the published items in the catalog. The published items can be services, service option groups, and service option group definitions. Accounts and users subscribe to or request catalog services. Services in the service catalog can be organized into folders. Each service contains detailed information about the price of the service. Services can represent one or more metrics and include service level agreements.

A *service catalog* is also known as a *catalog*.

Service Level Agreement (SLA)

A *Service Level Agreement* is a contract. This contract specifies the level of service to be provided while the agreement is in effect.

Service Level Objective (SLO)

A *Service Level Objective* is the building block for an SLA. The SLO provides the business objectives or business rules that set the warning and violation threshold levels. The SLO thus determines the success or failure of the overall SLA.

service option element

A *service option element* is the smallest unit of the catalog. This unit defines a piece of text, fee, or an application in a service. Service option elements are grouped or classified in service option groups.

service option group

A *service option group* contains the cost that is associated with subscribing to a service. The cost can be based on transaction, usage-based billing, or rate. Service Option Group can be composed of many types of chargeable and non-chargeable items. For example, rates, applications and agreements.

service worksheets

Service worksheets contain services, service option groups, and service option elements. Service worksheets are used to apply applicable costs to associated services. These costs can be direct or derived from associated activity cost pools. Formulas can be used to adjust costs spanning across fiscal periods and sets.

Simple Object Access Protocol (SOAP)

SOAP is a lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP uses HTTP as the transport protocol and XML as the payload encoding scheme. Developers can use any programming language to call the exposed methods of CA Service Catalog, using standard SOAP call syntax.

worksheets

Worksheets enable you to define costs that are related to business activities. Service Worksheet and Pool Worksheet are the two types of worksheets.

WSDL

WSDL (Web Services Description Language) is an XML format that is published for describing web services.

CA Service Management Common Data Object Field Level Mapping Details

This section describes the Common Data Object reference field level mapping details for implementers who are using Web Services with CA ITAM, CA SDM, and/or CA Service Catalog. As a CA Service Management solution implementer, you might need field level mapping details between point products like CA SDM, CA ITAM, CA Service Catalog in order to leverage the mapping information.

This section contains the following topics:

Field Level Reference Mapping for ca_company

Contents

The ca_company table describes the CA ITAM and CA Service Desk Manager reference mapping details.

CA ITAM Department	CA SDM Department	Database Column Name	Data Type
companyid	id	company_uuid	UUID
value	Company Name	company_name	string
companytypekey	company_type	company_type	Number
alias	alias	alias	String
bbs	bbs	bbs	String
inactiveflag	delete_flag	inactive	boolean
description	description	description	string
creationdate	creatioin_date	creation_date	date
creationuser	creation_user	creation_user	string
lastupdatedate	last_mod	last_update_date	date
lastupdateuser	last_update_user	last_update_user	String
description	description	description	String
defaultlocationid	location_uuid	location_uuid	UUID
fiscalmonthkey	month_fiscal_year_ends	month_fiscal_year_ends	Number
parentcompanyid	parent_company_uuid	parent_company_uuid	UUID
primarycontactid	primary_contact_uuid	primary_contact_uuid	UUID
website	web_address	web_address	String
Assetcount	(Not Applicable)	Asset_count	Number
Divisionid	(Not Applicable)	Division_id	Number
Domainuuid	(Not Applicable)	Domain_uuid	UUID
Duplicateid	(Not Applicable)	Duplicate_with_uuid	UUID
Employeecount	(Not Applicable)	Employee_count	Number
Fastflag	(Not Applicable)	Fast_flag	Number
siiaflag	(Not Applicable)	siia_flag	Number

CA ITAM Department	CA SDM Department	Database Column Name	Data Type
Sourcetypeid	(Not Applicable)	Source_type_id	Number
Userpriorityflag	(Not Applicable)	User_priority_flag	Number
(Not Applicable)	authentication_password	authentication_password	String
(Not Applicable)	authentication_user_name	authentication_user_name	number
(Not Applicable)	delete_time	delete_time	number
(Not Applicable)	exclude_registration	exclude_registration	Integer

Field Level Reference Mapping for ca_location

The ca_location table describes the field level reference mapping details for CA ITAM, CA Service Desk Manager, and CA Service Catalog.

CA ITAM Location	CA SDM Location	CA Service Catalog Location	DB Column Name	Data Type
Locationid	Id	(Not Applicable)	Location_uuid	UUID
Location Name	name	Name	Location_name	String
address1	address1	Address	address_1	String
address2	address2	Address	address_2	String
address3	address3	Address	address_3	String
address4	address4	Address	address_4	String
address5	address5	Address	address_5	String
address6	address6	Address	address_6	String
city	city	City	city	String
stateprovincekey	state	State/Province	state	Number
zip	zip	ZIP/Postal Code	zip	String
telephone	pri_phone_number	Primary Phone	pri_phone_number	String
fax	fax_number	Fax Number	fax_number	String
inactiveflag	delete_flag	(Not Applicable)	inactive	Boolean (1 or 0)
creationuser	(Not Applicable)	(Not Applicable)	Creation_user	String
creationdate	(Not Applicable)	(Not Applicable)	Creation_date	Long Number
lastupdateuser	last_update_user	(Not Applicable)	Last_update_user	String
lastupdatedate	last_mod	(Not Applicable)	Last_update_date	Long Number
locationtypekey	(Not Applicable)	(Not Applicable)	location_type_id	Number
countrykey	Country	Country	country	Number
regionid	(Not Applicable)	(Not Applicable)	region_id	Number
mailaddress1	mail_address1	(Not Applicable)	mail_address_1	String
mailaddress2	mail_address2	(Not Applicable)	mail_address_2	String

CA ITAM Location	CA SDM Location	CA Service Catalog Location	DB Column Name	Data Type
mailaddress3	mail_address3	(Not Applicable)	mail_address_3	String
mailaddress4	mail_address4	(Not Applicable)	mail_address_4	String
mailaddress5	mail_address5	(Not Applicable)	mail_address_5	String
mailaddress6	mail_address6	(Not Applicable)	mail_address_6	String
county	county	(Not Applicable)	county	String
siteid	Site	(Not Applicable)	site_id	Number
comments	description	Description	comments	String
organizationid	(Not Applicable)	(Not Applicable)	organization_uuid	UUID
individualid	primary_contact_uuid	(Not Applicable)	primary_contact_uuid	UUID
parentlocationid	(Not Applicable)	(Not Applicable)	parent_location_uuid	UUID

Field Level Reference Mapping for ca_site

The ca_site table describes the CA ITAM and CA SDM field level reference mapping details.

CA ITAM Site	CA SDM Site	Database Column Name	Data Type
siteid	id	Site_id	Number
sitename	name	name	String
inactiveflag	delete_flag	inactive	Boolean (1 or 0)
contactid	contact	contact_uuid	UUID
alias	alias	alias	String
description	description	description	String
lastupdatedate	last_mod	last_update_date	Number
lastupdateuser	last_update_user	last_update_user	String
creationdate	creation_date	creation_date	Number
creationuser	creation_user	creation_user	String

Field Level Reference Mapping for ca_organization

The ca_organization table describes the field reference mapping details CA ITAM and CA Service Desk Manager.

CA ITAM Organization	CA SDM Organization	Column Name	DataType
Organizationid	id	Organization_uuid	UUID

CA ITAM Organization	CA SDM Organization	Column Name	DataType
Name	name	name	String
abbreviation	org_num	abbreviation	String
inactiveflag	delete_flag	inactive	Boolean
primaryphonenumber	phone_number	pri_phone_number	String
altphonenumber	alt_phone	alt_phone_number	String
faxnumber	fax_phone	fax_number	String
contactid	contact	contact_uuid	UUID
emailaddress	email_addr	email_address	String
pageremailaddress	pemail_addr	pager_email_address	String
costcenterkey	billing_code	cost_center	Number
locationid	location	location_uuid	UUID
description	Description	description	String
lastupdatedate	last_mod	last_update_date	Number
lastupdateuser	Last Modified By	last_update_user	String
parentorganizationid	(Not Applicable)	parent_org_uuid	UUID
creationdate	(Not Applicable)	creation_date	Number
creationuser	(Not Applicable)	creation_user	String
(Not Applicable)	iorg_service_type	Table: usp_organization column: iorg_service_type	String
(Not Applicable)	owning_contract	Table: usp_organization column: owning_contract	Number

Field Level Reference Mapping for ca_owned_resource

The ca_owned_resource table describes the CA ITAM and CA Service Desk Manager reference mapping details.

CA ITAM Asset	CA SDM Configuration Item	Data Type	Ca_owned_resource Column	Reference Database Table
assetid	id	UUID	Own_resource_uuid	(Not Applicable)
assetname	name	String	Resource_name	(Not Applicable)
serialnumber	serial_number	String	Serial_number	(Not Applicable)
altassetid	alt ci id	String	resource_tag	(Not Applicable)
hostname	system_name	String	host_name	(Not Applicable)
dnsname	dns_name	String	dns_name	(Not Applicable)
macaddress	Mac_address	String	mac_address	(Not Applicable)

CA ITAM Asset	CA SDM Configuration Item	Data Type	Ca_owned_resource Column	Reference Database Table
costcenterkey	cost center	Number	cost_center	Ca_resource_cost_center
ci	ci	Boolean	is_ci	(Not Applicable)
asset	issnr	Boolean	is_asset	(Not Applicable)
inactive	delete_flag	Boolean	inactive	(Not Applicable)
floorlocation	loc_floor	UUID	floor_location	Ca_location
roomlocation	loc_room	UUID	room_location	Ca_location
cabinetlocation	loc_cabinet	UUID	cabinet_location	Ca_location
shelflocation	loc_shelf	UUID	shelf_location	Ca_location
slotlocation	loc_slot	UUID	slot_location	Ca_location
assettypekey	family	Number	resource_family	Ca_resource_family
class	class	Number	resource_class	Ca_resource_class
quantity	Asset_count	Number	resource_quantity	(Not Applicable)
itemid	model	UUID	model_uuid	Ca_model_def
contactid	resource_contact	UUID	resource_contact_uuid	ca_contact
locationid	location	UUID	Location_uuid	Ca_location
sellercompanyid	supplier	UUID	supply_vendor_uuid	Ca_company
statuskey	status	Number	resource_status	(Not Applicable)
description	description	String	Resource_description	(Not Applicable)
productversion	Product_version	String	product_version	(Not Applicable)
acquiredate	Acquire_date	Date	acquire_date	(Not Applicable)
installationdate	install_date	Date	installation_date	(Not Applicable)
billingcontactid	billing_contact_ uuid	UUID	billing_contact_uuid	ca_contact
supportcontact1id	support_contact1_uuid	UUID	support_contact1_uuid	ca_contact
Supportcontact2id	support_contact2_uuid	UUID	support_contact2_uuid	ca_contact
maintenancevendorid	vendor_repair	UUID	maintenance_vendor_uuid	Ca_company
manufacturerid	manufacturer	UUID	manufacturer_uuid	Ca_company
responsibleorganizationid	service_org	UUID	responsible_org_uuid	ca_organization
servicetypeid	(Not Applicable)	Number	Usp_owned_resource.service_type	(Not Applicable)

CA ITAM Asset	CA SDM Configuration Item	Data Type	Ca_owned_resource Column	Reference Database Table
priorityid	(Not Applicable)	Number	usp_owned_resource. nr_pr_id	(Not Applicable)
ipaddress	alarm_id	String	ip_address	(Not Applicable)
licenseinformation	license_number	String	license_information	(Not Applicable)
supportcontact3id	support_contact3_uuid	UUID	support_contact3_uuid	ca_contact
disasterrecoverycontactid	disaster_ recovery_ contact_uuid	UUID	disaster_recovery_contact_uuid	ca_contact
backupservicescontactid	backup_ services_ contact_uuid	UUID	backup_services_contact_uuid	ca_contact
networkcontactid	network_contact_uuid	UUID	network_contact_uuid	ca_contact
responsiblevendorid	vendor_restore	UUID	responsible_vendor_uuid	(Not Applicable)
maintenancevendorid	vendor_repair	UUID	maintenance_org_uuid	(Not Applicable)
assetalias	resource_alias	String	resource_alias	(Not Applicable)
companyboughtforid	company_bought_ for_uuid	UUID	company_bought_for_uuid	(Not Applicable)
organizationboughtforid	org_bought_for_ uuid	UUID	org_bought_for_uuid	(Not Applicable)
processorcount	(Not Applicable)	Number	processor_count	(Not Applicable)
glcodekey	Gl_code	Number	gl_code	Not Applicable)
auditdate	(Not Applicable)	Date	audit_date	(Not Applicable)
operatingsystemkey	operating_system	Number	operating_system	(Not Applicable)
capacity	(Not Applicable)	Number	resource_capacity	(Not Applicable)
capacityunitskey	(Not Applicable)	Number	resource_capacity_unit	(Not Applicable)
departmentkey	department	Number	department	(Not Applicable)
requisitionid	requisition_id		requisition_id	(Not Applicable)
purchaseorderid	purchase_order_id	Number	purchase_order_id	(Not Applicable)
lastupdatedate	last_mod	Date	last_update_date	(Not Applicable)
lastupdateuser	Last_mod_by	String	last_update_user	(Not Applicable)
statusdate	Status_date	Date	status_date	(Not Applicable)
deploymentstatuskey	(Not Applicable)	Number	(Not Applicable)	(Not Applicable)

CA ITAM Asset	CA SDM Configuration Item	Data Type	Ca_owned_resource Column	Reference Database Table
lifecyclestatuskey	(Not Applicable)	Number	lifecycle_status	(Not Applicable)
lifecyclestatusdate	(Not Applicable)	Date	lifecycle_status_date	(Not Applicable)
Subclass	(Not Applicable)	Number	resource_subclass	(Not Applicable)
contactid	resource_contact	UUID	resource_contact_uuid	(Not Applicable)
excludereconciliationkey	(Not Applicable)	Boolean	exclude_reconciliation	(Not Applicable)
managedkey	ufam	Number	ufam	(Not Applicable)
processortype	(Not Applicable)	Number	processor_type	(Not Applicable)
discoverylastrundate	(Not Applicable)	Date	discovery_last_run_date	(Not Applicable)
reconciliationdate	(Not Applicable)	Date	reconciliation_date	(Not Applicable)
creationdate	(Not Applicable)	Date	creation_date	(Not Applicable)
creationuser	(Not Applicable)	String	creation_user	(Not Applicable)

Field Level Reference Mapping for ca_contact

The ca_contact table describes the field level reference mapping details for CA ITAM, CA Service Desk Manager, and CA Service Catalog.

CA ITAM Contact	CA SDM Contact	CA Service Catalog User	Database Column Name	Data Type
lastname	last_name	last name	last_name	string
firstname	first_name	first name	first_name	string
middlename	middle_name	middle name	middle_name	string
companyid	company	(Not Applicable)	company_uuid	uuid
inactiveflag	delete_flag	(Not Applicable)	inactive	boolean (1 or 0)
altcontactid	contact_num	(Not Applicable)	alternate_identifier	string
userid	userid	user id	userid	string
contacttypekey	type	(Not Applicable)	contact_type	number
jobtitlekey	position	job title	job_title	number referring to id column of ca_job_title table
alias	alias	alias	alias	string

CA ITAM Contact	CA SDM Contact	CA Service Catalog User	Database Column Name	Data Type
lastupdatedate	Last_mod	(Not Applicable)	last_update_date	long number
lastupdateuser	last_mod_by	(Not Applicable)	last_update_user	string
telephone	phone_number	primary phone	pri_phone_number	string
fax	fax_phone	fax number	fax_number	string
pagertelephone	beeper_phone	pager number	pager_number	string
alttelephone	alt_phone	Secondary Phone	alttelephone	String
emailid	email_address	Email	email_address	String
pageremailaddress	pemail_address	(Not Applicable)	pager_email_address	String
locationid	location	Location	location_uuid	UUID
organizationid	organization	(Not Applicable)	organization_uuid	UUID
adminorganizationid	admin_org	(Not Applicable)	adminorganizationid	UUID
supervisorid	supervisor_contact_uuid	Manager	supervisor_contact_uuid	UUID
departmentkey	dept	(Not Applicable)	department	Number
costcenterkey	billing_code	(Not Applicable)	cost_center	Number
comments	notes	Description	comments	String
creationdate	(Not Applicable)	(Not Applicable)	Creation_date	Long number
creationuser	(Not Applicable)	(Not Applicable)	Creation_user	String

Field Level Reference Mapping for ca_resource_cost_center

The ca_resource_cost_center table describes the CA ITAM and CA SDM field level reference mapping details.

CA ITAM Cost Center	CA SDM Cost Center	Database Column Name	Data Type
id	id	id	number
value	name	name	string
inactiveflag	delete_flag	inactive	boolean

CA ITAM Cost Center	CA SDM Cost Center	Database Column Name	Data Type
description	description	description	string
creationdate	creation_date	creation_date	date
creationuser	creation_user	creation_user	string
lastupdatedate	last_mod	last_update_date	date
lastupdateuser	last_update_user	last_update_user	string
(Not Applicable)	delete_time	delete_time	number
(Not Applicable)	exclude_registration	exclude_registration	integer

Field Level Reference Mapping for ca_resource_family

The ca_resource_family table describes the CA APM and CA SDM field level reference mapping details.

CA APM Asset Family	CA SDM Family	Database Column Name	Data Type
id	**id**	**id**	**Number**
Value	sym	name	String
inactiveflag	delete_flag	inactive	Boolean
description	description	description	String
lastupdatedate	last_update_date	last_update_date	Number
lastupdateuser	last_update_user	last_update_user	String
extensiontablename	extension_name	table_extension_name	String
physicaltablename	physical_table_name	physical_table_name	String
includereconciliationkey	include_reconciliation	include_reconciliation	Boolean
Is ITAM	(Not Applicable)	is_itam	Boolean
creationdate	(Not Applicable)	creation_date	Number
creationuser	(Not Applicable)	creation_user	String
(Not Applicable)	exclude_registration	exclude_registration	Number

Field Level Reference Mapping for ca_resource_class

The ca_resource_class table describes the CA ITAM and CA Service Desk Manager field level reference mapping details.

CA ITAM Asset Class	CA SDM Class	Database Column Name	Data Type
Value	type	name	String
inactiveflag	delete_flag	inactive	Boolean
description	description	description	String

CA ITAM Asset Class	CA SDM Class	Database Column Name	Data Type
lastupdatedate	last_mod	last_update_date	Number
lastupdateuser	last_update_user	last_update_user	String
creationuser	creation_user	creation_user	String
creationdate	creation_date	creation_date	Number
familyid	family	id	Number
(Not Applicable)	exclude_ registration	exclude_ registration	(Not Applicable)

Field Level Reference Mapping for ca_resource_department

The ca_resource_department table describes the CA ITAM and CA Service Desk Manager field level reference mapping details.

CA ITAM Department	CA SDM Department	Database Column Name	Data Type
name	id	name	string
value	name	name	string
inactiveflag	delete_flag	inactive	boolean
description	description	description	string
creationdate	creation_date	creation_date	date
creationuser	creation_user	creation_user	string
lastupdatedate	last_mod	last_update_date	date
lastupdateuser	last_update_user	last_update_user	string
(Not Applicable)	delete_time	delete_time	number
(Not Applicable)	exclude_registration	exclude_registration	integer

USM Data Mapping for CA Service Desk Manager Connector

When connectors import services and CIs from domain managers, they normalize the classes, properties, relationships, and severities in the domain manager to adhere to the USM schema. This section lists the CA SDM classes, severities, and relationships and their USM mapping after the import.

Note: For more information about CI property mapping, see the CA SDM Connector policy file located at the policy registry location.

More Information:

Device Properties Calculation

Certain CIs, such as ProvisionedSoftware and NIC Card, are mapped to USM CI types that require device properties defined by USM import standards in Catalyst. When device properties are not defined for the CI, the connector uses this property to obtain the information from the system on which the CI is hosted. One or more of the following CI device properties may be required:

- DeviceAssetNumber
- DeviceBiosSystemID
- DeviceDnsName
- DeviceSysName
- DevicePhysSerialNumber
- DeviceMacAddress
- DeviceIPV4Address
- DeviceIPV4AddressWithDomain
- DeviceIPV6Address
- DeviceIPV6AddressWithDomain

CA SDM Connector queries CMDB for the device properties of the CI as follows:

1. Based on the system name, the connector queries CMDB for the CI device properties, and the CI is populated when found. For application discovered CIs in CMDB, the System Name field appears in the following format:

   ```
   SNMP_CI_name| CI_name | file_path
   ```

2. If the SNMP_CI_name does not exist in CMDB and the query fails, the connector uses the DeviceSysName attribute to query CMDB for the device properties of the CI.

3. If the queries described in step 1 and 2 are unsuccessful, the connector uses the DeviceXXXFromRelationship attribute to query CMDB for the CI device properties based on the relationship type.

Device Properties

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

Device (USM)	CA SDM Attributes	User Interface
DeviceAssetNumber	Calculated by the connector.	N/A
DeviceBiosSystemID	Calculated by the connector.	N/A
DeviceDnsName	Calculated by the connector.	N/A
DeviceSysName	Calculated by the connector.	System Name
DevicePhysSerialNumber	Calculated by the connector.	N/A
DeviceMacAddress	Calculated by the connector.	N/A
DeviceIPV4Address	Calculated by the connector.	N/A
DeviceIPV4AddressWithDomain	N/A	N/A
DeviceIPV6Address	Calculated by the connector.	N/A
DeviceIPV6AddressWithDomain	N/A	N/A

Mandatory Attributes for CI Mapping in CA Catalyst

The following table shows the mandatory attributes in CA SDM required to populate CIs in CA Catalyst:

USM Family	CMDB Family	Attribute	Format	Comments
Cluster	**Cluster**			
		Serial_num/ asset_num/ DNS name		
Database Instance	**Software. Database**			
		Asset_num		
		Server /System_name	System_name should contain the pipe (|) separated value	System_name example: "SDMServer|SQL|C:\Program Files\SQL\".
Provisioned Software	**Software. COTS**			
		System_name	System_name should contain the pipe (|) separated value	System_name example:

USM Family	CMDB Family	Attribute	Format	Comments
				"SDM Server|Cohesion Agent (Windows)|5.0-SP1|C:\Program Files\CA\Cohesion\Agent".
Media Drive	**Hardware. Storage**			
		System_name	System_name should contain the pipe (|) separated value	System_name example: SDMServer|HardDisk0
Operating System	**Software. Operating System**			
		Server /System_name	System_name should contain the pipe (|) separated value	System_name example: SDMServer|Windows 2008SP2
Virtual System	**Hardware. Virtual Machine**			
		Serial_num/ asset_num/ DNS name		
		system_name		
Computer System	**Hardware. Server**			
		Serial_num/ asset_num/ DNS name		
		system_name		
Port	**Network.Port**			
		Serial_num/ asset_num		
		system_name	System_name should contain the pipe (|) separated value	System_name Example: SDMServer|Apachetomcat
Application Server	**Software. Application Server**			
		asset_num		
		server /system_name		

USM Family	CMDB Family	Attribute	Format	Comments
Application	**Software. Application**			
		server /system_name		
GenericIPDevice	**Network. Hub**			
		Serial_num/ asset_num/ DNS name		
InterfaceCard	**Network. Network Interface Card**			
		Serial_num		
Printer (Network)	**Hardware. Printer**			
		Serial_num/ asset_num/ DNS name		
Router	**Network. Router**			
		Serial_num/ asset_num/ DNS name		
Running Hardware	**Hardware**			
		System_name	System_name should contain the pipe (|) separated value	System_name Example: SDMServer|Disk1
Switch	**Network. Switch**			
		Serial_num/ asset_num/ DNS name		
		system_name		

Relationship Mapping

This topic contains the following information:

Relationship Mapping

The CA SDM classes are transformed into USM types as shown in the following table:

BinaryRelationship	CA SDM Attributes	User Interface / CMDB Relationship Details
SourceMdrProduct	CA:00020	n/a
SourceMdrProdInstance	<primary server host name>	n/a
SourceMdrElementID	nr.persid/chg.persid/cr.persid	<bop_dump>
SourceCorrelatedKey	n/a	n/a
TargetMdrProduct	CA:00020	n/a
TargetMdrProdInstance	<primary server host name>	n/a
TargetMdrElementID	nr.persid/chg.persid/cr.persid	<bop_dump>
ScopeMdrProduct	CA:00020	n/a
ScopeMdrProdInstance	<primary server host name>	n/a
ScopeMdrElementID	Configured by the connector	<bop_dump>
Significance	n/a	n/a
Semantic	Bmhier:ci_rel_type	CMDB Relationships tab; Relationship

Relationship Semantic Mapping

The relationship semantic mapping is shown in the following table:

CA SDM <Property>	USM Type
Change, Problem, Incident, Request	IsImpactedBy
IsRequiredBy	HasRequirementFor
Connects To	IsConnectedTo
Contains	IsPartOf
Is Source Code For	IsInstanceOf
Hosts	IsHostedBy
Manages	IsManagedBy
IsUsedBy	HasAccessTo
Monitors	IsDiscoveredBy
Supports	IsAffectedBy

CA SDM <Property>	USM Type
Runs	HasMember
Is The Child Of	HasDetail
Is Location For	IsResidentOf
Administers	HasContact
Is Primary Contact For	HasContact
Is Business Owner Of	HasContact
Approves	HasContact
Has As Assignee	HasContact
Financially Belongs To	IsComposedOf
Is Bound To	IsBoundTo
Is Clone Of	IsCloneOf
Is Composed Of	IsComposedOf
Is Evolution Of	IsEvolutionOf
Is Result Of	IsResultOf
Is Successor Of	IsSuccessorOf
Is Triggered By	IsTriggeredBy
Is Affected By	IsAffectedBy
Has Member	HasMember
Is Discovered By	IsDiscoveredBy
Manages	IsManagedBy
Has Access To	HasAccessTo
Is Required By	HasRequirementFor
Is Triggered By	Is Triggered By
Has Detail	HasDetail
Is Successor Of	IsSuccessorOf
Is Source Code For	IsInstanceOf
Is Result Of	IsResultOf
Is Primary Contact For	HasContact
Is Location For	IsResidentOf
Is Evolution Of	IsEvolutionOf
Is Composed Of	IsComposedOf
Is Clone Of	IsCloneOf
Is Business Owner Of	HasContact
Is Bound To	IsBoundTo
Hosts	IsHostedBy
Has As Assignee	HasContact

Severity Mapping

The following table shows how the CA SDM Connector maps alert severities to USM severities:

CA SDM Connector Alerts	USM Severity
Too Many Open Incidents	Critical
SLA to Expire	Major
SLA Violated	Critical
Upcoming Maintenance Window	Critical
Upcoming Blackout Window	Critical

Note: In CA SDM, blackout windows are not configured with CIs, therefore, they do not appear in the Service Console. You can, however, view blackout windows for CIs in the REST interface by disabling the useAlertFilter through the Connector Controls panel.

Type Mapping

When connectors import services and CIs from domain managers, they normalize the classes in the domain manager to the standard USM types. This section lists the CA SDM classes and their mapping after the import.

The CMDB classes are transformed into USM types for CIs as shown in the following table:

USM Type (entitytype = CI)	User interface CI detail where CMDB family = ...
Application	Software.Application
ApplicationServer	Software.Application Server
Cluster	Cluster
ComputerSystem	Hardware.Server
DatabaseInstance	Software.Database
GenericIPDevice	Network.Hub
InterfaceCard	Network.Network Interface Card
MediaDrive	Hardware.Storage
OperatingSystem	Software.Operating System
Port	Network.Port
ProvisionedSoftware	Software.COTS
Printer (Network)	Hardware.Printer
Router	Network.Router

USM Type (entitytype = CI)	User interface CI detail where CMDB family = ...
RunningHardware	Hardware
Service	Enterprise.Service/Service
Switch	Network.Switch
VirtualSystem	Hardware.VirtualMachine

The CA SDM classes are transformed into USM types for other elements as shown in the following table:

USM type (entitytype = other elements)	CA SDM CMDB Definition	User Interface
Change Order	SDM: chg	Change Order
Incident	SDM: cr WHERE cr.type='I'	Incident
Location	SDM:loc CMDB: ci_location	Location
OrganizationEntity	SDM: org CMDB: ci_organization	Organization
Person	SDM: cnt WHERE cnt.type!=2308 CMDB: ci_contact	Contact
Problem	SDM: cr WHERE cr.type='P'	Problem
Request	SDM: cr WHERE cr.type='R'	Request

Application

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Note: You can define the Vendor and Model properties through the CA SDM connector policy to manage your configuration items. For more information about these properties, see Post-Installation: Manufacturers and Models.

Application (USM)	CA Service Management Attribute	User Interface (CI detail form)
Description	nr.description	
Vendor	nr.manufacturer.xym [ca_cmpny]	Inventory tab; Manufacturer (Configure this property in the connector policy to the requirement of your site)

Application (USM)	CA Service Management Attribute	User Interface (CI detail form)
ProductName	nr.name (http://nr.name)	Name
Version	app_extx.version	Attributes tab version
MajorVersion	n/a	n/a
BuildNumber	n/a	n/a
ServiceLevel	n/a	n/a
Device properties required (see page 4738)	n/a	n/a
ProcessID	n/a	n/a
AccessedViaTcpPort	n/a	n/a
ProcessDistinguishingID	app_extx. app_id	Attributes tab; Application ID

ApplicationServer

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Note: You can define the Vendor and Model properties through the CA SDM connector policy to manage your configuration items. For more information about these properties, see Post-Installation: Manufacturers and Models.

ApplicationServer (USM)	CA SDM Attribute	User Interface (CI detail form)
Vendor	nr.manufacturer.xym [ca_cmpny]	Inventory tab; Manufacturer (Configure this property in the connector policy to the requirement of your site)
ProductName	nr.name (http://nr.name)	Name
Version	app_extx.version	Attributes tab version
MajorVersion	n/a	n/a
BuildNumber	n/a	n/a
ServiceLevel	n/a	n/a
Device properties required (see page 4739)	n/a	n/a
ProcessID	n/a	n/a
AccessedViaTcpPort	n/a	n/a
ProcessDistinguishingID	app_extx. app_id	Attributes tab; Application ID
AppServerType	app_extx.type	Attributes tab; Type

Change Order

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

ChangeOrder (USM Type)	CA SDM Attributes	User Interface
AssignedID	chg.chg_reg_num	Text on button bar (left side)
IsTemplate	n/a	n/a
TemplateUsed	n/a	n/a
Severity	n/a	n/a
IsActive	issue 157	n/a
Urgency	n/a	n/a
Impact	chg.mpact; imp.sym	Impact
Priority	chg.priority; pri.sym	Priority
Open Timestamp	chg.target_start_last	Open Date (above tabs)
CallbackTimestamp	chg.call_back_date	Call Back Date/Time
Resolution Timestamp	chg.resolve_date	Resolve Date (above tabs)
Closure Timestamp	chg.close_date	Close Date (above tabs)
ChargebackID	n/a	n/a
RootCause	chg.rc	Root Cause
SolutionUrls	n/a	n/a
NeedByDate	chg.need_by	Need By Date
COType [COTypeEnum]	chg.chgtype; chgtype.sym	Type
RequiresCabApproval	chg.cab_approval	CAB Approval
COStatus [COStatusEnum]	chg.chgtype; chgtype.sym	Status
CompletionCode	chg.closure_code; closure_code.sym	Closure Code
FulfillmentData	n/a	config.items

ChangeOrder (USM Type)	CA SDM Attributes	User Interface
ChangeBackedOut [ChageReversonEnum]	n/a	n/a
COCategory [CoCategoryEnum]	chg.category; chgcat.code	Category
EstimatedCost	chg.est_cost	Costs/Plans tab; Est Cost
ActualCost	chg.cost	Costs/Plans tab; Actual Cost
Currency [CurrencyEnum]	n/a	n/a
EstimatedStartDate	chg.sched_start_date	Schedule Start Date
Estimated TotalTime	chg.sched_duration	Schedule Duration
ActualStartDate	chg.actual_start_date	Costs/Plans tab; Actual Implementation Start Date
ActualTotalTime	chg.actual_total_time	Costs/Plans tab; Actual Duration
ProjectID	chg.project; nr.family.extension_name; projex.clarity_id (if null, then use the chg.project.name (http://chg.project.name))	n/a
BusinessCase	chg.business_case	Costs/Plans tab; Business Case
Effort	chg.effort	Costs/Plans tab; Implementation Plan

Cluster

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Cluster (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
PrimaryIPV4Address	nr.alarm_id if IPV4 is formatted	Inventory tab; IP Address (V4)
PrimaryIPV6AddressWithDomain	n/a	n/a
PrimaryIPV6Address	nr.alarm_id if IPV6 is formatted	

Cluster (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
		Inventory tab; IP Address (V6)
PrimaryIPV4AddressWithDomain	n/a	n/a
GroupName	nr.name (http://nr.name)	Attributes Network Name
PrimaryIPV4AddressWithDomain	n/a	n/a
MemberCriteria	net_clux.quorum	Attributes; Quorum
PrimaryDnsName	nr.dns name	DNS Name
LoadBalancingType	n/a	n/a
usm-core2: MemberStatus	n/a	
InstanceName	<<AUTO-GENERATED BY GLOBAL Policy>>	
NamedAliases	<<AUTO-GENERATED BY GLOBAL Policy>>	
Label	<<AUTO-GENERATED BY GLOBAL Policy>>	
Tags	<<AUTO-GENERATED BY GLOBAL Policy>>	
Description	nr.description	
CreationTimestamp	nr.creation_user	
CreationUserName	nr.creation_date	
LastModTimestamp	nr.last_mod	
UrlParams	"nr"	

Common CI Properties

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
MdrProduct	ConnectorConfigMdrProduct	n/a
MdrProdInstance	ConnectorConfigMdrProdInstance	n/a
MdrElementID	nr.persid (Outbound)	<bop_dump>
UrlParams	nr	n/a
NamedAliases	nr.name (http://nr.name), nr.system_name, nr.dns_name	Name, Host Name, Dns Name
Label		n/a

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
	Auto generated by GLOBAL policy	
Description	nr.description	Notes
TenantID	nr.tenant	Tenant ID
Tags	Auto generated by GLOBAL policy	n/a
CreationTimestamp	nr.creation_date	<bop_dump>
CreationUserName	nr.creation.user	<bop_dump>
LastModTimestamp	nr.last_mod	<bop_dump>
LastModActivity	Generated by connector.	n/a
LastModUserName	nr.last_mod_by	<bop_dump>
Deletion Timestamp	This is the timestamp when the CI became inactive in SDM.	<bop_dump>
DeletionUserName	nr.last_mod_by (When it is deleted)	n/a
InstanceName	Auto generated by GLOBAL policy	n/a
TypeName	n/a	n/a
AdministrativeStatus	nr.status.sym [rss]	Inventory tab; Service Status (Ensure that AdministrativeStatus corresponds with AdministrativeStatusEnum in the connector policy)
Retirement Timestamp	nr.retire_date	Attributes tab; Retire Date
IsInMaintenance	nr.status.sym [rss]	Inventory tab; Service Status
MaintStartTimestamp	n/a	n/a
MainExpectedDuration	n/a	n/a
Vendor	nr.manufacturer	
Model	nr.model	
GroupName	nr.name	Name
WebSite	nr.class	Class
Software.WebSite	nr.family	Family
usm-core2: HomePage|usm-core2: DeviceBiosSystemID	nr.system_name	Hostname
usm-core2: DeviceAssetNumber	app_website. DeviceAssetNumber	Device Asset Number
usm-core2: DeviceBiosSystemID	app_website. DeviceBiosSystemID	Device Bios System ID

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
usm-core2: DeviceDnsName	app_website. DeviceDnsName	Device DNS Name
usm-core2: DevicePhysSerialNumber	app_website. DevicePhysSerialNumber	Device Physical Serial Number
usm-core2: DeviceMacAddress	app_website. DeviceMacAddress	Device MAC Address
usm-core2: DeviceIPV4Address	app_website. DeviceIPV4Address	Device IPv4 Address
usm-core2: DeviceIPV4AddressWithDomain	app_website. DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2: DeviceIPV6Address	app_website. DeviceIPV6Address	Device IPv6 Address
usm-core2: DeviceIPV6AddressWithDomain	app_website. DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain
usm-core2:IsHAEnabled	app_website.IsHAEnabled	Is HA Enabled
usm-core2: IsMonitoringMembers	app_website. IsMonitoringMembers	Is Monitoring Members
usm-core2:MaxFailures	app_website.MaxFailures	Max Failures
usm-core2: MemberCriteria	app_website. MemberCriteria	Member Criteria
usm-core2:GroupType	app_website.GroupType	Group Type
usm-core2:HomePage	app_website.HomePage	Home Page
usm-core2: BusinessRelevance	app_website. BusinessRelevance	Business Relevance

DiskPartition

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
PartitionType|usm-core2:OSDriveName	nr.name	Name
FAT32	nr.class	Class
Hardware.DiskPartition	nr.family	Family
PartitionType|OSNumeric|usm-core2: OSDriveName|DeviceDnsName	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	har_dpar. DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	har_dpar. DeviceBiosSystemID	Device Bios System ID

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
usm-core2:DeviceDnsName	har_dpar.DeviceDnsName	Device DNS Name
usm-core2:DeviceSysName	har_dpar.DeviceSysName	Device System Name
usm-core2:DevicePhysSerialNumber	har_dpar. DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	har_dpar. DeviceMacAddress	Device MAC Address
usm-core2:DeviceIPV4Address	har_dpar. DeviceIPV4Address	Device IPv4 Address
usm-core2:DeviceIPV4AddressWithDomain	har_dpar. DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	har_dpar. DeviceIPV6Address	Device IPv6 Address
usm-core2:DeviceIPV6AddressWithDomain	har_dpar. DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain
OSNumeric	har_dpar.OSNumeric	OS Numeric
ContainingIndex	har_dpar.ContainingIndex	Containing Index
IsPhysical	har_dpar.IsPhysical	Is Physical
usm-core2:OSDriveName	har_dpar.OSDriveName	OS Drive Name
IsBootable	har_dpar.IsBootable	Is Bootable
IsPrimary	har_dpar.IsPrimary	Is Primary
usm-core2:CapacityInMB	har_dpar.CapacityInMB	Capacity In MB
ContextID	har_dpar.ContextID	Context ID

EnvironmentalSensor

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
SensorType|OS Numeric |Containing Index|DeviceDnsName	nr.name (http://nr.name)	Name
Vibration	nr.class	Class
Hardware.EnvironmentalSensor	nr.family	Family
SensorType|OS Numeric |Containing Index|DeviceDnsName	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	har_compr. DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	har_compr. DeviceBiosSystemID	Device Bios System ID

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
usm-core2:DeviceDnsName	har_compr.DeviceDnsName	Device DNS Name
usm-core2:DeviceSysName	har_compr.DeviceSysName	Device System Name
usm-core2:DevicePhysSerialNumber	har_compr. DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	har_compr.DeviceMacAddress	Device MAC Address
usm-core2:DeviceIPV4Address	har_compr.DeviceIPV4Address	Device IPv4 Address
usm-core2:DeviceIPV4AddressWithDomain	har_compr. DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	har_compr.DeviceIPV6Address	Device IPv6 Address
usm-core2:DeviceIPV6AddressWithDomain	har_compr. DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain
OSNumeric	har_compr.OSNumeric	OS Numeric
ContainingIndex	har_compr.ContainingIndex	Containing Index
IsPhysical	har_compr.IsPhysical	Is Physical
ContextID	har_compr.ContextID	Context ID

ESXHypervisor

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	**CA SDM Attributes**	**User Interface / CI Detail Form**
ProductName	nr.name	Name
ESXHypervisor	nr.class	Class
Software.ESXHypervisor	nr.family	Family
ProductName|ProcessID	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	app_esx.DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	app_esx.DeviceBiosSystemID	Device Bios System ID
usm-core2:DeviceDnsName	app_esx.DeviceDnsName	Device DNS Name
usm-core2:DeviceSysName	app_esx.DeviceSysName	Device System Name
usm-core2:DevicePhysSerialNumber	app_esx.DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	app_esx.DeviceMacAddress	Device MAC Address
usm-core2:DeviceIPV4Address	app_esx.DeviceIPV4Address	Device IPv4 Address
usm-core2: DeviceIPV4AddressWithDomain	app_esx. DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	app_esx.DeviceIPV6Address	Device IPv6 Address

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
usm-core2: DeviceIPV6AddressWithDomain	app_esx. DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain
IsMigrationEnabled	app_esx.IsMigrationEnabled	Migration Enabled
usm-core2:ComputeResourceIndex	app_esx.ComputeResourceIndex	Compute Resource Index
usm-core2:HostIndex	app_esx.HostIndex	Host Index
usm-core2:DatacenterPath	app_esx.DatacenterPath	Datacenter Path
usm-core2:FTVersion	app_esx.FTVersion	FT Version
usm-core2:NumberOfPrimaryVMs	app_esx.NumberOfPrimaryVMs	Number Of Primary VMs
usm-core2: NumberOfSecondaryVMs	app_esx.NumberOfSecondaryVMs	Number Of Secondary VMs
ProcessID	app_esx.ProcessID	Process ID
AccessedViaTcpPort	app_esx.AccessedViaTcpPort	Accessed Via Tcp Port
ProcessDistinguishingID	app_esx.ProcessDistinguishingID	Process Distinguishing ID

File

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
FilePathUrl|FileType |DeviceDnsName	nr.name	Name
File	nr.class	Class
Hardware.File	nr.family	Family
FilePathUrl|FileType |DeviceDnsName	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	har_file.DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	har_file.DeviceBiosSystemID	Device Bios System ID
usm-core2:DeviceDnsName	har_file.DeviceDnsName	Device DNS Name
usm-core2:DeviceSysName	har_file.DeviceSysName	Device System Name
usm-core2:DevicePhysSerialNumber	har_file.DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	har_file.DeviceMacAddress	Device MAC Address
usm-core2:DeviceIPV4Address	har_file.DeviceIPV4Address	Device IPv4 Address
usm-core2: DeviceIPV4AddressWithDomain	har_file. DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	har_file.DeviceIPV6Address	Device IPv6 Address
usm-core2: DeviceIPV6AddressWithDomain	har_file. DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
FilePathUrl	har_file.FilePathUrl	File Path Url

HyperVHypervisorManager

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	**CA SDM Attributes**	**User Interface / CI Detail Form**
ProductName	nr.name	Name
HyperVHypervisor	nr.class	Class
Software.HyperVHypervisor	nr.family	Family
ProductName|ProcessID	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	app_hyp.DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	app_hyp.DeviceBiosSystemID	Device Bios System ID
usm-core2:DeviceDnsName	app_hyp.DeviceDnsName	Device DNS Name
usm-core2:DeviceSysName	app_hyp.DeviceSysName	Device System Name
usm-core2:DevicePhysSerialNumber	app_hyp.DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	app_hyp.DeviceMacAddress	Device MAC Address
usm-core2:DeviceIPV4Address	app_hyp.DeviceIPV4Address	Device IPv4 Address
usm-core2: DeviceIPV4AddressWithDomain	app_hyp. DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	app_hyp.DeviceIPV6Address	Device IPv6 Address
usm-core2: DeviceIPV6AddressWithDomain	app_hyp. DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain
IsMigrationEnabled	app_hyp.IsMigrationEnabled	Migration Enabled
AccessedViaTcpPort	app_hyp.DefaultExternalDataRoot	Accessed Via Tcp Port
usm-core2:DefaultExternalDataRoot	app_hyp.DefaultVhdPath	Default External Data Root
usm-core2:DefaultVhdPath	app_hyp.MinimumMacAddress	Default Vhd Path
usm-core2:MinimumMacAddress	app_hyp.MaximumMacAddress	Minimum Mac Address
usm-core2:MaximumMacAddress	app_hyp.ProcessID	Maximum Mac Address
ProcessDistinguishingID	app_hyp.AccessedViaTcpPort	Process Distinguishing ID
ProcessID	app_hyp.ProcessDistinguishingID	Process ID

Memory

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
MemoryType|SizeInMB |ContainingIndex|DeviceDnsName	nr.name	Name
Physical	nr.class	Class
Hardware.Memory	nr.family	Family
ClassName|MemoryType|SizeInMB |ContainingIndex|DeviceDnsName	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	har_mem. DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	har_mem. DeviceBiosSystemID	Device Bios System ID
usm-core2:DeviceDnsName	har_mem.DeviceDnsName	Device DNS Name
usm-core2:DeviceSysName	har_mem.DeviceSysName	Device System Name
usm-core2:DevicePhysSerialNumber	har_mem. DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	har_mem. DeviceMacAddress	Device MAC Address
usm-core2:DeviceIPV4Address	har_mem. DeviceIPV4Address	Device IPv4 Address
usm-core2:DeviceIPV4AddressWithDomain	har_mem. DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	har_mem. DeviceIPV6Address	Device IPv6 Address
usm-core2:DeviceIPV6AddressWithDomain	har_mem. DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain
OSNumeric	har_mem.OSNumeric	OS Numeric
ContainingIndex	har_mem.ContainingIndex	Containing Index
IsPhysical	har_mem.IsPhysical	Is Physical
SizeInMB	har_mem.SizeInMB	Size In MB
ContextID	har_mem.ContextID	Context ID

NetworkServer

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
ProductName	nr.name	Name
NetworkServer	nr.class	Class

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
Software.NetworkServer	nr.family	Family
Protocol|ProcessDistinguishingID|DeviceDnsName	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	app_netsvr.DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	app_netsvr.DeviceBiosSystemID	Device Bios System ID
usm-core2:DeviceDnsName	app_netsvr.DeviceDnsName	Device DNS Name
usm-core2:DeviceSysName	app_netsvr.DeviceSysName	Device System Name
usm-core2:DevicePhysSerialNumber	app_netsvr. DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	app_netsvr.DeviceMacAddress	Device MAC Address
usm-core2:DeviceIPV4Address	app_netsvr.DeviceIPV4Address	Device IPv4 Address
usm-core2: DeviceIPV4AddressWithDomain	app_netsvr. DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	app_netsvr.DeviceIPV6Address	Device IPv6 Address
usm-core2: DeviceIPV6AddressWithDomain	app_netsvr. DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain
ProcessID	app_netsvr.ProcessID	Process ID
AccessedViaTcpPort	app_netsvr.AccessedViaTcpPort	Accessed Via Tcp Port
ProcessDistinguishingID	app_netsvr. ProcessDistinguishingID	Process Distinguishing ID
Protocol	app_netsvr.Protocol	Protocol
ContextID	app_netsvr.ContextID	Context ID

Processor

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
ProcessorType|SpeedInGHz|DeviceDnsName	nr.name	Name
x86	nr.class	Class
Hardware.Processor	nr.family	Family
ProcessorType|OSNumeric|ContainingIndex| DeviceDnsName	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	har_prcr.DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	har_prcr.DeviceBiosSystemID	Device Bios System ID
usm-core2:DeviceDnsName	har_prcr.DeviceDnsName	Device DNS Name
usm-core2:DeviceSysName	har_prcr.DeviceSysName	Device System Name
usm-core2:DevicePhysSerialNumber		

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
	har_prcr.DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	har_prcr.DeviceMacAddress	Device MAC Address
usm-core2:DeviceIPV4Address	har_prcr.DeviceIPV4Address	Device IPv4 Address
usm-core2:DeviceIPV4AddressWithDomain	har_prcr.DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	har_prcr.DeviceIPV6Address	Device IPv6 Address
usm-core2:DeviceIPV6AddressWithDomain	har_prcr.DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain
OSNumeric	har_prcr.OSNumeric	OS Numeric
ContainingIndex	har_prcr.ContainingIndex	Containing Index
IsPhysical	har_prcr.IsPhysical	Is Physical
Speed In GHz	har_prcr.SpeedInGHz	Speed In GHz
ContextID	har_prcr.ContextID	Context ID

ResourceServer

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
ProductName	nr.name	Name
ResourceServer	nr.class	Class
Software.ResourceServer	nr.family	Family
ProductName|ProcessID	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	app_ressvr.DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	app_ressvr.DeviceBiosSystemID	Device Bios System ID
usm-core2:DeviceDnsName	app_ressvr.DeviceDnsName	Device DNS Name
usm-core2:DeviceSysName	app_ressvr.DeviceSysName	Device System Name
usm-core2:DevicePhysSerialNumber	app_ressvr.DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	app_ressvr.DeviceMacAddress	Device MAC Address
usm-core2:DeviceIPV4Address	app_ressvr.DeviceIPV4Address	Device IPv4 Address
usm-core2:DeviceIPV4AddressWithDomain	app_ressvr.DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	app_ressvr.DeviceIPV6Address	Device IPv6 Address
usm-core2:DeviceIPV6AddressWithDomain	app_ressvr.DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
ProcessID	app_ressvr.ProcessID	Process ID
AccessedViaTcpPort	app_ressvr.AccessedViaTcpPort	Accessed Via Tcp Port
ProcessDistinguishingID	app_ressvr.ProcessDistinguishingID	Process Distinguishing ID
Resources	app_ressvr.capabilities	Capabilities
ContextID	app_ressvr.ContextID	Context ID

StoragePool

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	**CA SDM Attributes**	**User Interface / CI Detail Form**
GroupName	nr.name (http://nr.name)	Name
StoragePool	nr.class	Class
Hardware.StoragePool	nr.family	Family
GroupName|GroupType|usm-core2: DeviceDnsName	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	har_stgpl.DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	har_stgpl.DeviceBiosSystemID	Device Bios System ID
usm-core2:DeviceDnsName	har_stgpl.DeviceDnsName	Device Dns Name
usm-core2:DeviceSysName	har_stgpl.DeviceSysName	Device Sys Name
usm-core2:DevicePhysSerialNumber	har_stgpl. DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	har_stgpl.DeviceMacAddress	Device Mac Address
usm-core2:DeviceIPV4Address	har_stgpl.DeviceIPV4Address	Device IPv4 Address
usm-core2: DeviceIPV4AddressWithDomain	har_stgpl. DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	har_stgpl.DeviceIPV6Address	Device IPv6 Address
usm-core2: DeviceIPV6AddressWithDomain	har_stgpl. DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain
usm-core2:IsHAEnabled	har_stgpl.IsHAEnabled	Is HA Enabled
usm-core2:IsMonitoringMembers	har_stgpl. IsMonitoringMembers	Is Monitoring Members
usm-core2:MaxFailures	har_stgpl.MaxFailures	Max Failures
usm-core2:MemberCriteria	har_stgpl.MemberCriteria	Member Criteria
usm-core2:GroupType	har_stgpl.GroupType	Group Type
usm-core2:BusinessRelevance	har_stgpl.BusinessRelevance	Business Relevance
usm-core2:CapacityInGB	har_stgpl.CapacityInGB	Capacity In GB
usm-core2:RaidLevel	har_stgpl.RaidLevel	Raid Level

StorageVolume

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
usm-core2:StorageID	nr.name	Name
StorageVolume	nr.class	Class
Hardware.StorageVolume	nr.family	Family
usm-core2:StorageID|usm-core2:PortWWName|usm-core2:PortID	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	har_stgvol.DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	har_stgvol.DeviceBiosSystemID	Device Bios System ID
usm-core2:DeviceDnsName	har_stgvol.DeviceDnsName	Device DNS Name
usm-core2:DeviceSysName	har_stgvol.DeviceSysName	Device System Name
usm-core2:DevicePhysSerialNumber	har_stgvol.DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	har_stgvol.DeviceMacAddress	Device MAC Address
usm-core2:DeviceIPV4Address	har_stgvol.DeviceIPV4Address	Device IPv4 Address
usm-core2:DeviceIPV4AddressWithDomain	har_stgvol.DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	har_stgvol.DeviceIPV6Address	Device IPv6 Address
usm-core2:DeviceIPV6AddressWithDomain	har_stgvol.DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain
usm-core2:OSNumeric	har_stgvol.OSNumeric	OS Numeric
usm-core2:ContainingIndex	har_stgvol.ContainingIndex	Containing Index
IsPhysical	har_stgvol.IsPhysical	Is Physical
usm-core2:LogicalUnitNumber	har_stgvol.LogicalUnitNumber	Logical Unit Number
usm-core2:PortID	har_stgvol.PortID	Port ID
usm-core2:PortWWName	har_stgvol.PortWWName	Port WW Name
usm-core2:CapacityInMB	har_stgvol.CapacityInMB	Capacity In MB
usm-core2:IsThinlyProvisioned	har_stgvol.IsThinlyProvisioned	Is Thinly Provisioned
usm-core2:IsDeDupeEnabled	har_stgvol.IsDeDupeEnabled	Is DeDupe Eanbled

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
usm-core2:IsMasked	har_stgvol.IsMasked	Is Masked
usm-core2:MaskedWWNames	har_stgvol. MaskedWWNames	Masked WW Names
usm-core2:RaidLevel	har_stgvol.RaidLevel	Raid Level

TransactionContext

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
ContextName	nr.name (http://nr.name)	Name
TransactionContext	nr.class	Class
Enterprise TransactionContext	nr.family	Family
ContextName|ContextType	nr.system_name	Hostname
ContextType	trn_ctx.ContextType	ContextType

VirtualManager

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
ProductName	nr.name (http://nr.name)	Name
VirtualManager	nr.class	Class
Software.VirtualManager	nr.family	Family
ProductName|ProcessID	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	app_virmgr.DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	app_virmgr.DeviceBiosSystemID	Device Bios System ID
usm-core2:DeviceDnsName	app_virmgr.DeviceDnsName	Device DNS Name
usm-core2:DeviceSysName	app_virmgr.DeviceSysName	Device System Name
usm-core2: DevicePhysSerialNumber	app_virmgr. DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	app_virmgr.DeviceMacAddress	Device MAC Address
usm-core2:DeviceIPV4Address	app_virmgr.DeviceIPV4Address	Device IPv4 Address
usm-core2: DeviceIPV4AddressWithDomain	app_virmgr. DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	app_virmgr.DeviceIPV6Address	Device IPv6 Address
usm-core2: DeviceIPV6AddressWithDomain	app_virmgr. DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
ProcessID	app_virmgr.ProcessID	Process ID
AccessedViaTcpPort	app_virmgr.AccessedViaTcpPort	Accessed Via Tcp Port
ProcessDistinguishingID	app_virmgr.ProcessDistinguishingID	Process Distinguishing ID
ApiVersion	app_virmgr.ApiVersion	Api Version
ContextID	app_virmgr.ContextID	Context ID

VMDataStore

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
StoreName	nr.name	Name
NetworkFileSystem	nr.class	Class
Hardware.VMDataStore	nr.family	Family
StoreName|FilePathUrl	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	har_vmds.DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	har_vmds.DeviceBiosSystemID	Device Bios System ID
usm-core2:DeviceDnsName	har_vmds.DeviceDnsName	Device DNS Name
usm-core2:DeviceSysName	har_vmds.DeviceSysName	Device System Name
usm-core2: DevicePhysSerialNumber	har_vmds. DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	har_vmds.DeviceMacAddress	Device MAC Address
usm-core2:DeviceIPV4Address	har_vmds.DeviceIPV4Address	Device IPv4 Address
usm-core2: DeviceIPV4AddressWithDomain	har_vmds. DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	har_vmds.DeviceIPV6Address	Device IPv6 Address
usm-core2: DeviceIPV6AddressWithDomain	har_vmds. DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain
FilePathUrl	har_vmds.FilePathUrl	File Path Url
CapacityInMB	har_vmds.CapacityInMB	Capacity In MB
IsMultiHost	har_vmds.IsMultiHost	Is Multi Host

Website

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
GroupName	nr.name (http://nr.name)	Name

Common CI Properties (USM)	CA SDM Attributes	User Interface / CI Detail Form
WebSite	nr.class	Class
Software.WebSite	nr.family	Family
usm-core2:HomePage|usm-core2: DeviceBiosSystemID	nr.system_name	Hostname
usm-core2:DeviceAssetNumber	app_website. DeviceAssetNumber	Device Asset Number
usm-core2:DeviceBiosSystemID	app_website.DeviceBiosSystemID	Device Bios System ID
usm-core2:DeviceDnsName	app_website.DeviceDnsName	Device DNS Name
usm-core2:DevicePhysSerialNumber	app_website. DevicePhysSerialNumber	Device Physical Serial Number
usm-core2:DeviceMacAddress	app_website.DeviceMacAddress	Device MAC Address
usm-core2:DeviceIPV4Address	app_website.DeviceIPV4Address	Device IPv4 Address
usm-core2: DeviceIPV4AddressWithDomain	app_website. DeviceIPV4AddressWithDomain	Device IPv4 Address With Domain
usm-core2:DeviceIPV6Address	app_website.DeviceIPV6Address	Device IPv6 Address
usm-core2: DeviceIPV6AddressWithDomain	app_website. DeviceIPV6AddressWithDomain	Device IPv6 Address With Domain
usm-core2:IsHAEnabled	app_website.IsHAEnabled	Is HA Enabled
usm-core2:IsMonitoringMembers	app_website. IsMonitoringMembers	Is Monitoring Members
usm-core2:MaxFailures	app_website.MaxFailures	Max Failures
usm-core2:MemberCriteria	app_website.MemberCriteria	Member Criteria
usm-core2:GroupType	app_website.GroupType	Group Type
usm-core2:HomePage	app_website.HomePage	Home Page
usm-core2:BusinessRelevance	app_website.BusinessRelevance	Business Relevance
usm-core2:DeviceSysName	app_website.DeviceSysName	Device System Name

ComputerSystem

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Note: You can define the Vendor and Model properties through the CA SDM connector policy to manage your configuration items. For more information about these properties, see Post-Installation: Manufacturers and Models.

ComputerSystem (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
Vendor	nr.manufacturer	Inventory tab; Manufacturer

ComputerSystem (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
		(Configure this property in the connector policy to the requirement of your site)
Model	nr.model	Inventory tab; Model (Configure this property in the connector policy to the requirement of your site)
PhysSerialNumber	nr.serial_number	Serial Number
VendorSerialNumber	n/a	n/a
AssetNumber	nr.asset_num	Alternate CI ID
PrimaryDnsName	nr.dns_name	DNS Name
OtherDnsNames	n/a	n/a
SysName	n/a	n/a
PrimaryMacAddress	nr.mac_address	MAC Address
OtherMacAddresses	n/a	n/a
PrimaryIPV4Address	nr.alarm_id	Inventory tab; IP Address
PrimaryIPV6Address	nr.alarm_id (if IPV6 is formatted)	n/a
OtherIPAddresses	n/a	n/a
ComputerName	nr.system_name	Name
SystemType	nr.family	Family
MemoryInGB	har_serx. phys_mem	Attributes tab; Memory Installed
StorageInGB	har_serx. hard_drive_capacity	Attributes tab; Disk Capacity
ProcessorType	har_serx.proc_type	Attributes tab; Processor Type
NumberOfCores	har_serx. number_proc_inst	Attributes tab; Number of Processors Installed
ProcessorSpeedInGHz	har_serx. proc_speed	Attributes tab; Processor Speed
PrimaryOSType	nr.class	Class
PrimaryOSVersion	n/a	n/a
OtherOSDetails	n/a	n/a
Description	nr.description	
usm-core2:OSName	n/a	
PrimaryOSVersion	n/a	
usm-core2:BiosVersion	har_serx.bios_ver	
ProcessorType	har_serx.proc_type	
ProcessorSpeedInGHz		

ComputerSystem (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
	har_serx. proc_speed	
NumberOfCores	har_serx. number_proc_inst	
CreationUserName	nr.creation_user	
CreationTimestamp	nr.creation_date	
PrimaryOSType	nr.class	
LastModTimestamp	nr.last_mod	
MdrElementID	nr.persid (Outbound)	
usm-core2: BusinessRelevance	n/a	
LastModTimeStamp	nr.last_mod	
AdministrativeStatus(New, managed, unmanged)	nr.status.sym [rss]	
UrlParams	"nr"	
usm-core2:NumberOf InterfaceCards	har_serx. number_net_card	
usm-core2:BiosDate	n/a	
usm-core2:OSPatchLevel	har_serx. security_patch_leve l	
StorageInGB	har_serx. hard_drive_capacity	
usm-core2: NumberOfDiskPartitions	n/a	
usm-core2: NumberOfPhysicalDrives	n/a	
usm-core2: NumberOfMemorySlots	har_serx. slot_total_mem	

DatabaseInstance

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

DatabaseInstance (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
DBInstanceName	dat_basx.db_id If db_id is found, then set to nr. system_name	Attributes tab; Database ID or System Name
ProductName	nr.name (http://nr.name)	Name
DBServerType	nr.class	Class

DatabaseInstance (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
ProcessDistinguishingID	dat_basx.db_id	Attributes tab; Database ID
Device properties required (see page 4758)	n/a	n/a

GenericIPDevice

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

GenericIPDevice (USM)	CA SDM Attribute	User Interface (CI detail form)
PrimaryDnsName	nr.dns_name	DNS Name
OtherDnsNames	n/a	n/a
SysName	n/a	n/a
PrimaryMacAddress	nr.mac_address	MAC Address
OtherMacAddresses	n/a	n/a
PrimaryIPV4Address	nr.alarm_id	Inventory tab; IP Address
PrimaryIPV4AddressWithDomain	n/a	n/a
PrimaryIPV6Address	nr.alarm_id (if IPv6 is formatted)	Inventory tab; IP Address (if IPv6 is formatted)
PrimaryIPV6AddressWithDomain	n/a	n/a
OtherIPAddresses	n/a	n/a
OtherIPAddressesWithDomains	n/a	n/a

Idea

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

Idea (USM)	CA SDM Attributes	User Interface
usm-udm:IdeaName	nr.name (http://nr.name/)	Name
usm-udm:IsActive	nr.delete_flag	Active?
usm-udm:Manager	invidex.target_manager	Target Manager
usm-udm:GeneralNotes	invidex.general_notes	General Notes
usm-core2:URI	nr.zinvestment_uri	n/a
usm-udm:Priority	invidex.zudm_idea_priority	SPM Idea Priority
usm-udm:IdeaStatus	invidex.zudm_idea_lifecycle_status	SPM Idea Lifecycle Status
usm-udm:OriginatingRequestor	invidex.zoriginating_requestor	Originating Requestor
usm-udm:RequestID	invidex.zrequest_id	Request ID
usm-core2:CompleteUrl	invidex.zcomplete_url	n/a

Incident

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Incident (USM Type)	CA SDM Attributes	User Interface
AssignedID	cr.ref_num	Text on button bar (left side)
Urgency	n/a	Urgency
Impact	cr.impact; imp.sym	Impact
CalculatedPriority	cr.priority; pri.sym	Priority
Open Timestamp	cr.target_start	<bop_dump>
CallbackTimestamp	cr.call_back_date	Call Back Date/Time
Resolution Timestamp	cr.resolve_date	Resolve Date (above tabs)
Closure Timestamp	cr.close_date	Close Date (above tabs)
ChargebackID	n/a	n/a
RootCause	cr.rc	n/a
SolutionUrls	soln_log	n/a
IncidentCategory	cr.category	Incident Area
IsMajor	cr.major_incident	Major Incident
IncidentStatus	cr.status; cr.sym	Status
CreationDocUrl	n/a	n/a
OutageStartTimestamp	cr.outage_start_time	Outage tab; Start Time
OutageEndTimestamp	cr.outage_end_time	Outage tab; End Time
OutageType	cr.outage_type	Outage tab; Type
IsReturnedToService	cr.return_to_service	Outage tab; Return to Service
SymptomCodes	cr.symptom code	Symptom

InterfaceCard

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

Note: You can define the Vendor and Model properties through the CA SDM connector policy to manage your configuration items. For more information about these properties, see Post-Installation: Manufacturers and Models.

InterfaceCard (USM)	CA SDM Attributes	User Interface
Vendor	nr.manufacturer.xym [ca_cmpny]	Inventory tab; Manufacturer (Configure this property in the connector policy to the requirement of your site)

InterfaceCard (USM)	CA SDM Attributes	User Interface
Model	nr.model.sym [mfrmod]	Inventory tab; Model (Configure this property in the connector policy to the requirement of your site)
PhysSerialNumber	nr.serial_number	Serial Number
AssetNumber	nr.asset_num	Alternate CI ID
Device properties required (see page 4760)	n/a	n/a
OSNumeric	n/a	n/a
ContainingIndex	n/a	n/a
IsPhysical	n/a	n/a

Location

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

Location (USM)	CA SDM Attributes	User Interface
LocationName	loc.name (http://loc.name)	Name
Uri	n/a	n/a
CountryCode	loc.country	Address tab; Country
CountryName	loc.country	Address tab; Country
PostalCode	loc.zip	Addresss tab; ZIP/Postal Code
StateOrProvince	loc.state	Address tab; State/Province
City	loc.city	Address tab; City
County	loc.county	n/a
AddressLine1	loc.address1	Address; Address (1)
AddressLine2	loc.address2	Address; Address (2)
AddressLine3	loc.address3	Address; Address (3)
Building	n/a	n/a
Floor	n/a	n/a
Room	n/a	n/a
Description	nr.description, loc.description	
PostalCode	loc.zip	
StateOrProvince	loc.state	
City	loc.city	
County	loc.county	
AddressLine1	loc.address1	
AddressLine2	loc.address2	

Location (USM)	CA SDM Attributes	User Interface
AddressLine3	loc.address3	
Floor	nr.loc_floor	
Room	nr.loc_room	

MediaDrive

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

Note: You can define the Vendor and Model properties through the CA SDM connector policy to manage your configuration items. For more information about these properties, see Post-Installation: Manufacturers and Models.

MediaDrive (USM)	CA SDM Attributes	User Interface
Vendor	nr.manufacturer. xym [ca_cmpny]	Inventory tab; Manufacturer (Configure this property in the connector policy to the requirement of your site)
Model	nr.model.sym [mfrmod]	Inventory tab; Model (Configure this property in the connector policy to the requirement of your site)
PhysSerialNumber	nr.serial_number	Serial Number
AssetNumber	nr.asset_num	Alternate CI ID
Device properties required (see page 4762)	n/a	n/a
OSNumeric	n/a	n/a
ContainingIndex	n/a	n/a
IsPhysical	n/a	n/a
DriveType	nr.class	Class
CapacityInMB	har_stox. media_drive_num	Attributes Tab memory capacity
SupportsRemovableMedia	n/a	n/a
SupportsWrite	n/a	n/a
Description	nr.description	
usm-core2: DriveInterfaceType	har_stox. Disk_type	

OperatingSystem

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

Note: You can define the Vendor and Model properties through the CA SDM connector policy to manage your configuration items. For more information about these properties, see Post-Installation: Manufacturers and Models.

OperatingSystem (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
Vendor	nr. manufacturer	Inventory tab; Manufacturer (Configure this property within the connector policy to the requirement of your site)
ProductName	nr.name (http://nr.name)	Name
Version	nr.version	Attributes tab; Version
MajorVersion	nr. product_version	n/a
MinorVersion	nr. product_version	n/a
BuildNumber	n/a	n/a
Device properties required (see page 4763)	n/a	n/a
NamedAliases	nr.name (http://nr.name)	
Description	nr.description	
OSType	nr.class	

OrganizationEntity

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

OrganizationEntity (USM Type)	CA SDM Attributes	User Interface
GroupName	n/a	Name
MemberCriteria	n/a	n/a
Category	n/a	n/a
OrgType	n/a	n/a

PrimaryPhoneNumber	org.phone_number	Primary Phone Number
OtherPhoneNumbers	org.phone	Alternate Phone Number
EmailAddresses	org.email_addr	Email Address
WebSites	n/a	n/a

Person

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

Person (USM)	CA SDM Attributes	User Interface
FirstName	cnt.first_name	First Name
MiddleNames	cnt.middle_name	Middle Name
FamilyName	cnt.last_name	Last Name
FullName	cnt.combo_name	n/a
EmployeeID	cnt.userid	Contact ID
UserName	cnt.userid	User ID
JobTitle	cnt.position	Job Title
CompanyName	n/a	n/a
IsActive	cnt.available	n/a
PrimaryPhoneNumber	cnt.phone_number	Notification tab; Telephone Number
OtherPhoneNumbers	n/a	n/a
EmailAddresses	cnt.email_address	Notification tab; Email Address

Port

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

Note: You can define the Vendor and Model properties through the CA SDM connector policy to manage your configuration items. For more information about these properties, see Post-Installation: Manufacturers and Models.

Port (USM)	CA SDM Attributes	User Interface
Vendor	nr.manufacturer.xym [ca_cmpny]	Inventory tab; Manufacturer (Configure this property in the connector policy to the requirement of your site)

Port (USM)	CA SDM Attributes	User Interface
Model	nr.model.sym [mfrmod]	Inventory tab; Model (Configure this property in the connector policy to the requirement of your site)
PhysSerialNumber	nr.serial_number	Serial Number
AssetNumber	nr.asset_num	Alternate CI ID
Device properties required (see page 4764)	n/a	n/a
OSNumeric	n/a	n/a
ContainingIndex	n/a	n/a
IsPhysical	n/a	n/a
PortID	n/a	n/a
CardOSNumeric	n/a	n/a
CardContainingIndex	n/a	n/a
ifindex	n/a	n/a
IfType	net_porx. technology	Attributes tab Technology
IfTypeExtension	n/a	n/a
NomSpeedInBitsPerSec	n/a	n/a
PrimaryMacAddress	nr.mac_address	MAC Address
OtherMacAddresses	n/a	n/a
PrimaryIPV4Address	nr.alarm_id	Inventory tab; IP Address
PrimaryIPV6Address	nr.alarm_id (if IPV6 is formatted)	Inventory tab; IP Address
OtherIPAddresses	n/a	n/a
OtherIPAddressesWithDomains	n/a	n/a
Description	nr.description	
PrimaryIPV4Address, PrimaryIPV6Address or OtherIPAddresses	nr.alarm_id	
PrimaryMacAddress or OtherMacAddresses	nr.mac_address	
usm-core2:IsFullDuplex	n/a	
usm-core2:DuplexIsNegotiated	n/a	

PortfolioApplication

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

PortfolioApplication (USM)	CA SDM Attributes	User Interface
usm-udm:PortfolioAppName	nr.name (http://nr.name/)	Name
usm-udm:IsActive	nr.delete_flag	Active?
usm-udm:AvailabilityStart	invothx.start_date	Start Date
usm-udm:AvailabilityEnd	invothx.finish_date	Finish Date
usm-udm:Manager	invothx.manager	Manager
usm-core2:URI	nr.zinvestment_uri	n/a
usm-udm:OpenForTimeEntry	invothx.zopen_for_time_entry	Open for Time Entry?
usm-udm:Stage	invothx.zudm_stage	SPM Stage

Printer

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

Note: You can define the Vendor and Model properties through the CA SDM connector policy to manage your configuration items. For more information about these properties, see Post-Installation: Manufacturers and Models.

Network Printer (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
Vendor	nr.manuafacturer	Inventory tab; Manufacturer (Configure this property within the connector policy to the requirement of your site)
Model	nr.model.sym [mfrmod]	Inventory tab; Model (Configure this property within the IE Policy file to the requirement of your site)
RetirementTimestamp	nr.retire_date	Attributes tab; Retire Date
SerialNumber	nr.serial_number	Serial Number
VendorSerialNumber	n/a	n/a
AssetNumber	nr.asset_num	Alt CI ID
PrimaryDnsName	nr.dns_name	DNS Name
OtherDnsNames	n/a	n/a
LocalPrintername	nr.system_name	n/a
PrimaryMacAddress	nr.mac_address	MAC Address

Network Printer (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
OtherMacAddresses	n/a	n/a
PrimaryIPV4Address	nr.alarm_id (if IPV4 format)	Inventory tab; IP Address (V4)
PrimaryIPV6Address	nr.alarm_id (if IPV6 format)	Inventory tab; IP Address (V6)
OtherIPAddresses	n/a	n/a
SupportsColor	n/a	n/a
IsPhotoPrinter	n/a	n/a
SupportsDoubleSided	n/a	n/a
SupportsStapling	n/a	n/a
IsScanner	n/a	n/a
IsCopier	n/a	n/a
IsFax	n/a	n/a
FaxNumber	n/a	n/a

Problem

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Problem (USM Type)	CA SDM Attributes	User Interface
AssignedID	cr.ref_num	Text on button bar (left side)
IsActive [transform to "true" or "false"]	n/a	n/a
Urgency [IssueUrgencyEnum]	n/a	n/a
Impact	cr.impact; imp.sym	Impact
CalculatedPriority [IssuePriorityEnum]	cr.priority; pri.sym	Priority
Open Timestamp	cr.target_start_last	<bop_dump>
CallbackTimestamp	cr.call_back_date	Call Back Date/Time

Problem (USM Type)	CA SDM Attributes	User Interface
Resolution Timestamp	cr. resolve_date	Resolve Date (above tabs)
Closure Timestamp	cr.close_date	Close Date (above tabs)
ChargebackID	n/a	n/a
RootCause [Issue Root Cause Enum]	cr.rc	Root Cause (Configure this property in the connector policy to the requirement of your site)
SolutionUrls	n/a	No Knowledge on Problem
ProblemCategory	cr.category	Problem Area
IsMajor	n/a	n/a
Status [Incident Status Enum]	cr.status; cr. sym	Status
CreationDocUrl	n/a	n/a

ProvisionedSoftware

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Note: You can define the Vendor and Model properties through the CA SDM connector policy to manage your configuration items. For more information about these properties, see Post-Installation: Manufacturers and Models.

ProvisionedSoftware (USM)	CA SDM Attribute	User Interface (CI detail form)
Vendor	nr.manufacturer. xym [ca_cmpny]	Inventory tab; Manufacturer (Configure this property in the connector policy to the requirement of your site)
ProductName	nr.name (http://nr. name)	Name
Version	app_extx.version	Attributes tab version
MajorVersion	n/a	n/a
BuildNumber	n/a	n/a
ServiceLevel	n/a	n/a
Locales	n/a	n/a
ProcessorEnvironments	n/a	n/a
OSEnvironments	n/a	n/a
VirtualizationEnvironments	n/a	n/a

ProvisionedSoftware (USM)	CA SDM Attribute	User Interface (CI detail form)
ReleaseType	n/a	n/a
SoftwareCategories	app_extx.category	Attributes tab category
IsLocal		
Device properties required (see page 4768)	n/a	n/a
DeviceIPV6AddressWithDomain	n/a	n/a
ProvisionedForItem	n/a	n/a
SoftwarePathUrl	app_extx. install_dir	Attributes tab Install Directory
ProvisioningMethod	n/a	n/a
MdrElementID	nr.persid (Outbound)	
SoftwarePathUrl	app_extx. install_dir	
CreationTimestamp	nr.creation_date	
AdministrativeStatus = "Missing-InSubseqDiscover"	nr.status.sym [rss]	
usm-core2: BlueprintName	nr.family.sym + nr. class.sym	
SoftwareCategories	app_extx.category	

Request (USM Type)

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Request (USM Type)	CA SDM Attributes	User Interface
DeletionUserName	n/a	n/a
InstanceName	n/a	n/a
TypeName	n/a	n/a
AssignedID	cr.ref_num	Text on button bar (left side)
IsTemplate	n/a	n/a
TemplateUsed	n/a	n/a
Severity	n/a	Severity
Urgency [RequestUrgencyEnum]	n/a	Urgency
Priority	cr.priority; pri.sym	Priority
OpenTimestamp	cr.target_start	<bop_dump>
CallbackTimestamp	cr.call_back_date	Call Back Date/Time

Request (USM Type)	CA SDM Attributes	User Interface
ResolutionTimestamp	cr.resolve_date	Resolve Date (above tabs)
ClosureTimestamp	cr.close_date	Close Date (above tabs)
ChargebackID	n/a	n/a
RootCause	cr.rc	Root Cause
SolutionUrls	soln_log	n/a
RequestStatus	cr.status; cr.sym	Status
RequestCategory	cr.category	Request Area
UserAspect	n/a	n/a
CreationDocUrl	n/a	n/a
IsReturnedToService	cr.return_to_service	Outage tab; Return to Service

Router

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Note: You can define the Vendor and Model properties through the CA SDM connector policy to manage your configuration items. For more information about these properties, see Post-Installation: Manufacturers and Models.

Router (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
Vendor	nr.manuafacturer	Inventory tab; Manufacturer (Configure this property in the connector policy to the requirement of your site)
Model	nr.model.sym [mfrmod]	Inventory tab; Model (Configure this property in the connector policy to the requirement of your site)
SerialNumber	nr.serial_number	Serial Number
VendorSerialNumber	n/a	n/a
AssetNumber	nr.asset_num	Alternate CI ID
PrimaryDnsName	nr.dns_name	DNS name
OtherDnsNames	n/a	n/a
SysName	n/a	n/a
PrimaryMacAddress	nr.mac_address	MAC Address
	n/a	n/a

Router (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
OtherMacAddresses		
PrimaryIPV4Address	nr.alarm_id	Inventory tab; IP Address (V4)
PrimaryIPV6Address	nr.alarm_id	IP Inventory tab; IP Address (V6)
OtherIPAddresses	n/a	n/a
FirmwareVersion	net_roux.rout_prot	Attributes tab; Router Protocol
Redundancy Type	n/a	n/a
FirmwareVersion	net_roux.os_version	
RoutingProtocolTypes	net_roux.rout_prot	
RoutingRedundancyType	n/a	

RunningHardware

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

Note: You can define the Vendor and Model properties through the CA SDM connector policy to manage your configuration items. For more information about these properties, see Post-Installation: Manufacturers and Models.

RunningHardware (USM)	CA SDM Attributes	User Interface
Vendor	nr.manufacturer.xym [ca_cmpny]	Inventory tab; Manufacturer (Configure this property in the connector policy to the requirement of your site)
Model	nr.model.sym [mfrmod]	Inventory tab; Model (Configure this property in the connector policy to the requirement of your site)
PhysSerialNumber	nr.serial_number	Serial Number
AssetNumber	nr.asset_num	Alternate CI ID
Device properties required (see page 4771)	n/a	n/a
OSNumeric	n/a	n/a

RunningHardware (USM)	CA SDM Attributes	User Interface
ContainingIndex	n/a	n/a
IsPhysical	n/a	n/a
Description	nr.description	

Service (USM Type)

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Service (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
ServiceName	nr.name (http://nr.name)	Name
ServiceVersion	serx.version or entservx	Attributes tab; Version
AccessedViaTCPPort	n/a	n/a
BusinessRisk	entservx.business_risk or servx.business_risk	Attributes tab; Business Risk
BusinessImpact	n/a	Attributes tab; Business Impact
ImpactDescription	entservx.business_impact or serx. business_impact	n/a
AvailabilityStart	entservx.availability_start or serx. availability_start	Attributes tab; Availability Start
AvailabilityEnd	entservx.availability_end or serx. lifecycle_state	Attributes tab; Availability End
MdrElementID	nr.persid (OutBound)	
Description	nr.description	
CreationUserName	nr.creation_user (SREL --> cnt.user_name)	
CreationTimestamp	nr.creation_date	
LastModTimestamp	nr.last_mod	
UrlParams	"nr"	
ServiceCapabilities	nr.class	
usm-udm:IsActive	nr.delete_flag	Active?
usm-udm: ServiceManager	entservx.service_manager	Service Manager
usm-core2:URI	nr.zinvestment_uri	n/a
usm-udm: OpenForTimeEntry	entservx.zopen_for_time_entry	Open for Time Entry?
ServiceLifecycleState	entservx.zudm_lifecycle_state	SPM Service Lifecycle State

entservx.availability_start or serx.availability start

Switch

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

> **Note**: You can define the Vendor and Model properties through the CA SDM connector policy to manage your configuration items. For more information about these properties, see Post-Installation: Manufacturers and Models.

Switch (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
Vendor	nr.manuafacturer	Inventory tab; Manufacturer (Configure this property in the connector policy to the requirement of your site)
Model	nr.model.sym [mfrmod]	Inventory tab; Model (Configure this property in the connector policy to the requirement of your site)
SerialNumber	nr.serial_number	Serial Number
VendorSerialNumber	n/a	n/a
AssetNumber	nr.asset_num	Alt CI ID
PrimaryDnsName	nr.dns_name	DNS Name
OtherDnsNames	n/a	n/a
PrimaryMacAddress	n/a	n/a
PrimaryIPV4Address	nr.alarm_id	Inventory tab; IP Address
PrimaryIPV6Address	nr.alarm_id (if IPV6 format)	Inventory tab; IP Address
OtherIPAddresses	n/a	n/a
FirmwareVersion	net_nubx.os_version	Attributes tab; OS version

TimeReporting

The CA SDM Connector maps to the USM types based on the values of the following CA SDM properties.

usm-core2:TimeReporting (USM)	CA SDM Attributes	User Interface
usm-core2:ReportingID	alg.persistent_id or chgalg.persistent_id	n/a
usm-core2:IssueType	cr.type or chg.type	n/a
usm-core2: TimeSpentInHours	alg.time_spent or chgalg.time_spent	Time Spent
usm-core2:StartingDate	alg.time_stamp or chgalg.time_stamp	Date of Activity
Description	alg.description or chgalg.description	User Description
usm-core2:IssueID	alg.call_req_id or chg.persistent_id	n/a
usm-udm:InvestmentURI	nr.zinvesement_uri or chg.zproject_id	n/a
usm-udm:InvestmentType	based on the selection from nr.zinvestment_uri or chg. zproject_id	n/a
usm-core2:ProjectTaskID	chg.zproject_task_id	n/a
usm-udm:OriginatingURL	n/a	n/a
usm-core2:UserID	cnt.userid	Analyst

VirtualSystem

The CA SDM Connector maps to USM types based on the values of the following CA SDM properties.

Note: You can define the Vendor and Model properties through the CA SDM connector policy to manage your configuration items. For more information about these properties, see Post-Installation: Manufacturers and Models.

VirtualSystem (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
Vendor	nr.manufacturer.xym [ca_cmpny]	Inventory tab; Manufacturer (Configure this property in the connector policy to the requirement of your site)
Model	nr.model.sym [mfrmod]	Inventory tab; Model (Configure this property in the connector policy to the requirement of your site)
PhysSerialNumber	nr.serial_number	Serial Number
AssetNumber	nr.asset_num	Alternate CI ID
PrimaryDnsName	dns_name	Virtual Host Name
OtherDnsNames	n/a	n/a

VirtualSystem (USM Type)	CA SDM Attributes	User Interface / CI Detail Form
SysName	n/a	n/a
PrimaryMacAddress	nr.mac_address	MAC Address
OtherMacAddresses	n/a	n/a
PrimaryIPV4Address	nr.alarm_id	Inventory tab; IP Address
PrimaryIPV6Address	nr.alarm_id (if IPV6 format)	Inventory tab; IP Address (if IPV6 format)
OtherIPAddresses	n/a	n/a
ComputerName	nr.name (http://nr.name)	Name
BiosSystemID	har_virx.bios_ver	Attributes tab; Bios Version
Type	n/a	n/a
MemoryInGB	har_virx.phys_mem (SDM no float type)	Attributes tab; Memory Installed
StorageInGB	har_virx.hard_drive_capacity (SDM no float type)	Attributes tab; Disk Capacity
ProcessorType	har_virx.proc_type	Attributes tab; Processor Type
NumberOfCores	har_virx.virtual_processors	Attributes tab; No of Process Installed
ProcessorSpeedInGHz	har_virx.proc_speed	Attributes tab; Processor Speed
PrimaryOSType	nr.class	Class
PrimaryOSVersion	n/a	n/a
OtherOSDetails	n/a	n/a
usm-core2: VirtualizationEnvironment	nr.class	
usm-core2: IsAutomaticallyStarted	n/a	

Attributes tab; No of Processs Installed

Default Port Numbers and Connectivity

The following list shows all of the default port numbers available for each of the components in the CA SDM-CA SOI integration:

Note: The list describes only the default ports. Some of the ports may or may not be applicable for this integration.

CA Catalyst

- Server Container: 7000
- Connector Container: 8080
- Search Server: 7443 (HTTPS)
- Persistence Store (Microsoft SQL database): 1433
- ActiveMQ Server: 61616
- Registry shutdown: 8005
- Registry AJP: 8009
- Registry: 8081, 8443
- Persistence Store (Oracle Database Server): 1521
- Administration UI: 8082
- Administration UI AJP: 8010
- Administration UI shutdown: 8006

CA SDM Server

- Server Tomcat Port: 8080
- SA Tomcat Port: 8070
- SA Tomcat Shutdown Port: 8075
- Shutdown Port: 8085
- CA CMDB Visualizer: 9080
- CA CMDB Visualizer Shutdown Port: 9085

CA SOI

- Shutdown Port: 7095 (Manager)
- Shutdown Port: 7005 (UI Server)
- Tomcat Server Port: 7090 (Manager)
- Tomcat Server Port: 7070 (UI Server)
- SSL Port: 7493 (Manager)
- SSL Port: 7403 (UI Server)

- JDBC Port: 1433
- CMS Server Port: 6400

Relationship and Service Mapping

This topic includes the following information about Relationship and Service Mapping for CA CMDB and CA Configuration Automation integration:

Supported CIs and Relationships

The ServiceDeskManagerConnector_policy.xml and ServiceDeskManager_policySB.xml files contain complete mapping information of the CI and CI relationship data for the integration.

The following table lists the Relationship mapping for the integration:

Parent	Relationship Type	Child Type	CMDB Support?
Service			Yes
	IsHostedBy	ComputerSystem	Yes
	HasDetail	ComplianceStatus	No
	HasContact	Person	Yes
ComputerSystem			Yes
	IsHostFor	ProvisionedSoftware	Yes
	IsHostFor	ComputerSystem	Yes
	IsManagerFor	ComputerSystem	Yes
	HasDetail	ComplianceStatus	No
	HasContact	Person	Yes
	HasDetail	IPConfig	No
	IsComposedOf	Port	Yes
	IsComposedOf	OperatingSystem	Yes
	IsComposedOf	RunningHardware	Yes
	IsComposedOf	Memory	No
	IsComposedOf	MediaDrive	Yes
	IsComposedOf	Processor	No
ProvisionedSoftware			Yes
	HasAccessTo	ComputerSystem	Yes
	HasRequirementFor	ComputerSystem	Yes
Compliance Status			No

Parent	Relationship Type	Child Type	CMDB Support?
Location			Yes
	IsLocationFor	ComputerSystem	Yes
	IsLocationFor	Router	Yes
	IsLocationFor	Service	Yes
VirtualSystem			Yes
Router			Yes
Port			Yes
	HasDetail	IPConfig	No
Cluster			Yes
	HasMember	ComputerSystem	Yes
MediaDrive			Yes
	IsHostFor	File	Yes
Application			Yes
	HasRequirementFor	Port	Yes
	IsConnectedTo	Port	Yes
	IsConnectedTo	Application	Yes
BackgroundProcess			No
	HasRequirementFor	Port	No
	IsConnectedTo	BackgroundProcess	No
RunningHardware			Yes
Memory			No
OperatingSystem			Yes
Processor			No
DiskPartition			No
File			Yes
IPConfig			No
BinaryRelationship			Yes
ApplicationServer			Yes
DatabaseInstance			Yes
GenericIPDevice			Yes
InterfaceCard			Yes
Printer			Yes
Switch			Yes
Person			Yes
OrganizationEntity			Yes
Incident			Supported (Only Outbound)

Parent	Relationship Type	Child Type	CMDB Support?
	IsImpactedBy	(Any Supported CMDB CI)	Supported (Only Outbound)
Problem			Supported (Only Outbound)
	IsImpactedBy	(Any Supported CMDB CI)	Supported (Only Outbound)
Request			Supported (Only Outbound)
	IsImpactedBy	(Any Supported CMDB CI)	Supported (Only Outbound)
ChangeOrder			Supported (Only Outbound)
	IsImpactedBy	(Any Supported CMDB CI)	Supported (Only Outbound)

Service Mapping

The following table lists the mapping for the Services:

Services (CA Configuration Automation)	CA Configuration Automation Schema [acm_svc]	USM:Service	CA SDM Business Service
service uuid	svc_uuid	MdrElementID	nr.persid (Outbound)
service name	svc_name	ServiceName	nr.name (http://nr.name/)
description	descr	Description	nr.description
created by	created_by	CreationUserName	nr.creation_user (SREL cnt.user_name)
creation time	creation_tm	CreationTimestamp	nr.creation_date
business process	business_process	usm-core2: BusinessRelevance **Note:** All CIs contain this field, not only for USM:Service	nr.service_goal
modification time	modification_tm	LastModTimestamp	nr.last_mod
Launch-in-context URL	[acm_svc].svc_name	UrlParams	nr **Note:** This integration only uses the CA SDM object factory for backward compatibility with SSA/Catalyst 2.5.
N/A	N/A	ServiceVersion	serx.version or entservx.version
N/A	N/A	AccessedViaTCPPort	N/A
N/A	N/A	BusinessRisk	entservx.business_risk or servx.business_risk
N/A	N/A	ImpactDescription	entservx.business_impact or serx.business_impact

Services (CA Configuration Automation)	CA Configuration Automation Schema [acm_svc]	USM:Service	CA SDM Business Service
N/A	N/A	AvailabilityStart	entservx.availability_start or serx.availability start
N/A	N/A	AvailabilityEnd	entservx.availability_start or serx.availability start
N/A	N/A	usm-core2: CommonlyKnownNames	nr.asset_num
N/A	N/A	ServiceCapabilities	nr.class Note: For Services, you can also use Alt CI Id
N/A	N/A	ServiceLifecycleState	entservx.lifecycle_state

Post Installation Steps for CA Unified Self-Service

Perform the following optional post-installation steps for USS 14.1.02:

- Customize CA SDM Data Source Property (see page 4780)
- Enable or Disable the Community (see page 4781)
- Enable Clickjacking Filter (see page 4781)

Prerequisites

Create a backup of the *US4SM\OSOP\portal-ext.properties* file.

Note: *US4SM* is the default Unified Self-Service installation directory.

Customize CA SDM Data Source Property

Perform the following steps to customize the CA SDM Data Source Property:

1. Open the *US4SM\OSOP\portal-ext.properties* file and copy the following content at the end of the file:

```
# SDM Datasource Config Fields
# Maximum number of the SDM Fields that can be shown in SDM Datasource config
Fields sections
# If no value/invalid value/ value less than 4 is specified, it will default to
10
sdm.configFields.maxFieldsToShowInConfigOptionsPage = 10
# If you want this property to be tenant specific, prefix the Web ID of the
tenant to the property. It is case-sensitive
# (Web Id can be obtained from the http(s)://server-name:<port-no>/group
/control panel > Portal Instances)
# Example Format:
# someCompany.com (http://someCompany.com).sdm.configFields.
maxFieldsToShowInConfigOptionsPage = 10
```

2. Save the file and restart (see page 1704) the services.

Enable or Disable the Community

Perform the following steps to enable or disable the community:

1. Open *US4SM\OSOP\portal-ext.properties* and copy the following content at the end of the file:

```
# Community On/Off
# Community/Message board feature can be disabled by the setting property
disable.uss.community to true (case sensitive)
# Example - with Multi tenancy
# For a specific tenant, prefix the property with the tenant webID
# For tenants, if the value is not defined or the property is missing,Community
is enabled, by default.

# someCompany.com (http://someCompany.com).disable.uss.community = true

# Example - All other tenant Community will be disabled if the value for the
property is true (case sensitive).
# If the value is not defined or the property is missing, Community is enabled,
by default.

# disable.uss.community = true
```

2. Save the file and restart (see page 1704) the services.

Enable Clickjacking Filter

Follow these steps:

1. Open the *US4SM\OSOP\tomcat-7.0.40\conf\web.xml* file.

2. Search for the text: *Built In Filter Definitions*
   The Built In Filter section appears as follows:
   <!-- ================== Built In Filter Definitions ==================== -->

<filter>
.
.
.
</filter>

3. Add the following filter at the end of the *Built In Filter Definitions* section:

```
<!-- Filter :Restricts framing of USS application in all domains expect the
current domain in which USS is hosted -->
<filter>
<filter-name>ClickjackFilterSameOrigin</filter-name>
<filter-class>org.owasp.esapi.filters.ClickjackFilter</filter-class>
<init-param>
<param-name>mode</param-name>
<param-value>SAMEORIGIN</param-value>
</init-param>
</filter>
<filter-mapping>
<filter-name> ClickjackFilterSameOrigin </filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>
```

4. Save and close the file and restart (see page 1704) the services.

USS Announcements are Formatted Incorrectly for Windows

1. Navigate to the *US4SM\OSOP\tomcat-7.0.40\bin* folder and edit the file *wrapper.conf:*

   a. Modify the variable *wrapper.java.additional.20* value from *-Duser.timezone=GMT* to *-Duser.timezone=sdm-time-zone*
   For Example: '-Duser.timezone=America/Denver'. (Mountain Time)

   b. Save and close the file.

2. Navigate to *US4SM\OSOP* folder and *a*ppend the following content at the end of the *portal-ext.properties* file.

```
#set this to show the announcement date format in 24/12 hr
#format:
# dd-MMM-yy hh.mm (http://hh.mm).ss aa for 12 hr format
# dd-MMM-yy HH.mm (http://HH.mm).ss for 24 hr format
announcement.date.format=dd-MMM-yy hh.mm (http://hh.mm).ss aa
```

3. Save the file and restart (see page 1704) the services.

USS Announcements are Formatted Incorrectly for Linux

1. Navigate to the *US4SM\OSOP\tomcat-7.0.40\bin* folder and edit the file *setupenv.sh*

   a. Modify the variable *Duser.timezone* value from *-Duser.timezone=GMT* to *-Duser.timezone=sdm-time-zone*
   For Example: '-Duser.timezone=America/Denver'. (Mountain Time)

b. Save and close the file.

2. Navigate to *US4SM\OSOP* folder and *a*ppend the following content at the end of the *portal-ext.properties* file.

```
#set this to show the announcement date format in 24/12 hr
#format:
# dd-MMM-yy hh.mm (http://hh.mm).ss aa for 12 hr format
# dd-MMM-yy HH.mm (http://HH.mm).ss for 24 hr format
announcement.date.format=dd-MMM-yy hh.mm (http://hh.mm).ss aa
```

3. Save the file and restart (see page 1704) the services.

For more information about USS enhancements, see CA Service Management Release 14.1.02 Enhancements (see page 69).

Additional Resources

This section contains additional resources that you help you with using CA Service Management.

Content Pack for ITIL CA Service Desk Manager

The Information Technology Infrastructure Library (ITIL®) is a set of books developed by the United Kingdom's Office of Government Commerce (OGC). The books describe an integrated, process based, best practice framework for managing IT services. The current version of ITIL is 2011.

The Content Pack for ITIL for the current release of CA Service Desk Manager provides additional content for CA Service Desk Manager (CA SDM) to fully support the following 15 IT Service Management ITIL 2011 edition processes:

- Availability Management
- Capacity Management
- Change Management
- Event Management
- Financial Management
- Incident Management
- IT Service Continuity Management
- Knowledge Management
- Problem Management
- Release & Deployment Management
- Request Fulfillment
- Service Asset & Configuration Management
- Service Catalog Management

- Service Level Management
- Service Portfolio Management

This document records the content and modifications that are included in the Content Pack. This package includes:

- Schema and object modifications
- New and updated analyst web forms (htmpl files)
- Updated help files (html)
- New CA Process Automation Manager workflows
- New BOXI CA Service Desk universe
- New WebI and Crystal reports

Important! Review the list of schema and data updates included in this package to ensure that your CA SDM environment does not have any conflicts.

For example, if you have already created a “z” table or “z” field with the same name that the installer will configure, it is not recommended to run the installer. See the Schema Updates for information on the schema delivered with this package. Although CA SDM will ignore any schema conflicts deployed with the package, the forms delivered with the package will reference them. See New and Updated HTMPL Forms and Updated Help Files sections for a list of modified forms.
If you already have data in your system as specified in the ITIL Content Data section, the installer may create duplicates. See the ITIL Content Data section for information on what data will be loaded into the server to identify any possible duplication.

Schema Updates

The MDB will be modified to support additional data capturing for ITIL process support. Several fields were added to existing tables and new tables were added to the MDB. The installer will put the updated schema in place for you automatically. When the installer script is run, a schema_done file will be created. The schema_done file is used to identify whether the ITIL schema was added to the server. Flag files will be created under the $NX_ROOT\samples\ITIL_Content_14_1 folder.
A vanilla or out of the box installation or upgrade of CA SDM will not have any schema conflicts. If you have modified your environment, ensure that there are not conflicts with what you have created and what the content pack delivers.
The installer will automatically create schema modifications to the MDB. If matching schema is found in the form of a table or field name, the installer will ignore the attempted update by the content installer and will not modify the site defined field, table or schema definition.
The following updates to the MDB database schema were made. Note that the ‘TABLE’ name column represents the table name as defined in $NX_ROOT/site/ddict.sch. For more information on TABLE name, SQL Name, and Object Name, see the Data Element Dictionary (see page 3496).

TABLE	FIELD	TYPE	Summary of Modification
Change_Request	zcategory_init	STRING 12 REF Change_Category	Initial change category
	zchg_bus_cls	INTEGER REF zchg_bus_cls	Business Classification
	zisRelease	INTEGER REF Boolean_Table	RFC authorization for Release
	zowner	UUID REF ca_contact	Change Owner
	zscope	STRING 1024	Change Order Scope
	zurgency	INTEGER REF Urgency	Urgency of change
Call_Req	zcategory_init	STRING 30 REF Prob_Category	Initial category on the incident, problem or request.
usp_owned_resource	zDML_path	STRING 1024	DML Path
	zSPMLifecycleStage	INTEGER REF zSPMLifecycleStage	SPM Lifecycle Stage
	zactual_budget	INTEGER	Actual Budget
	zbiz_proc_supported	STRING 255	Business processes supported
	zbusiness_approver_group	UUID REF ca_contact	
	zbusiness_impact	INTEGER REF zbusiness_impact	Business Impact
	zbusiness_owners	UUID REF ca_contact	Business Owner
	zbusiness_users	UUID REF ca_contact	Business User
	zcharges_service	INTEGER	CI service charges
	zchg_bus_cls	INTEGER REF zchg_bus_cls	
	zci_cost_category	INTEGER REF zci_cost_category	CI cost category
	zcost_biz_units	STRING 255	Business units where costs should be allocated
	zcost_hw_maintenance	INTEGER	Hardware maintenance cost
	zcost_hw_purchases	INTEGER	Hardware purchases cost
	zcost_personnel	INTEGER	Personnel costs
	zcost_service	INTEGER	Service Cost
	zcost_sw_licenses	INTEGER	Software licenses cost
	zcost_sw_maintenance	INTEGER	Software maintenance cost
	zcost_utility	INTEGER	Utility costs
		INTEGER	Current Monthly Service Cost

TABLE	FIELD	TYPE	Summary of Modification
	zcurrent_monthly_service_cost		
	zcurrentAvailabiity	INTEGER	Current availability
	zcurrentCapacity	INTEGER	Current capacity
	zcurrentPerformance	INTEGER	Current performance
	zcurrent_monthly_service_cost	INTEGER	Current monthly service cost
	zest_budget	INTEGER	Estimated budget
	zpost_program_ROI	INTEGER	Post-Program ROI
	zpre_program_ROI	INTEGER	Pre-Program ROI
	zprevAvailability	INTEGER	Previous availability
	zprevCapacity	INTEGER	Previous capacity
	zprevPerformance	INTEGER	Previous performance
	zprice_service	INTEGER	Service price
	zrevenue_service	INTEGER	Service revenue
	zrelease_package_num	INTEGER	Release package number
	zservice_description	STRING 1024	Service description
	zstakeholders_group	UUID REF ca_contact;	Stakeholders group
	ztechnical_approver_group	UUID REF ca_contact;	Technical approver group
	zvalue_prop	STRING 1024;	Value proposition
usp_organization	zcost_center	SREL cost_cntr	Cost Center
Service_Desc	zKPI1	STRING 255	KPI
	zKPI2	STRING 255	KPI
	zKPI3	STRING 255	KPI
	zagreement_date	LOCAL_TIME	Agreement Date
	zfield_date	LOCAL_TIME	Agreement Start
	zfield_date2	LOCAL_TIME	Agreement End
	zfield_int	INTEGER	Additional field
	zfield_long	STRING 1024	Scope
	zfield_small	STRING 255	Additional field
	zquestion1	STRING 255	Locations Included
	zquestion2	STRING 255	Definitions
	zquestion3	STRING 255	Responsibilities and Dependencies
	zquestion4_short	STRING 50	Additional field

TABLE	FIELD	TYPE	Summary of Modification
	zquestion5_short	STRING 50	Additional field
	ztype	INTEGER REF zservice_type_class	Service Type Classification
zSPMLifecycleStage	description	STRING 255	Description
	sym	STRING 40	Symbol
zbusiness_impact	description	STRING 255	Description
	delete_flag	INTEGER REF Active_Boolean_Table	Active/Inactive
	sym	STRING 60	Symbol
zci_cost_category	description	STRING 255	Description
	sym	STRING 40	Symbol
zservice_type_class	description	STRING 255	Description
	Sym	STRING 60	Symbol
zchg_bus_cls	Description	STRING 255	Description
	Delete_flag	INTEGER REF Active_Boolean_Table	Active/Inactive
	Sym	STRING 60	Symbol

New and Updated HTMPL Forms

Several HTMPL forms were modified to support the ITIL Content. The installer will automatically take a backup of your existing site defined htmpl files before doing a copy and replace of the files noted in the table below. Any matching site defined htmpl files located in $NX_ROOT\site\mods\www\htmpl\web\analyst will be copied to $NX_ROOT\samples\ITIL_Content_14_1\<platform>\backups\<date-time>, where <platform> is either nt or unix. If you do not want to use the updated htmpl files that the installer will provide, you will need to delete the ITIL Content version from $NX_ROOT\site\mods\www\htmpl\web\analyst and replace the it with your original file located in the backups folder. Alternately, you can use the Web Screen Painter to update the ITIL Content version to include your previous updates. The original out of the box htmpl files will not be altered.
The following HTMPL forms were modified as part of the extended ITIL content support.

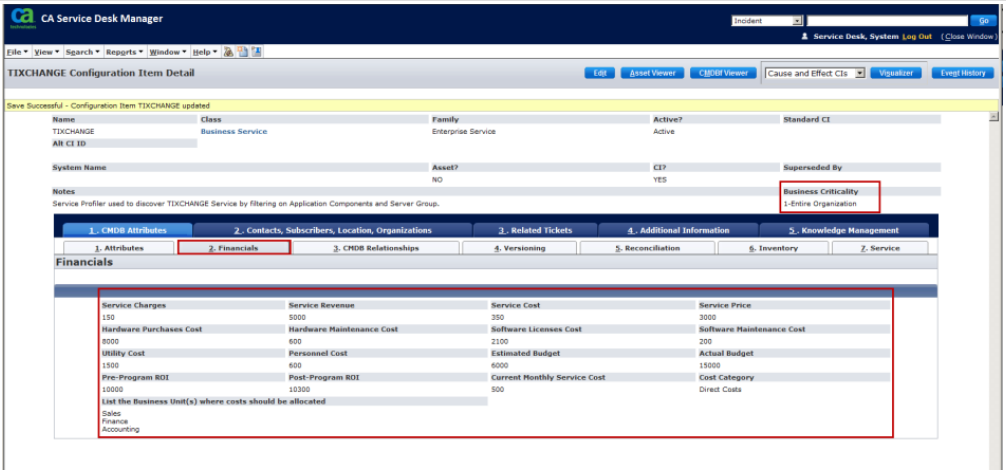
Form Name	Modification Made
cmdb_detail.htmpl	Field added: Business Criticality (Zbusiness_impact)
	Contacts tab renamed to “Contacts, Subscribers”

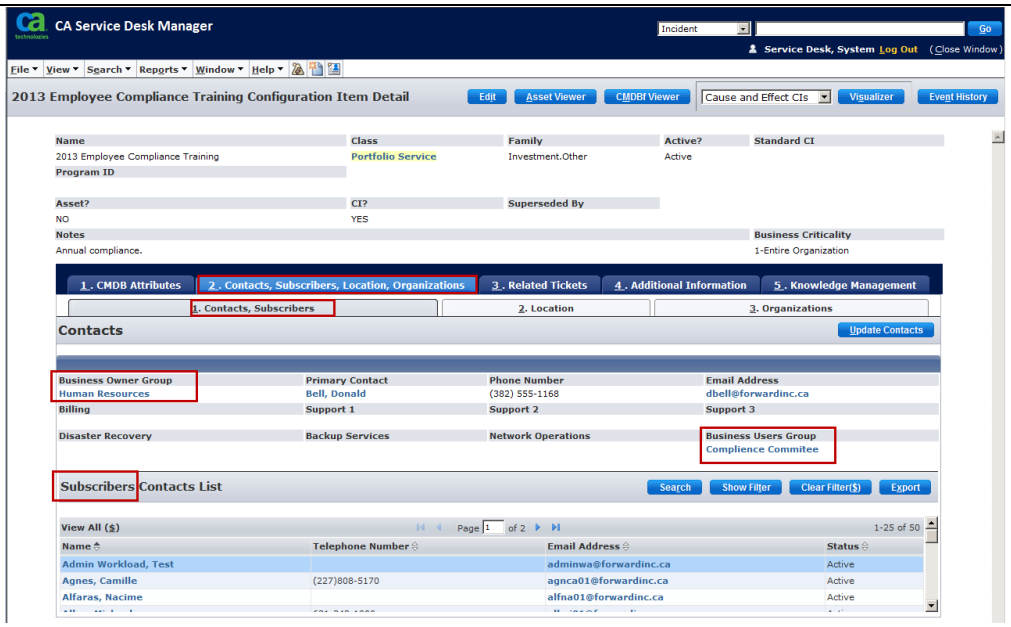
Form Name	Modification Made
cmdbNotebook.htmpl	
detail_chg.htmpl	New function on form to copy category to zcategory_init Fields added: ▪ Business Classification (zchg_bus_cls), ▪ Urgency (zurgency) ▪ Authorized for Release (zisRelease)
detail_cr.htmpl	New function on form to copy category to zcategory_init
detail_in.htmpl	Exposed Created Via (created_via.sym) ootb field New function on form to copy category to zcategory_init
detail_org.htmpl	Field added: Cost Center (zcost_center)
detail_pr.htmpl	Exposed Symptom (symptom_code), Major Problem (major_incident) and Created Via (created_via) ootb fields on form New function on form to copy category to zcategory_init
detail_sdsc.htmpl	Fields added: ▪ Record Type (ztype) ▪ Agreement Start Date (zfield_date) ▪ Agreement End Date (zfield_date2) Tab added with three sub tabs: ▪ Related Contacts (displays all contacts with this ST) ▪ Related Configuration Items (displays all CIs with the ST) ▪ Additional Content: link to zsdsc_tab.htmpl
detail_zbusiness_impact.htmpl	New form with fields: Symbol, Description fields
detail_zchg_bus_cls.htmpl	New form with fields: Symbol, Description fields, last modified by/date
in_relreq_tab.htmpl	New button: Link Incidents, Updated list to show cr and not in
list_chg.htmpl	Search Fields added: ▪ Business Classification (zchg_bus_cls), ▪ Urgency (zurgency) ▪ Authorized for Release (zisRelease)

Form Name	Modification Made
	List updated to include Authorized for Release
list_nr.htmpl	Search Fields added: ▪ Business Criticality (zbusiness_impact) ▪ SPM Lifecycle Stage List updated to include Business Criticality
list_sdsc.htmpl	Search Field added: ▪ Record Type (ztype) List updated to include Type
list_zbusiness_impact.htmpl	New form: Symbol, Description fields
list_zchg_bus_cls.htmpl	New form: Symbol, Description fields
menubar_sd.htmpl	Added to File menu item: New Knowledge Document
nr_cmdb_invothx_tab.htmpl	Fields added: ▪ SPM Lifecycle Stage (zSPMLifecycleStage)
nr_contact_tab.htmpl	Fields added: ▪ Business Owner Group (zbusiness_owners) ▪ Business Users Group (zbusiness_users)
nr_financials_tab.htmpl	New form with fields: zcharges_service, zrevenue_service, zcost_service, zprice_service, zcost_hw_purchases, zcost_hw_maintenance, zcost_sw_licenses, zcost_sw_maintenance, zcost_utility, zcost_personnel, zest_budget, zactual_budget, zpre_program_ROI, zpost_program_ROI, zcurrent_monthly_service_cost, zci_cost_category, zcost_biz_units
nr_inv_tab.htmpl	Field added: ▪ Release Package Number (zrelease_package_num)
nr_loc_tab.htmpl	Field added: ▪ Definitive Media Library Path (zDML_path)
nr_serv_tab.htmpl	Fields added: ▪ Previous Availability (zprevAvailability) ▪ Previous Capacity (prevCapacity) ▪ Previous Performance (prevPerformance) ▪ Current Availability (zcurrentAvailability) ▪ Current Capacity (zcurrentCapacity)

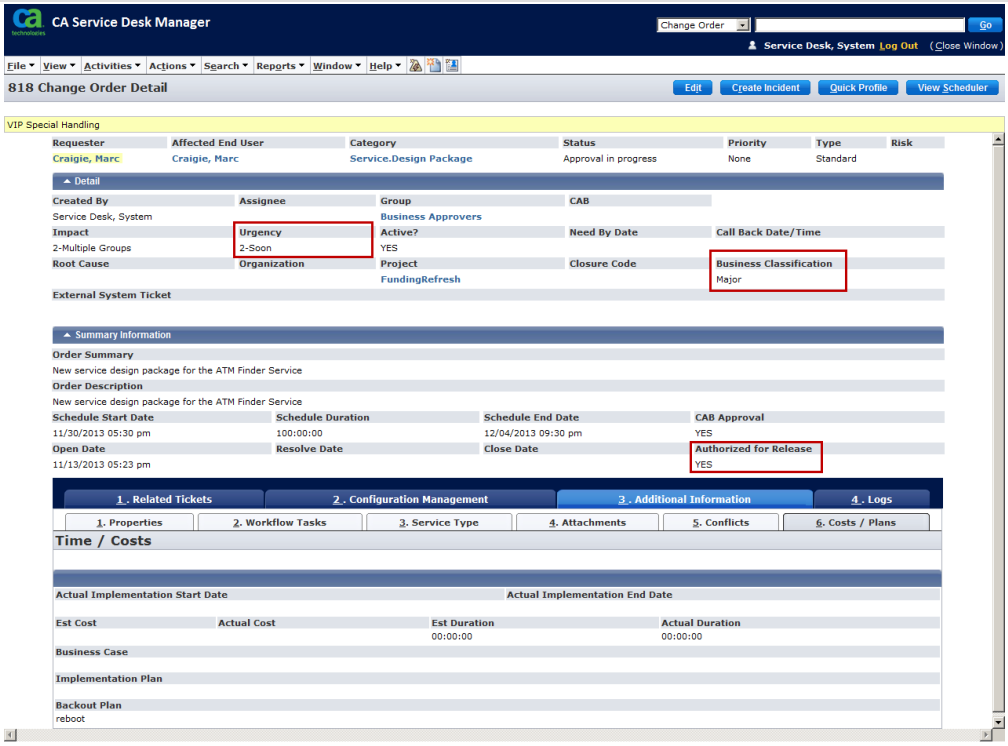
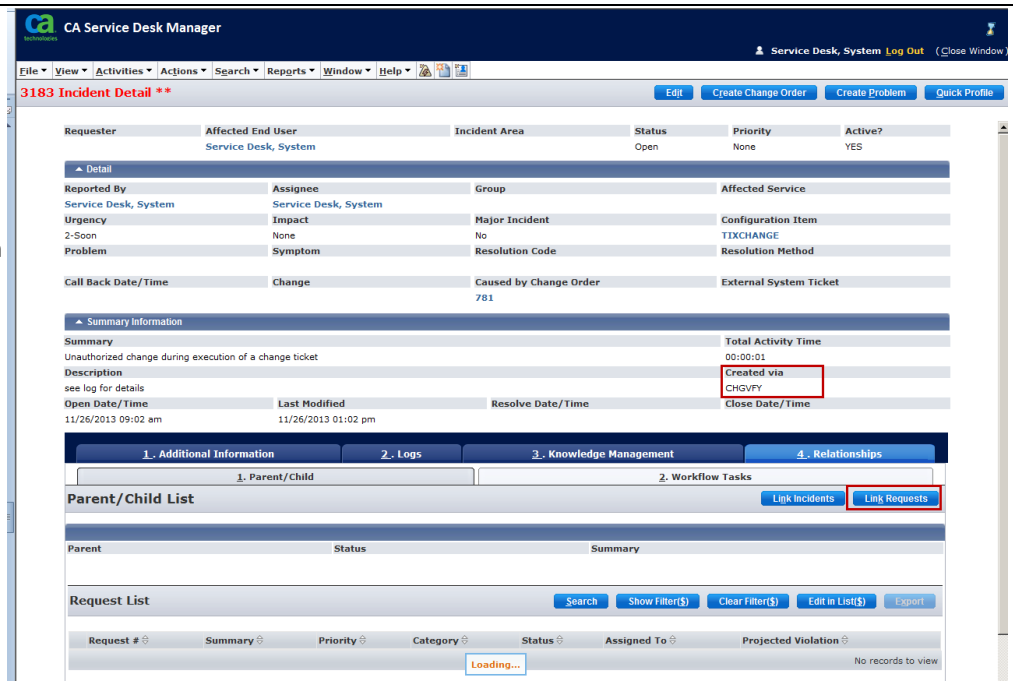
Form Name	Modification Made
	▪ Current Performance (zcurrentPerformance) ▪ Service Description (zservice_description) ▪ Service Value Proposition (zvalue_prop) ▪ Business Processes Supported (zbiz_proc_supported)
xx_prop_tab.htmpl	Field added: ▪ zscope
zsdsc_tab.htmpl	Fields added: ▪ Location included (zquestion1) ▪ Definitions (zquestion2) ▪ Responsibilities and Dependencies (zquestion3) ▪ Scope (zfield_long) ▪ KPI (zKPI1) ▪ KPI (zKPI2) ▪ KPI (zKPI3)

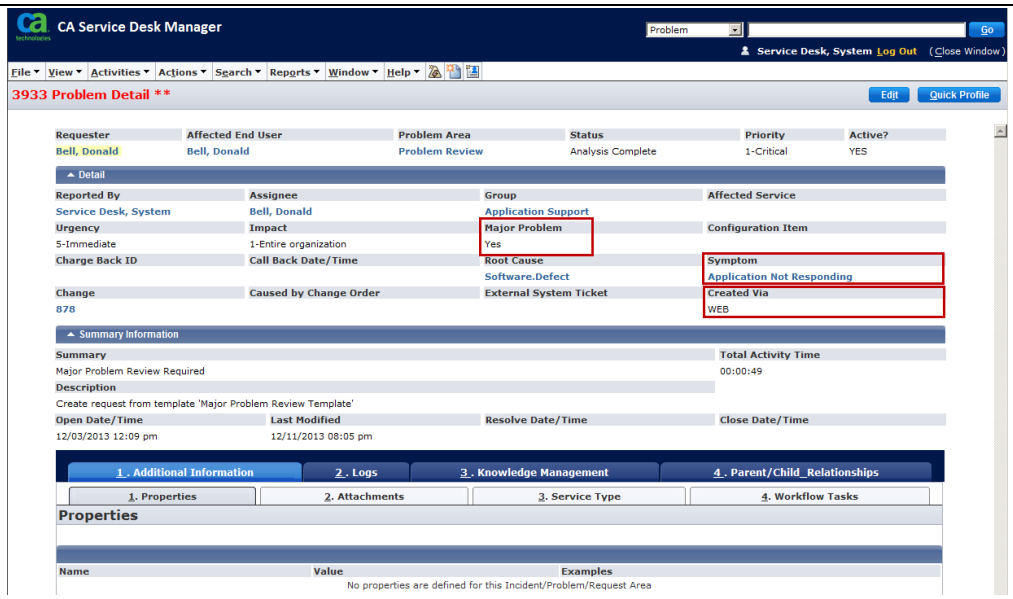
Screen Shots

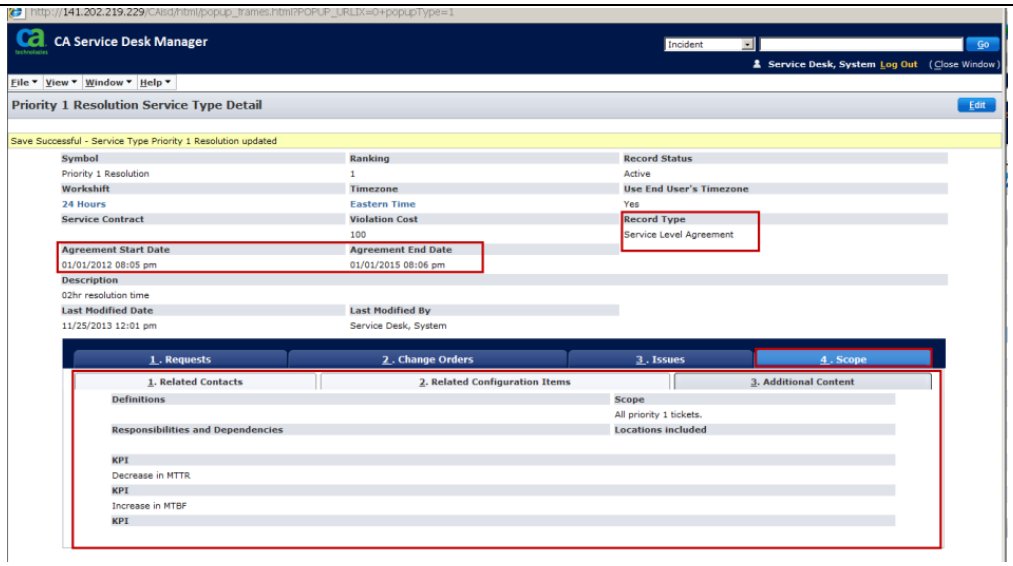
Name	Form View
Configuration Item (cmdb_detail.htmpl) New Field Added: ▪ Business Criticality New Tab	

Name	Form View
	Added: ▪ Financials (all fields on Financials tab are new)
Configuration Item Notebook Tab 2 (cmdbNotebook.htmpl) Rename Tab 2	 ▪ Renamed Contacts to Cont

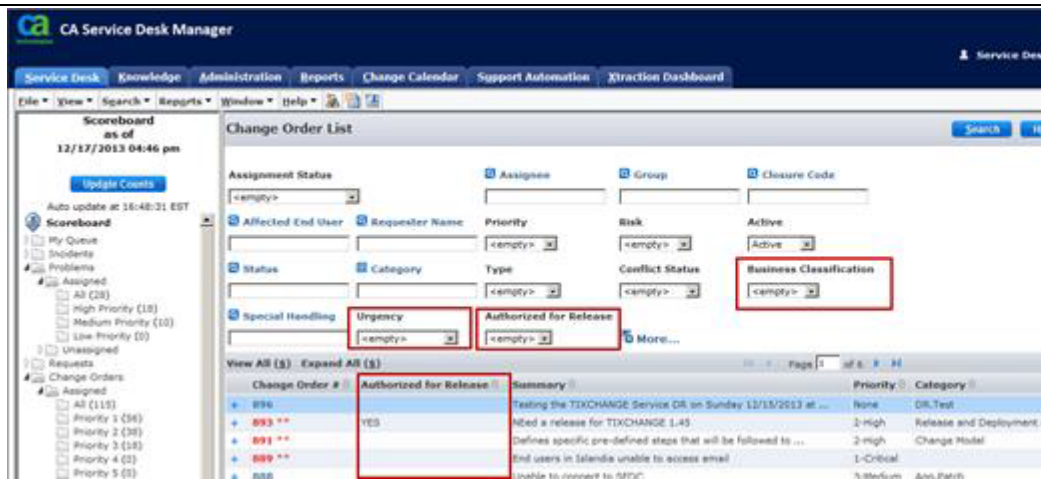
Name	Form View
	acts, Subscribers New Fields Added: ▪ Business Owner Group ▪ Business Users Group
Change Order Detail (detail_chg.htmpl)	New Fields Added: ▪ Business Cl

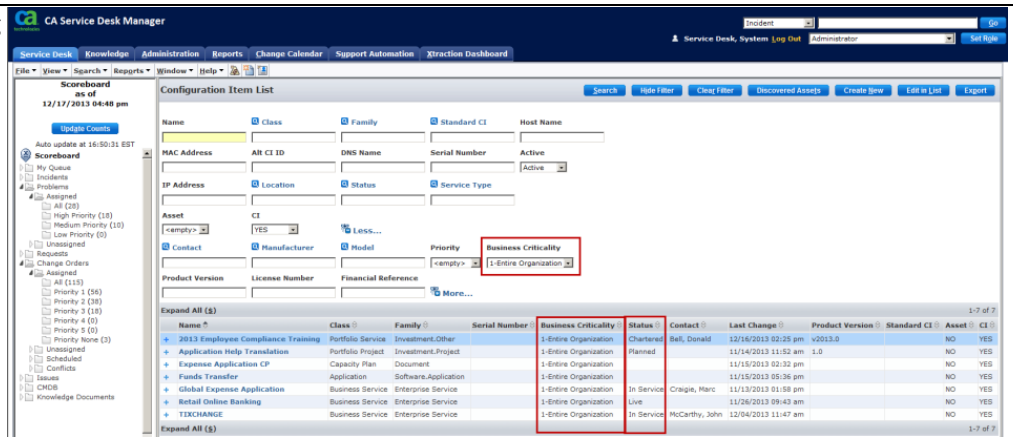
Name	Form View
asification ▪ Urgency ▪ Authorized for Release	
Incident Detail (detail_in.htmpl) Existing Field Exposed: ▪ Created Via New button:	

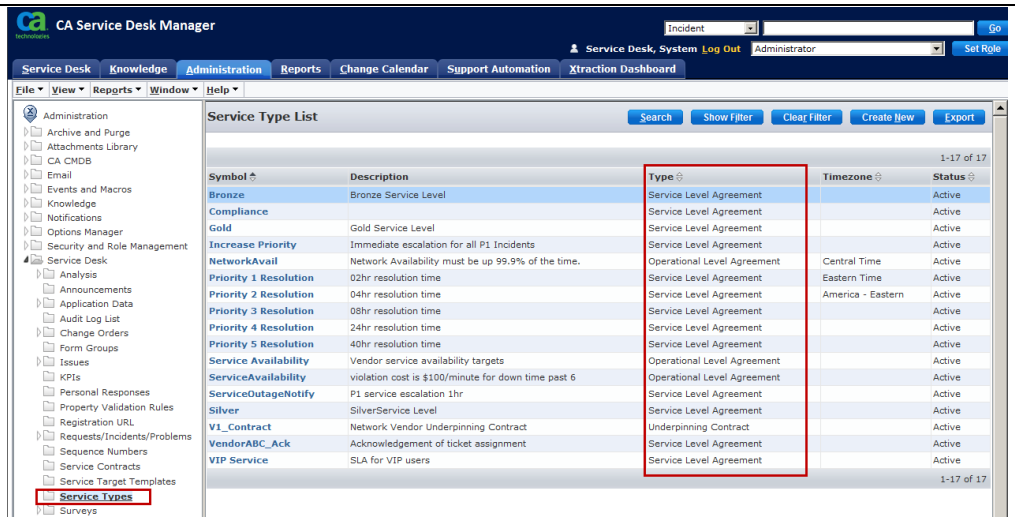
Name	Form View
▪ Link Requests Updated list query to pull the Request List to show both requests and incidents	
Problem Detail (detail_pr.htmpl) New Field added: ▪ Symptom ▪ Created Via ▪ Major	

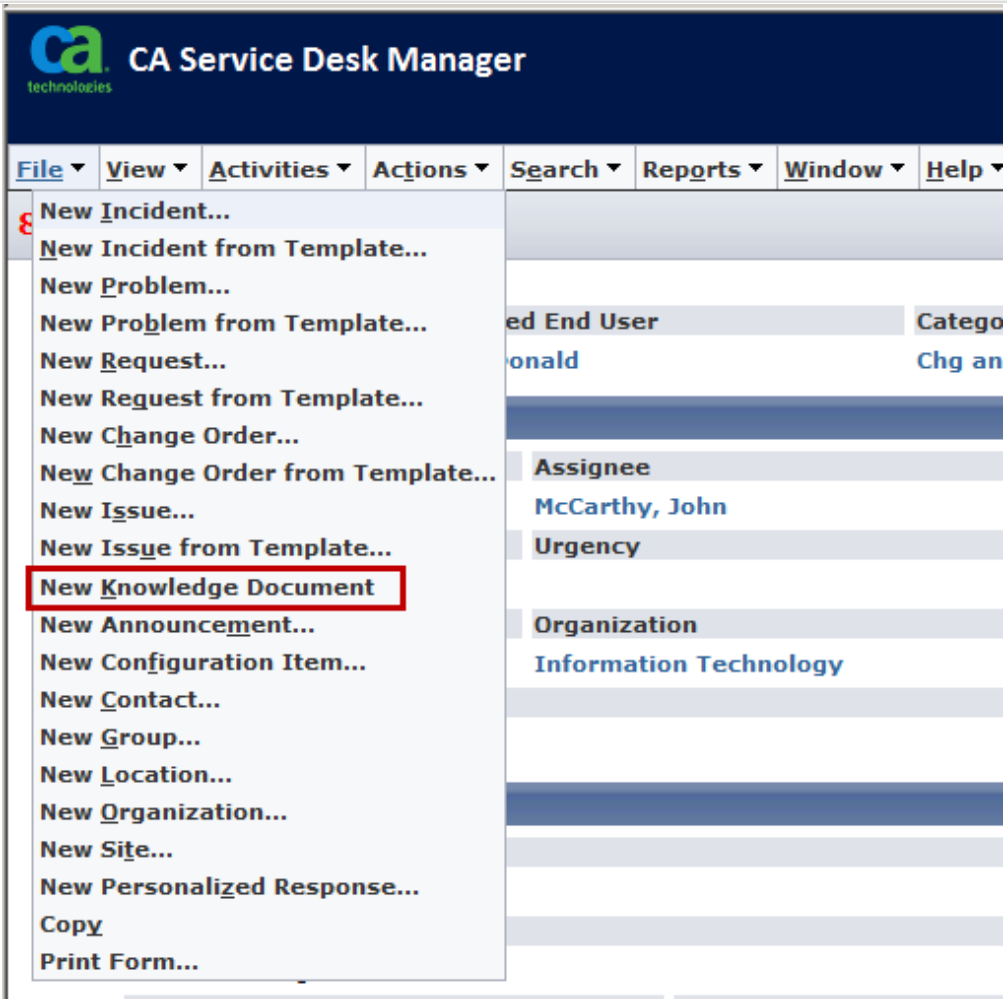
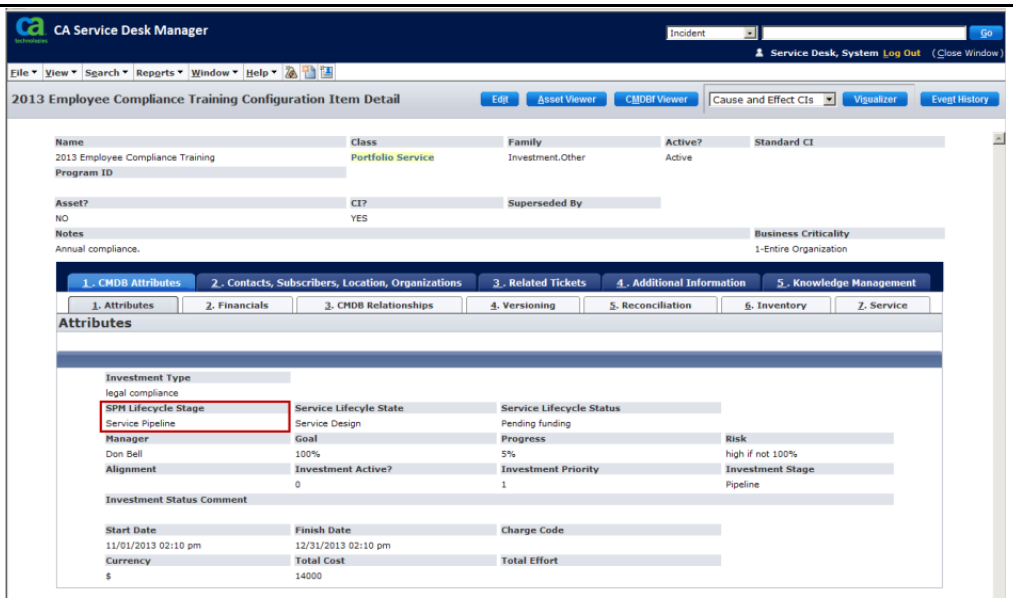
Name	Form View
Problem	
Service Type Detail (detail_sdsc.htmpl) New Fields added: ▪ Record Type ▪ Agreement Start Date ▪ Agreement End Date New Scope Tab Added:	

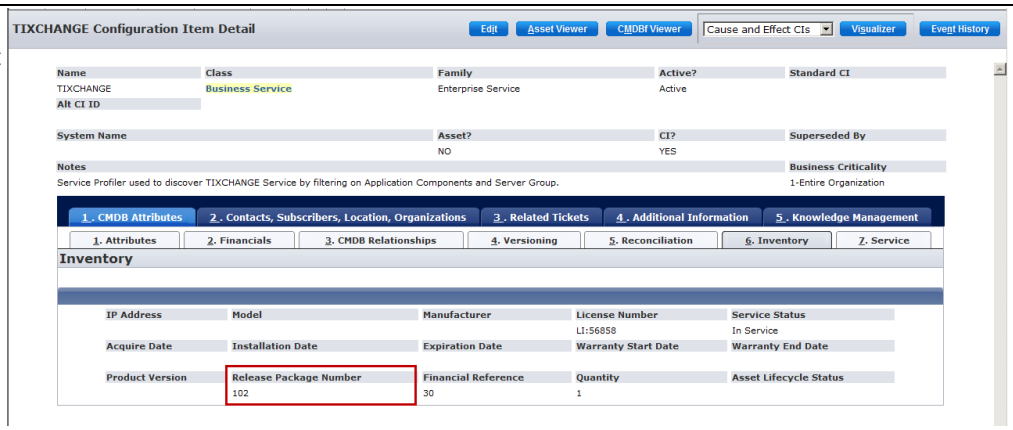
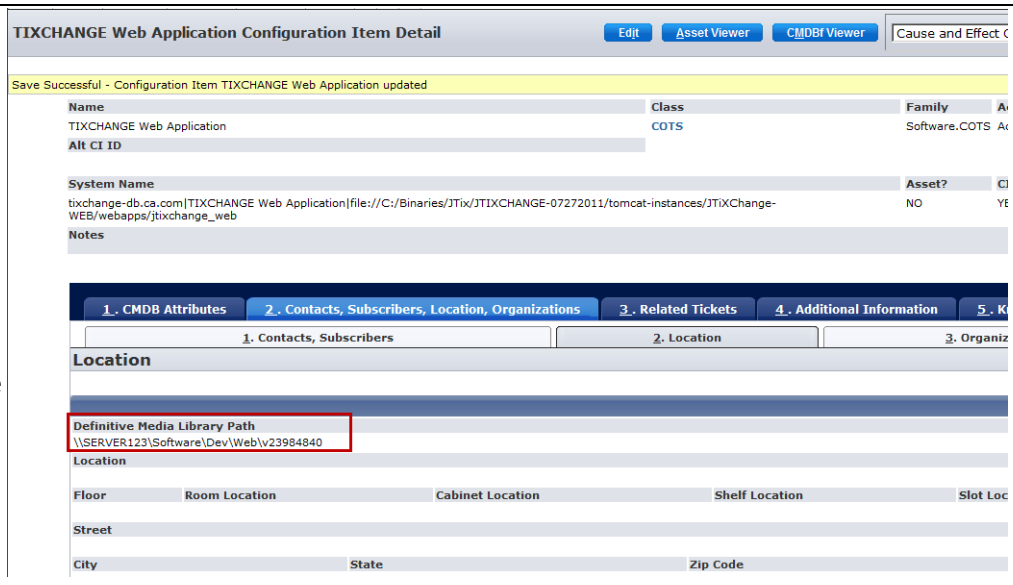
Name	Form View
▪ Related Contacts Tab - displays all contacts with this ST ▪ Related Configuration Items Tab - displays all CIs with the ST	

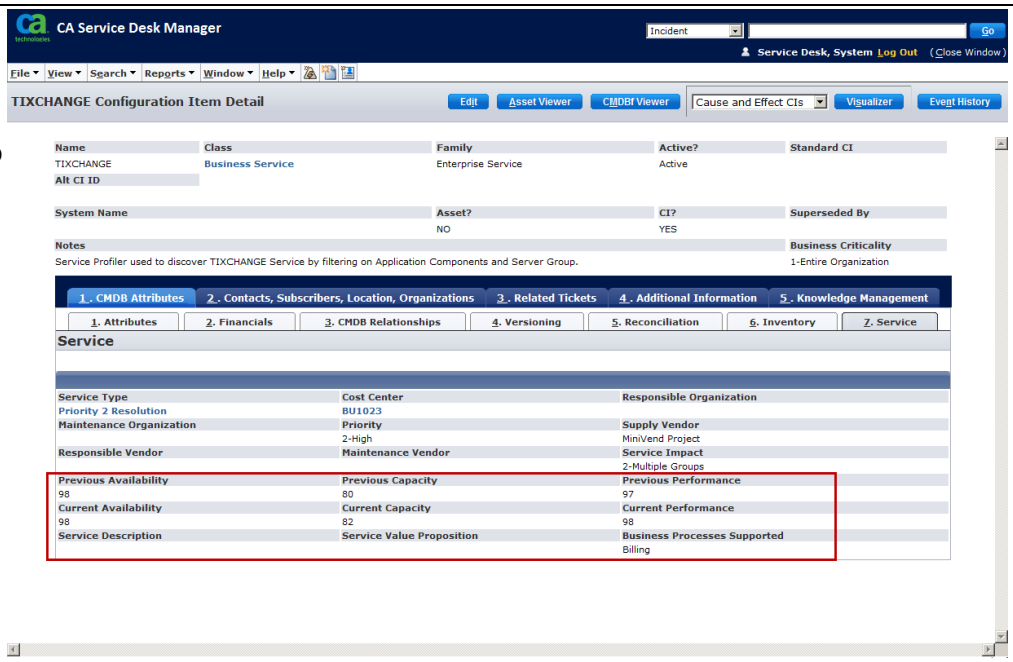
Name	Form View
	▪ Additional Content Tab: link to zsdsc_tab.htmpl
Change Order List (list_chg.htmpl) Search Fields added:	 ▪ Business Classification ▪ Urgency

Name	Form View
Authorized for Release Search List updated: ▪ Authorized for Release	
Configuration Item List: Search Fields added: ▪ Business Criticality Search List updated: ▪ Business Criticality	

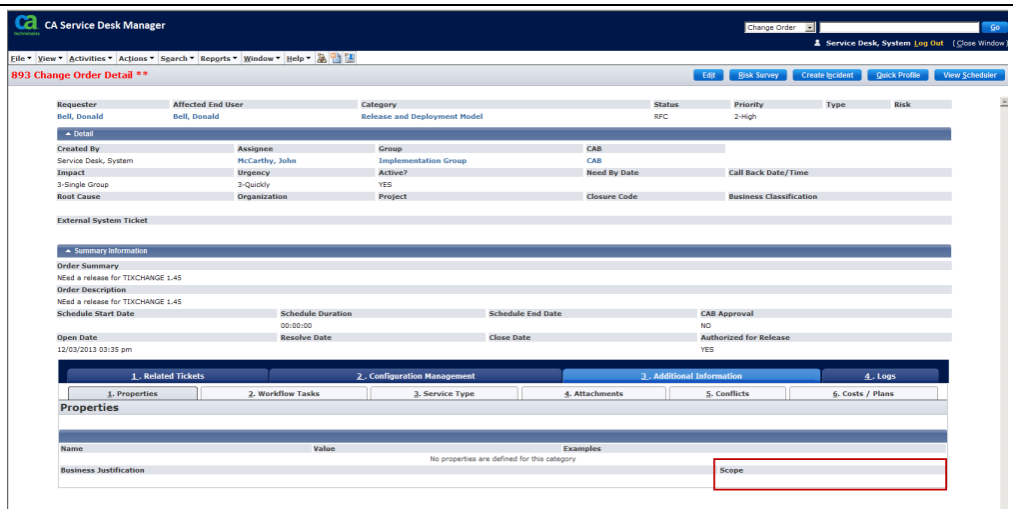
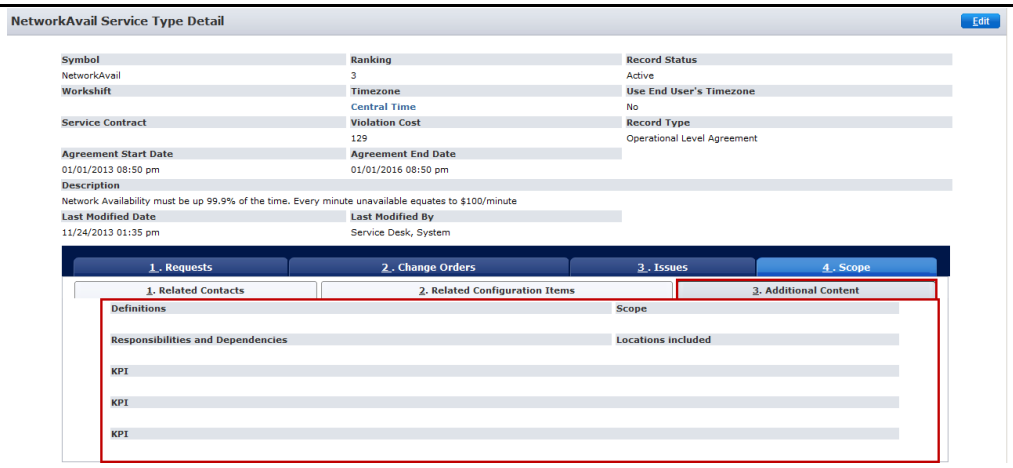
Name	Form View
	▪ Status
Service Type List (list_sdsc.htmpl) Search Field added: ▪ Record Type Search List updated: ▪ Type	
Menu Bar (menubar_sd.htmpl) New File Menu: ▪ New Knowledge Do	

Name	Form View
cument	
Investment. Other Attributes Tab (nr_cmdb_invothx_tab.htmpl) Field Added: ▪ SMP	

Name	Form View
Lifecycle Stage	
CI Inventory Tab (nr_inv_tab.htmpl) Field added: ▪ Release Package Number	
CI Location Tab (nr_loc_tab.htmpl) Field added: ▪ Definitive Media Li	

Name	Form View
brary Path	
CI Service Tab (nr_serv_tab.htmpl) Fields added: ▪ Previous Availability ▪ Current Availability ▪ Previous Capacity ▪ Current Capacity	

Name	Form View
▪ Previous Performance ▪ Current Performance ▪ Service Description ▪ Service Value Proposition ▪ Business Processes Su	

Name	Form View
pported	
Properties Tab xx_prop_tab.htmpl Field added: zscope	
Service Type Additional Content Tab (zsdsc_tab.htmpl) Fields added: ▪ Locations included ▪ Definitions	

Name	Form View
▪ Responsibilities and Dependencies ▪ Scope ▪ 3 KPI fields	Organization Detail (detail_ort.htmpl) Field Added: Cost Center 

ITIL Content Data

Content Data

When the installer script is run, a dataLoad_done file will be created. The dataLoad_done file identifies if the ITIL content was loaded on the server. This will ensure that if the script is re-executed that duplicate data will not be loaded into the system. It also allows CA Support to track if the content exists or not. Flag files will be created under the $NX_ROOT\samples\ITIL_Content_14_1 folder.

The following table shows what tables will have data loaded into them and what the values of that data will be. Before running the install script, ensure that the values listed below do not already exist in your environment. For example, if you already have a Change Category titled “Service. Improvement Plan” you may not want to create a duplicate value in your database when the install script is run. You can manually modify the data that gets loaded into the application by editing the data files located in the ITIL_Content_14_1\files\data folder.

Description: Table	Data File(s)	Values
Activity Type Association : Act_Type_Assoc	Act_Type_Assoc.dat	RFC Authorized for Release
Aliases attr_alias	attribute_alias.dat	map_sdsc_servicetype_class_description map_sdsc_servicetype_class_symbol map_sdsc_violation_cost request_created_via request_sla_macro_predicted category_init (for chg, cr, in, pr) zServiceType configuration_item_financial_number
Macro Conditions: Atomic_Condition	Atomic_Condition.dat Atomic_Cond_Deref.dat	Must have a backout plan to go from Approval in Progress -> Approved status. RFC is Authorized for Release
Categories Change_Category	Change_Category.dat	Change Model DR.Test Release and Deployment Model Service.Design Package Service.Design Package.New Service.Improvement Plan Service.Quality Plan
Change Status Change_Status	Change_Status.dat	Build (zBLD) Test (zTST) Deployed (zDPLY) Incomplete (zINCPL)

Description: Table	Data File(s)	Values
Change Status Transitions chg_trans	chg_trans_input.dat chg_trans_upd.dat chg_trans_Deref.dat	Approval in progress -> Approved (updated) Build->Test Test->Deploy Deploy->Closed Implemented->Closed Implementation in progress->Implemented Implementation in progress->Deployed RFC->Build Build->Rejected Build->Incomplete Test->Approval in progress
CI Status Codes: ca_resource_status	ca_resource_status.dat	Analyzed Approved Chartered Defined In Development Live Pipeline Retired
Incident, Problem, and /or Request Status: Cr_Status	cr_status.dat	Pending Major Problem Review Pending Fulfillment
Request Status Transition cr_trans	cr_trans.dat	Approved (PRBAPP)-->Pending Fulfillment (zPendRul)
Knowledge Categories: O_INDEXES	O_INDEXES_deref.dat O_INDEXEX_input.dat O_INDEXES_load.dat	Availability Plans Capacity Plans Compliance CSI Register Disaster Recovery Plans DML Known Errors Release and Deployment Service Lifecycle Knowledge Articles Service Quality Plan
Problem Status Transition pr_trans	pr_trans_input.dat pr_trans_Deref.dat	Pending Major Problem Review to Closed Pending Major Problem Review to Cancelled Pending Major Problem Review to Fixed Pending Major Problem Review to Known Error Pending Major Problem Review to Problem Closed

Description: Table	Data File(s)	Values
		Fixed to Pending Major Problem Review Analysis Complete to Pending Major Problem Review Resolved to Pending Major Problem Review
Indicent, Problem, Request Categories: Problem_Category	Prob_Category.dat	Incident Model Knowledge.Broken Link Problem Model Problem Review User.Complaint User.Compliment Service.Improvement Plan Service.Quality Plan Service.Development Service.Outage Service.Portfolio
Macros: Spell_Macro	spell_macro.dat	'Backout Plan <> NULL' RFC Authorized for Release
Survey Answers : Survey_Answer_Template	ITIL_Survey_Answer.dat Survey_Answers_Deref.dat	view ITIL_Survey_Answer.dat file for details
Survey Questions : Survey_Question_Template	ITIL_Survey_Question.dat Survey_Questions_Deref.dat	view ITIL_Survey_Question.dat file for details
Survey: Survey_Template	Survey_Step1_pdm_load.dat	Request Fulfillment Survey Service Desk Quality Survey
Role: Usp_role	usp_role.dat	Release and Deployment Management Role
Link Roles and Reports: usp_role_web_form	usp_role_web_form_input.dat web_form_obj_Deref.dat	inc_priority_detail inc_priority
Web Reports: usp_web_form	usp_web_form.dat	Active Incident by Priority - Detail Active incident by priority
Business Impact: zbusiness_impact	zbusiness_impact.dat	5-One person 4-Small group 3-single group 2-multiple groups 1-entire organization
Business Classification: zchg_bus_cls	zchg_bus_cls.dat	Minor Significant Major Business Classification
CI Cost Category: zci_cost_category	zci_cost_category.dat	

Description: Table	Data File(s)	Values
		capital operational direct, indirect fixed, variable unit costs
Type of Service Agreement: zservice_type_class	zServiceTypeClassData.dat	SLA (Service Level Agreement) OLA (Operational Level Agreement) UC (Underpinning Contract)
Portfolio lifecycle stages: zSPMLifecycleStage	zSPMLifecycleStage.dat	Service Catalog Service Pipeline Retired Service
Menu Tree Resource: usp_menu_tree_res	usp_menu_tree_res.dat	Business Classification Business Impact

Additional Content Data

Templates

The following data is not supplied automatically by the ITIL Content installer, however it is recommended that you manually add the following templates to your CA SDM application to further support the incident, request, problem, change, and release and deployment ITIL processes

Object	Suggested Name /Title	Suggested Default Data	Description	How-to Documentation
Incident Template	Incident Model for <insert type of Incident> For example: Incident Model for Printer Repair	Incident Area = <any>	Contains the pre-defined steps that should be taken for dealing with a particular type of Incident. Further supported through incident status transitions.	CA SDM online help, Section on 'Create an Incident Template'
Incident Template	User Compliment	Incident Area = User. Compliment	Used to record user compliments received from interaction with analyst.	CA SDM online help, Section on 'Create an Incident Template'
Incident Template	User Complaint	Incident Area = User. Complaint	Used to record user complaints received from interaction with analyst.	CA SDM online help, Section on 'Create an Incident Template'

Object	Suggested Name /Title	Suggested Default Data	Description	How-to Documentation
Request Template	Knowledge Document Update	Request Area = Knowledge. BrokenLink	Request to update knowledge documents that have been flagged with a broken link.	CA SDM online help, Section on 'Create a Request Template'
Request Template	New Service Request	Request Area = <any>	Contains the pre-defined steps that should be taken for dealing with a service request. Further supported through request status transitions.	CA SDM online help, Section on 'Create a Request Template'
Problem Template	Problem Model for <insert type of Problem> For example: Problem Model for Known Error	Problem Area = <any>	Use for the resolution of dormant and underlying problems. Further supported through problem status transitions.	CA SDM online help, Section on 'Create a Problem Template'
Problem Template	Major Problem Review	Problem Area = Problem Review	Major Problem Review Required	CA SDM online help, Section on 'Create a Problem Template'
Change Order Template	Change Model for <insert type of change> For example: Change Model for New Hires	Category = <any> Change Type = Normal	Defines specific pre-defined steps that will be followed to manage a Change. Further supported through change status transitions.	CA SDM online help, Section on 'Create a Change Order Template'
Change Order Template	Release and Deployment Model	Category = Release and Deployment Model	Defines specific pre-defined steps that will be followed to manage a Release. Further supported through the CA Process Automation Workflow, Change and Release Management, when that workflow is linked to the Release and Deployment Model Change Category.	CA SDM online help, Section on 'Create a Change Order Template'
Change Category	Release and Deployment Model	Properties: ▪ Is this a known or scheduled disaster recovery test? ▪ Does the count towards the	Properties added to support the gathering of data.	CA SDM online help, Section on 'Define Change Order Categories'

Object	Suggested Name /Title	Suggested Default Data	Description	How-to Documentation
		yearly failover test requirements? ▪ Was the failover plan followed? ▪ How long did the failover test occur for? ▪ Was the failover successful? ▪ Was failback implemented?		

Administrative Data

The following data is not supplied automatically by the ITIL Content installer, however it is recommended that you manually add the following Administrative Data to your CA SDM application to further support the incident, request, problem, change, and release and deployment ITIL processes

Object	Suggested Name /Title	Suggested Default Data	Description	How-to Documentation
Change Category	Release and Deployment Model	Properties: ▪ Is this a known or scheduled disaster recovery test?	Properties added to support the gathering of data.	CA SDM online help, Section on 'Define Change Order Categories'

Object	Suggested Name /Title	Suggested Default Data	Description	How-to Documentation
		▪ Does the count towards the yearly failover test requirements? ▪ Was the failover plan followed? ▪ How long did the failover test occur for? ▪ Was the failover successful? ▪ Was failback implemented?		
Knowledge Document	Test Checklist	Knowledge Category = Disaster Recovery Plans	Test checklists should be created and stored under relevant knowledge categories.	CA SDM online help, Section on 'Create Knowledge Documents'
Knowledge Document	Technical and Service Information	Knowledge Category = Service Quality Plan	Record technical and service related information under relevant knowledge categories.	CA SDM online help, Section on 'Create Knowledge Documents'
Knowledge Document	Plans	Knowledge Categories = Availability Plans, Capacity Plans, Disaster Recovery Plans	Record plans under relevant knowledge categories.	CA SDM online help, Section on 'Create Knowledge Documents'
Knowledge Document	Procedures	Knowledge Categories = Compliance	Record procedures under relevant knowledge categories.	CA SDM online help, 'Section on 'Create Knowledge Documents'
CI Class	Design Package	Family = Service	Service Design Package	CA SDM online help, Section on 'Configuration Item Classes'
Menu Tree Resource	Business Impact	Sample Business Impacts are provided with the Content Pack for ITIL for CA SDM.	If you would like to add to the content we provided, we recommend doing so via a menu tree resource for 'Business Impact', under the Administration Tab->Service Desk->Application Data -> Codes	'Menu Trees', as well as the CA SDM online help, section on 'Create a Menu Tree Resource'

Object	Suggested Name /Title	Suggested Default Data	Description	How-to Documentation
Menu Tree Resource	Business Classification	Sample Business Classifications are provided with the Content Pack for ITIL for CA SDM.	If you would like to add to the content we provided, we recommend doing so via a menu tree resource for 'Business Classification, under the Administration Tab->Service Desk->Application Data -> Codes	'Menu Trees', as well as the CA SDM online help, section on 'Create a Menu Tree Resource'

Updated Help Files

Several help files were updated to support the extended ITIL content. Help data is in standard HTML files, not HTMPL templates, so the web engine cannot dynamically change file references. Since there is no /CAisd/site/mods/help subdirectory, all modified help files will be copied to /CAisd/help. For example: $NX_ROOT\bopcfg\www\wwwroot\help\web. The installer will back up the original html files to $NX_ROOT\samples\ ITIL_Content_14_1\files\help.
If you have modified any of the following help files you will want to review the Summary of Modifications column below to understand what was modified and decide whether to use the out of the box version or the supplied modified file. The original files will be backed up under the $NX_ROOT\samples\ITIL_Content_14_1\Backups folder and the modified version will be to /CAisd /help by the installer.
Due to the structure of help files, any patch or future version of CA SDM that delivers any of the same help files included in the content pack will be over ridden with the version included in the patch or new release.

HTML HELP FILE	Summary of Modifications
add_act_to_co.html	Updated summary text
add_act_to_inc.html	Updated summary text
add_act_to_prob.html	Updated summary text
add_act_to_req.html	Updated summary text
chg_order_fields.html	Added Authorized for Release
CI_inv_flds.html	Added Release Package Number
CI-svc_flds.html	Also added Service Description and Business Processes Supported
ci_tabs.html	Update tab name to Contacts, Subscribers Added Financials Tab
CI-flds.html	Field documented: Business Criticality
	Field documented: DML Path

HTML HELP FILE	Summary of Modifications
CI-loc_info.html	
CI-srch_flds.html	Field documented: Business Criticality, SPM Lifecycle Stage
CI-svc_flds.html	Field documented: SPM Lifecycle Stage, Service Value Proposition field, Previous Availability, Previous Capacity, Previous Performance, Current Availability, Current Capacity, Current Performance
CO-use_temp.html	Description updated
CO-srch_flds.html	Added Authorized for Release
co_tabs.html	Properties updated, Cost/Plans updated
create_act_not.html	Added created_via
create_quick_close_ticket.html	Note sample quick close templates for complaint and compliment.
create_svc_type.html	Add instructions for how to Edit a Service Type
def_CO_cat.html	Document categories: Service.Improvement Plan, Service.Quality Plan
define_knowfiles_fields.html	Field documented: Doc ID
define_status_transitions.html	Added pending major problem review note
from_inc.html	Documented the Create Incident button
Inc_def_areas.html	Document categories: Service.Improvement Plan, Service.Quality Plan
INC-use-temp.html	Documented template: Create Incident Model Template Note that templates can be used to log events from monitoring tools.
incident_fields.html	Field documented: created_via, open date/time fields added
manage_CI_classes.html	Document new CI Classes: Design Package, Portfolio Service
manage_co_chg_win.html	

HTML HELP FILE	Summary of Modifications
manage_know_cat.html	Data documented: knowledge categories of Availability Plans, Capacity Plans, Known Errors, business cases, Compliance, CSI Register, Service Improvement and Quality Plans, Release & Deployment, Workaround
organization_fields.html	Help page added for organization fields
prob_fields.html	Fields documented: symptom, created via, Major Problem
PROB-use_temp.html	Documented templates
REQ-flds.html	Field documented: RFC open date/time field, Service Development listed as a request area example.
req-inc-prob-area_flds.html	Field documented: symbol
role_list.html	Removed reference to “ITIL v3” and just used “ITIL”
search_for_documents.html	Added summary sentence
survey_templates.html	Note 2 OOTB surveys: Service Desk Quality Survey and Request Fulfillment Survey
svc_type_flds.html	Fields documented: Record Type, Agreement Start Date, Agreement End Date, and Scope tab
service_type_tabs.html	Document the new Scope tab
view_req.html	Button documented: ‘Create Incident’ button

New Reports

Find the following additional reports under Folder Name (Public Folders-> CA Reports -> CA Service Desk).

Report Name	Report Description	Report Type
Business Impact	Ticket list per service CI showing business impact.	Web Intelligence Report

Report Name	Report Description	Report Type
Incident Closure Category Summary Report	Incident report showing the initial categorization and the closing categorization. This report shows the total count of Incidents with pie charts showing categories with the highest number of re-classifications.	Web Intelligence Report
Problem Closure Category Summary Report	Problem report showing the initial categorization and the closing categorization. This report shows the total count of problems with pie charts showing categories with the highest number of re-classifications.	Web Intelligence Report
Service Request Closing Category Summary Report	Service Request report showing the initial categorization and the closing categorization. This report shows the total count of problems with pie charts showing categories with the highest number of re-classifications.	Web Intelligence Report
RFC Closure Category Summary Report	Request for Change report showing the initial categorization and the closing categorization. This report shows the total count of RFCs with pie charts showing categories with the highest number of re-classifications.	Web Intelligence Report
SLA Management Report	Service level management report showing different trends based on ticket type and service.	Web Intelligence Report
SLA Management Report Previous 12 months	Service level management report showing different trends based on ticket type and service for the last 12 months.	Web Intelligence Report
SLA Management Report Previous 3 Months	Service level management report showing different trends based on ticket type and service for the last 3 months.	Web Intelligence Report
SLA Management Report Previous 7 Days	Service level management report showing different trends based on ticket type and service for the last 7 days.	Web Intelligence Report
SLAs To be validated Today	Service levels that will be violated today.	Web Intelligence Report
SLAs Violating Today Summary Report	Summary report showing SLAs with a validation date of today.	Web Intelligence Report
Violations Report	Service type violations report. Filter available for selecting OLA, SLA, or UC.	Crystal Report
SLA Monitoring Chart	Service Level Agreement Monitoring chart to show service level performance history.	Crystal Report
Change Order Closure Category	Detailed report to track the initial and closing categorization on change requests.	Crystal Report

Incident Closure Category Report	Detailed report to track the initial and closing categorization on incidents.	Crystal Report
Incidents Closure Category Count Report	High level summary to view the total count of categorization differences between initial and closing categorization on incidents.	Crystal Report
Problems Closure Category Report	Detailed report to track the initial and closing categorization on problems.	Crystal Report
Request Closure Category Report	Detailed report to track the initial and closing categorization on requests.	Crystal Report
Service Requests by Requests Area	Graph showing the number of requests over a period of time grouped by request area.	Crystal Report
Trend: RFCs and Affected CIs	Report to show Change Orders with associated Configuration Items. Sort filters are by earliest Open Date, Latest Open Date, CI, CI Class Type or CI Family.	Crystal Report
Service Availability and Performance Violation Report	Service type violations report for service availability and performance tickets. Filter available for created via, category, and affected end user.	Crystal Report

For the out of the box reports, see CA Service Desk Manager Reports (see page 4784)

Options Manager

Options Manager settings can be found under the Administrative tab in the Options Manager folder. It is recommended to install the following Options Manager Options when using the ITIL Content Pack for CA SDM:

- employee_intf_incident_support
- catalog_server

CA Process Automation Workflows

When the installer script is run, a subdirectory is created called ‘workflows’. It contains two files.
1.) An XML file with all of the Processes, SRF’s, IRF’s, and Custom Operators required for implementation of the process.
2.) A PDF file with setup, configuration, integration, and Best Practices information. It also contains a screenshot demo of all Process Definitions ‘In Action’. Note that this content builds upon the existing ‘CA Process Automation Sample Process Definitions for CA SDM’. The chart below outlines those process definitions that are new with the Content Pack for ITIL for CA SDM, the ones that are updated for the Content Pack for ITIL for CA SDM, and those that existed previously in an OOB install of CA SDM.

Process Name	New /Updated	What it does
Request Fulfillment	New	The goal of this process is to provide a foundation for Request Fulfillment which aligns to ITIL 2011.
Change and Release Management	Updated	This process definition adds Release and Deployment Management to the existing Change Management process included in the 'CA Process Automation Sample Process Definitions for CA SDM'. The goal of this process is to provide a foundation for Change and Release and Deployment Management which aligns to ITIL 2011. Provides the ability to manage a Change Management process for all Standard, Normal or Emergency Changes from the initial Request for Change through to its deployment and Post Implementation Review. It analyzes the 'Type' of Change Order and associated 'Risk' Level to determine what level of approvals are necessary for Change implementation. Should be called from a Change Category.
Change Management	Existing, no updates	Replaced with Change and Release Management Process Definition
Order PC	Existing, no updates	Sample building block which walks you through approval steps for and end user to raise the request and fulfill a PC Order.
Problem Analysis	Existing, no updates	The goal of this process definition is to make a decision regarding if an RFC /Change should be created for a given problem. Once the problem assignee has finished researching the problem and has a suggested solution, they will fill out this problem survey and provide a recommendation. The survey should give the approver a good idea of the impact of the problem and if it is necessary to resolve it through Change Management. The idea of a Problem Pain/Value Analysis comes from ITIL v3 and should help CA better align to ITIL.

Install the ITIL Content for CA Service Desk Manager

Run the installer for one of the following instances:

- Fresh installation of CA SDM ITIL content
- When you upgrade to CA SDM 14.1, the ITIL content is also migrated, but some schema files may be missing. To rectify this issue, you need to run the installer.

Follow these instructions to run the installer.

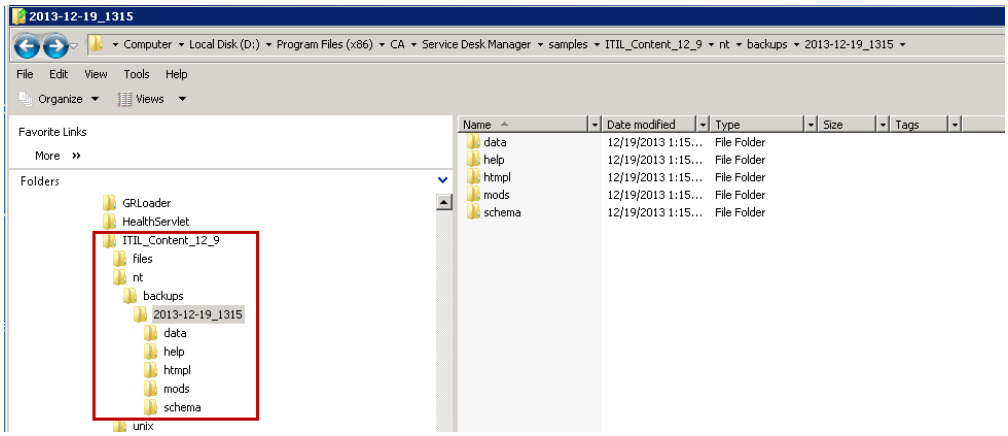
Verify the Prerequisites

Perform the following pre-requisite steps before running the installer:

1. Ensure you have a functional version of CA SDM running in a test or development environment. It is not recommended to run the installer on a production instance of CA SDM without strict change control and validation testing first.

2. Unzip ITIL_Content_14_1.zip to the $NX_ROOT\samples folder on your CA SDM primary server and all CA SDM standby servers if using Advanced Availability.

3. Backups will be made under $NX_ROOT \samples\ITIL_Content_14_1\<platform>\backups\<date-time> folder



4. Review the content included with the installer as defined throughout this document.

5. Log files will be created under the $NX_ROOT\logs folder.

Run the Installer

Install the Content on Windows

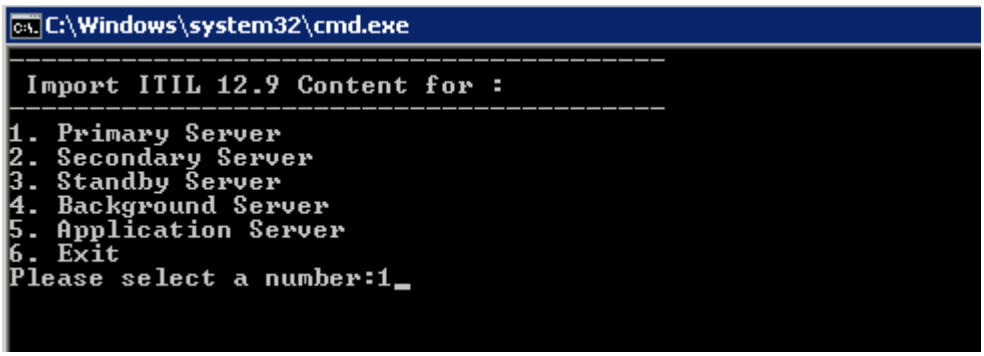
For Conventional Environment – Primary Server Install

1. Login to the Primary CA SDM Server.

2. Navigate to $NX_ROOT\Samples\ITIL_Content_14_1\nt and execute setup.bat

3. Select Run

4. Select the appropriate option based on your server environment. For example, select 1 if you are installing onto your Primary Server:



5. The install will initiate and start CA SDM if necessary.

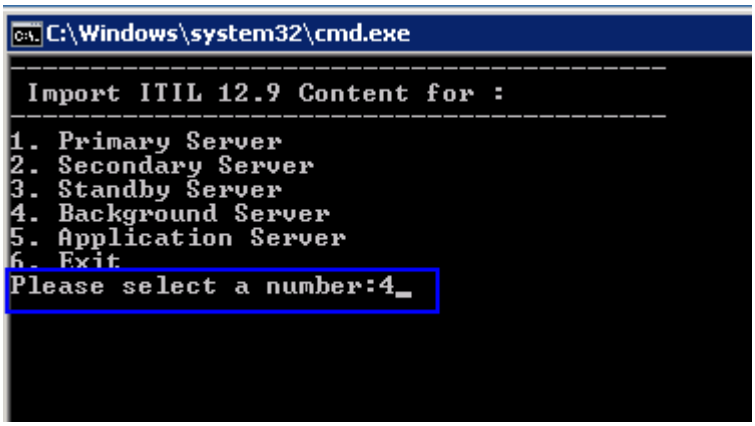
For Advanced Availability Environment

ITIL Data will be loaded only if the Primary or Background options are selected, and is executed only one time.
Complete the following steps on the original Standby Server:

1. Login to the Standby Server. After the deployment of the ITIL Content pack on this machine, a failover will be performed and this server will become the new Background server.

2. Navigate to $NX_ROOT/samples/ITIL_Content_14_1/nt and execute setup.bat

3. When prompted, select option 4, for Background Server



4. Click "Y" to do fail-over during pdm_publish.

5. On the original Background Server, now Standby Server

    a. Login to the “new” Standby Server (Former Background)

    b. Navigate to $NX_ROOT/samples/ITIL_Content_14_1/nt and execute setup.bat

    c. When prompted, select option 3 for Standby Server.

6. On the Application Servers,

    a. Login to the Application Server

b. Navigate to $NX_ROOT/samples/ITIL_Content_14_1/nt and execute setup.bat

c. When prompted, select option 5 for Application Server

Install the Content on UNIX

Note: CA SDM services will restarted during the deployment process, ensure that the environment variables (PATH - Oracle executables, ORACLE variables) are set in the terminal /console before executing the setup.sh file

For Conventional Setup:

1. Login to the Primary Server
2. Navigate to /opt/CAisd/samples/ITIL_Content_14_1/unix and execute ./setup.sh
3. Select appropriate option based on server.

For Advanced Availability Setup:

1. Login to Standby Server and select Option as Background server, as during pdm_publish we do failover and make this server as Background.
2. Navigate to /opt/CAisd/samples/ITIL_Content_14_1/unix and execute ./setup.sh
3. Click "Y" to do fail-over during pdm_publish
4. Login to Standby Server (Former Background, Now standby after fail-over) or Application Server
5. Select appropriate option based on server.

Note:

- Ensure that the ITIL Content pack is deployed on the new background server. If not, perform a manual failover, using the command: pdm_server_control -b
- ITIL Data will be loaded only in Primary and Background option. So it has to execute only once.
- Data Extract and Load will happen only on Background and Primary Server only. Choose option carefully.

Install CA Process Automation Workflows

CA Process Automation workflows are located under $NX_ROOT\Samples\ITIL_Content_14_1\files\workflows\

Follow these steps:

1. Import CA SDM CA Process Automation Process Definitions (see page 4824)
2. Configure SDM Dataset for Sample Process Definitions (see page 4828)
3. Increase 'Maximum Number of Log Messages' in CA Process Automation (see page 4832)
4. Verify CA SDM Options Manager Options (see page 4833)
5. Troubleshooting Note (see page 4834)

Install ITIL Reports

Find the BIAR report is under <NX_ROOT>\Samples\ITIL_Content_14_1\files\reports\. CA Business Intelligence also includes BIConfig, a utility that can be used to add, modify, delete, and otherwise affect various BusinessObjects objects. BIConfig is generally used during a CA product's installation or maintenance process and is run in a batch mode.

Important! If you have migrated from CA SDM 12.9, ensure that you have installed CA Business Intelligence 4.1 SP3 for the ITIL content reports.

The BiConfig utility takes inputs from the command line and an XML file that describes the configuration updates to be performed on the Business Objects environment.

Follow these steps:

1. Create the directory c:\BIConfig on your local machine where BOXI is installed.
2. Copy and Unzip the contents of the BIConfig folder from the Business Intelligence Embedding Kit [<ServiceDeskManager_Installation_CD>\ca_tps.nt\CABO\biconfig.zip] to C:\BIConfig.
3. Copy "xml_biar_import.xml" file from <NX_ROOT>\Samples\ITIL_Content_14_1\files\reports\ folder to BIConfig folder.
4. Edit "xml_biar_import.xml" file and specify necessary values for path of the biar file located, DB Username, DB password, System DSN (data source name) specified under Windows Administrative Tools -> Data Sources (ODBC drivers). Find the xml_biar_import.xml file under <NX_ROOT>\Samples\ITIL_Content_14_1\files\reports\ folder.

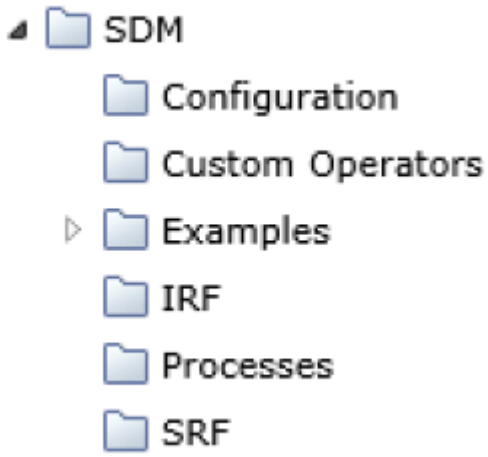
   The BIConfig utility is run from the command line, can be invoked silently, and requires the JRE. Invoke BIConfig by executing the BIConfig.bat file using the syntax and example shown below. Log messages are written to the BIConfig.log file.

Syntax:
biconfig.bat -h "<BOXI-hostname>" –u "<BOXI username>" –p "<BOXI pwd>" -f "xml_biar_import.xml"

Example:
C:\biconfig>biconfig.bat -h "itcse-r121" –u "Administrator" –p "BOXI1" -f "xml_biar_import.xml"

Import CA SDM CA Process Automation Process Definitions

Note: These process definitions are imported to the CA SDM directory off of the root directory in PAM, as shown in the screenshot below. This is the same place that the CA SDM CA Process Automation Sample Process Definitions available in $NX_ROOT/samples /CA_PAM_Workflows, are imported to. The Process Definitions that are provided with the Content Pack for ITIL for CA SDM build upon and enhance those previously provided in the directory below, if you have already imported the CA SDM CA Process Automation Sample Process Definitions. Be sure to take a backup prior to importing the process definitions provided with the Content Pack for ITIL for CA SDM.



Before we begin: The XML File we will be importing into PAM in the instructions to follow includes the following components to ensure that these flows will function properly. This XML file can be found at: $NX_ROOT/samples/ITIL_Content_14_1/files/workflows /ContentPackITILCASDM141PAMWF.XML

CA Process Automation Object	What it Does
Custom Operators	Pre-configure parameters for repeated use in many different processes
Global Datasets	

CA Process Automation Object	What it Does
	Define and group variables used as parameters for module and job invocations. Datasets can define common parameters-such as application locations, passwords, and profile names-required by modules and applications on a network. These variables can be easily configured so that Processes and scheduling can be efficiently updated to reflect changes in an application environment.
Interaction Request Forms (IRF's)	Provides field and other UI elements with which users can enter information required to execute an Operator or continue a process.
Processes	Graphically describe the ordering and dependencies for Operations Performed by modules. Operators are represented in a Process graphically and by Operators with links and dependencies that define the order and logic for performing tasks in a Process. These processes are samples with which you can use as-is, or modify to meet your business needs.
Start Request Forms (SRF's)	Define shortcuts to allow an operator to invoke processes manually using the Management Console. Start Request Form objects define custom dialogs that prompt operators for the values of parameters required by the associated project. These are also used by CA SDM to launch CA Process Automation Process definitions by attaching a definition to a Request/Incident/Problem Area, or Change Order/Issue Category.

Follow these steps:

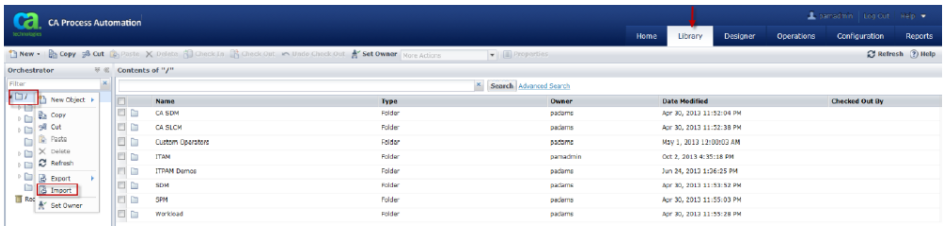
1. To manually import the sample process definitions do the following. Login to CA Process Automation by either navigating to Start, Programs, CA, <*CA Process Automation*>, Start CA Process Automation locally on the CA Process Automation Server, or via the direct URL if you are launching it from a server remote from CA SDM:

    a. Login as 'itpamadmin' on an upgraded instance of CA Process Automation, or 'pamadmin' on a fresh install of CA Process Automation 4.1 SP01 or above.

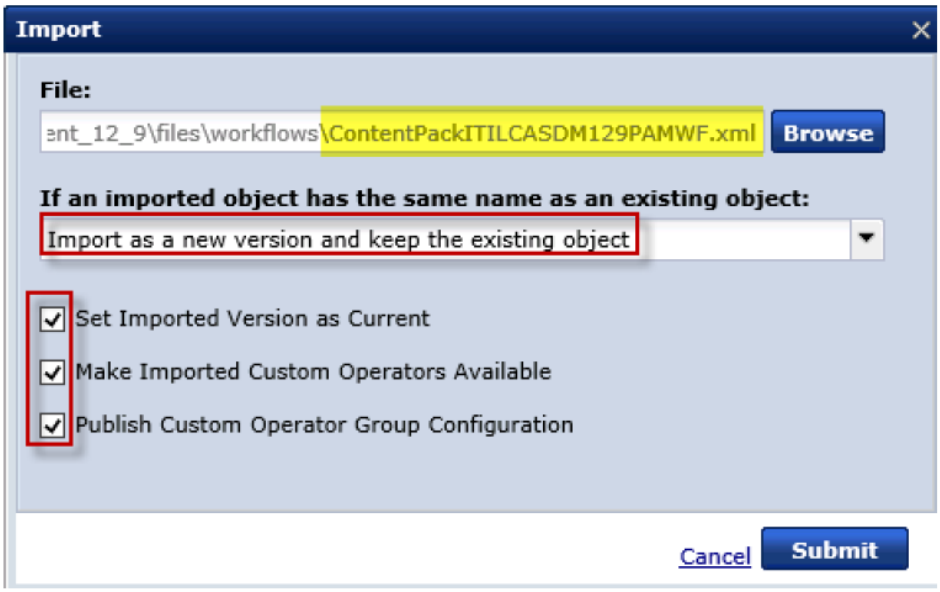
2. Import the Process Definitions into CA Process Automation:

    a. Click on the 'Library' Tab

    b. RMC on the root directory, and select 'Import:

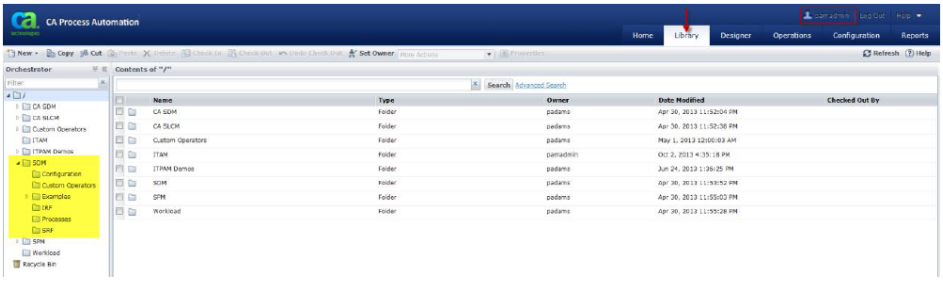


    c. Browse to the XML File which contains the CA Process Automation Process Definitions, select it, then select all remaining checkboxes, then hi 'submit'. In my example I have logged into CA Process Automation via url from the CA SDM Server. I have browsed to the ContentPackITILCASDM141PAMWF.XML file under $NX_ROOT/samples /ITIL_Content_14_1/files/workflows/



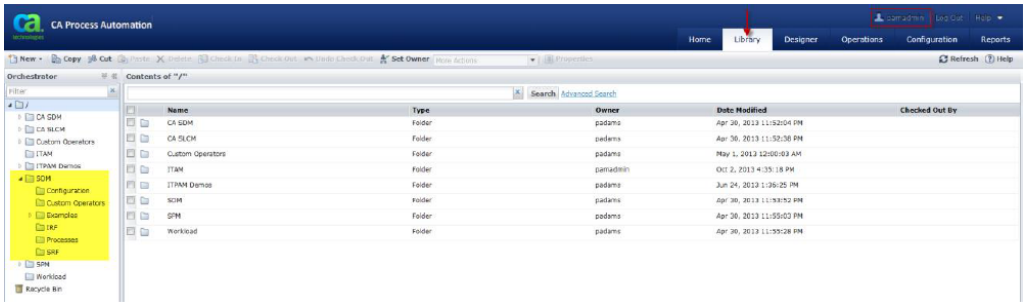
d. You will now see a new folder, SDM, as shown in the screenshot below.

Note: If you have already imported the process definitions available in $NX_ROOT/samples/CA_PAM_Workflows then this will overwrite the content already in the 'SDM' directory, however, depending on the flag you specified above during the import, it will also create a new 'version'.

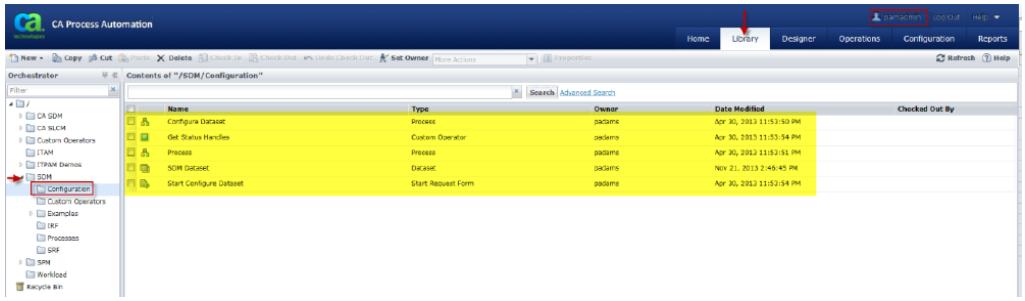


View Imported Process Definitions

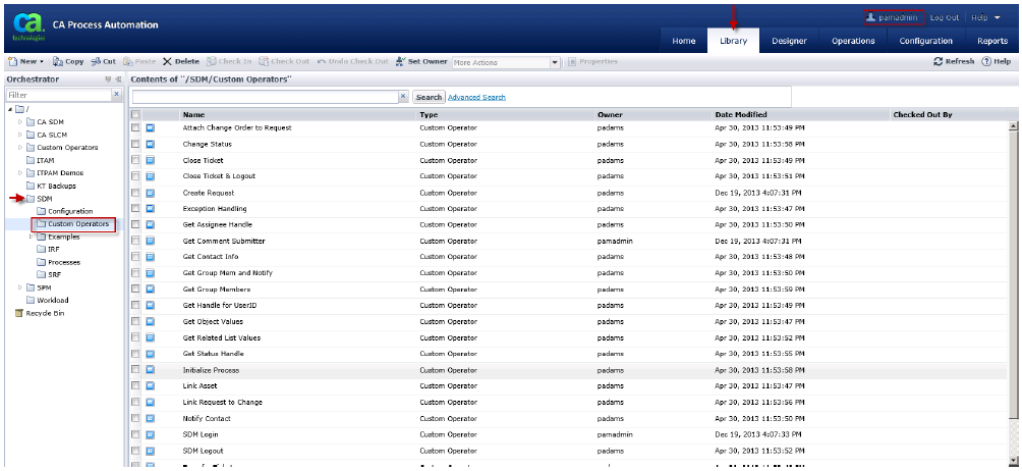
1. Once you have imported the Process Definitions, a new folder called 'SDM' appears, which includes Configuration, Custom Operators, Examples, IRF's, Processes, and SRF's:



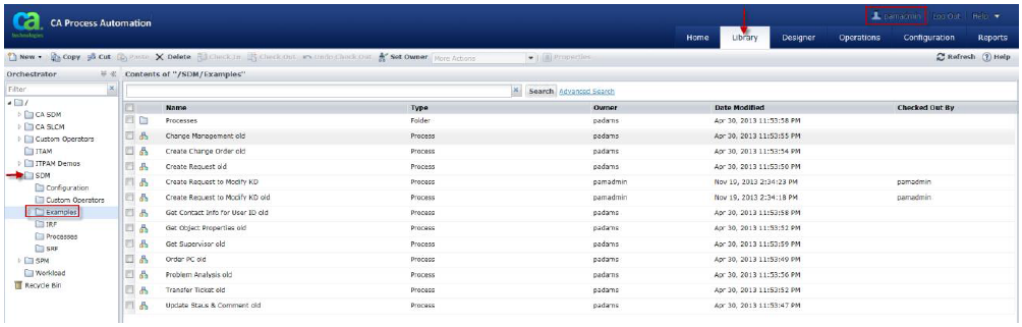
2. Configuration:



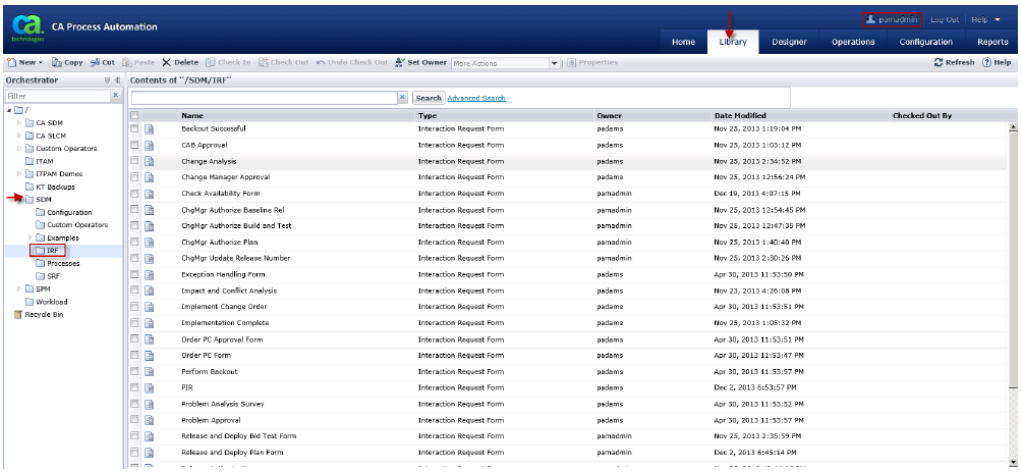
3. Custom Operators:



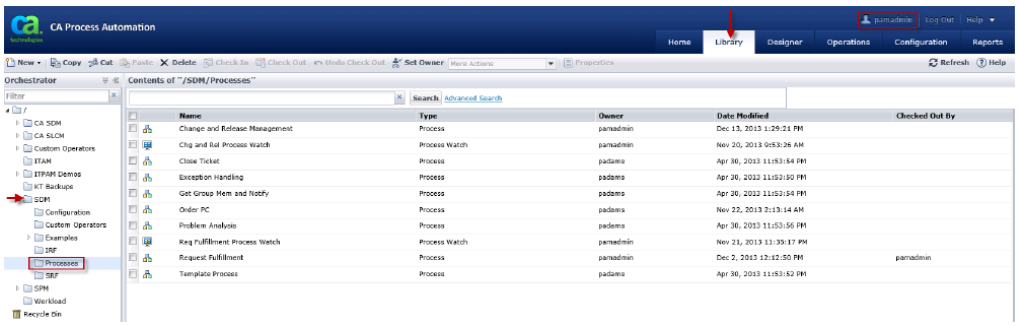
4. Examples:



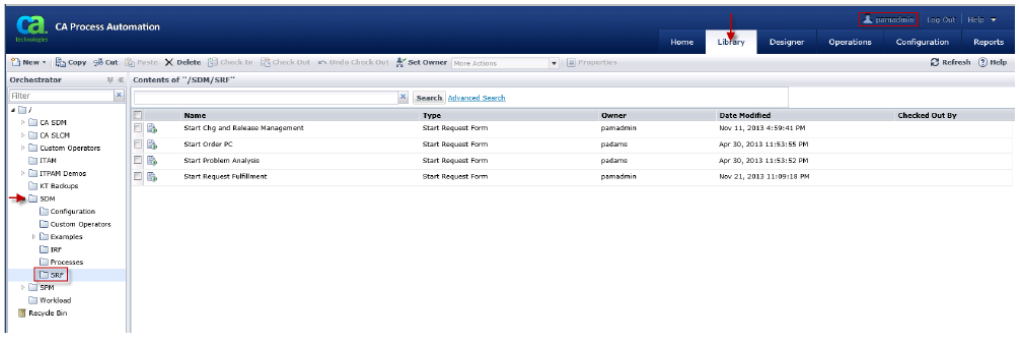
5. IRF's:



6. Processes:

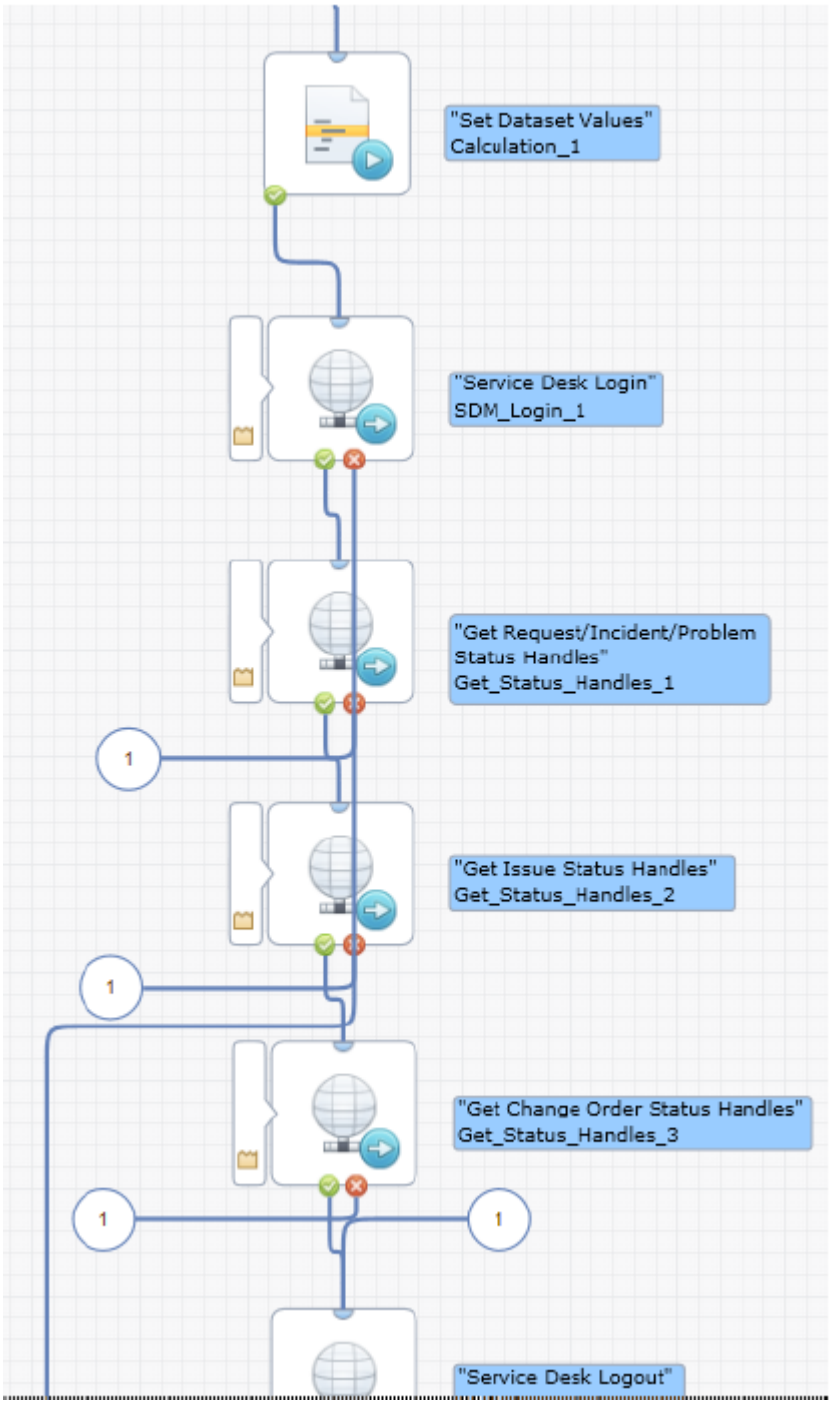


7. SRF's:

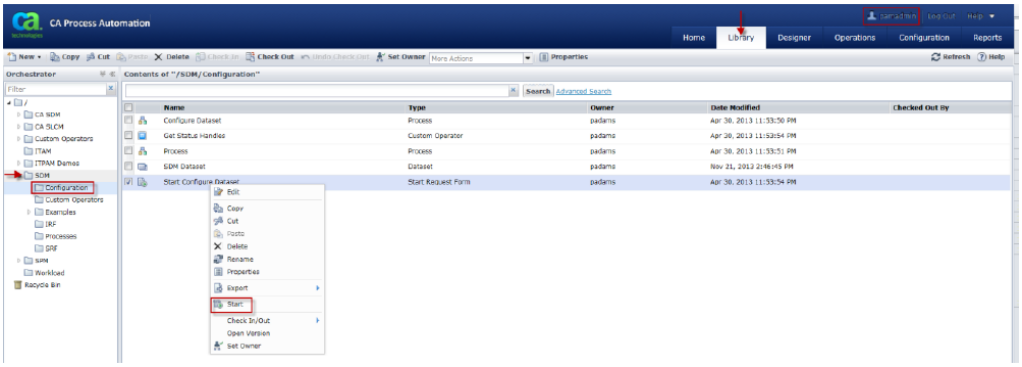


Configure SDM Dataset for Sample Process Definitions

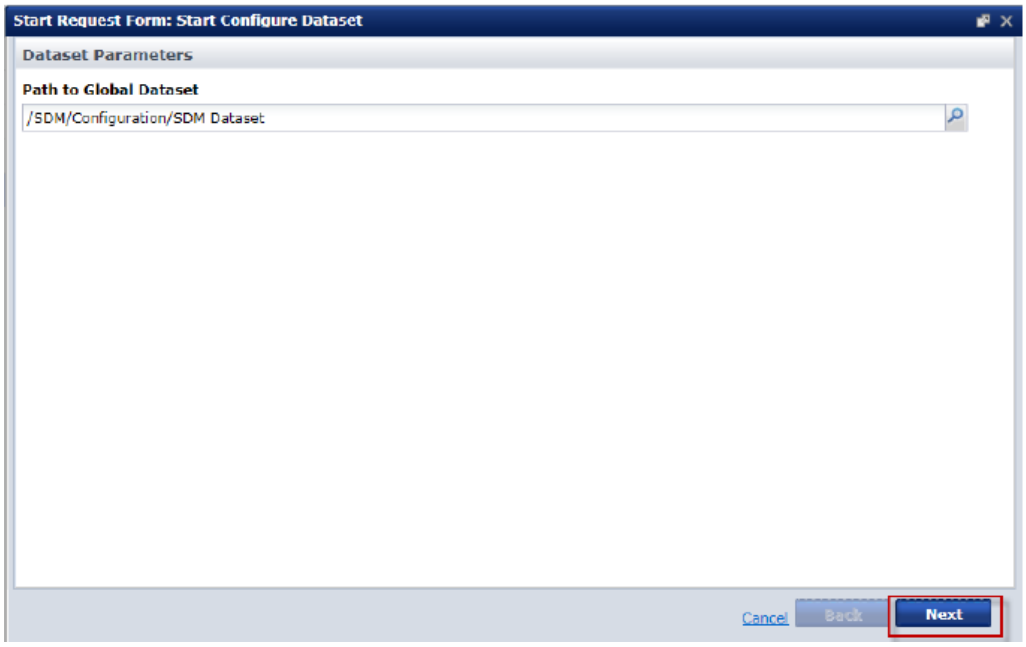
1. In the CA Process Automation Client, navigate back to SDM, Configuration. Here is where the dataset is configured for the sample process definitions. There is an SRF, 'Start Configure Dataset', which instantiates a 'Configure Dataset' Process which initializes the CA SDM Server, CA Process Automation Server, Exception Handling, and also obtains all handles (persid's) for all ticket statuses:



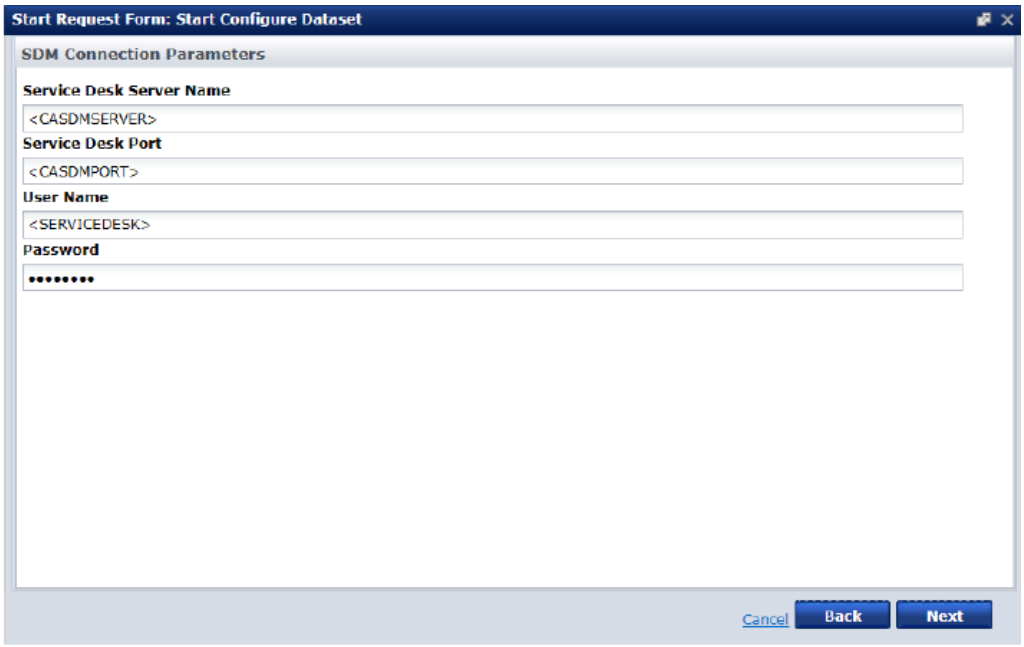
2. Launch the ‘Start Request Form’ for ‘Start Configure Dataset’:



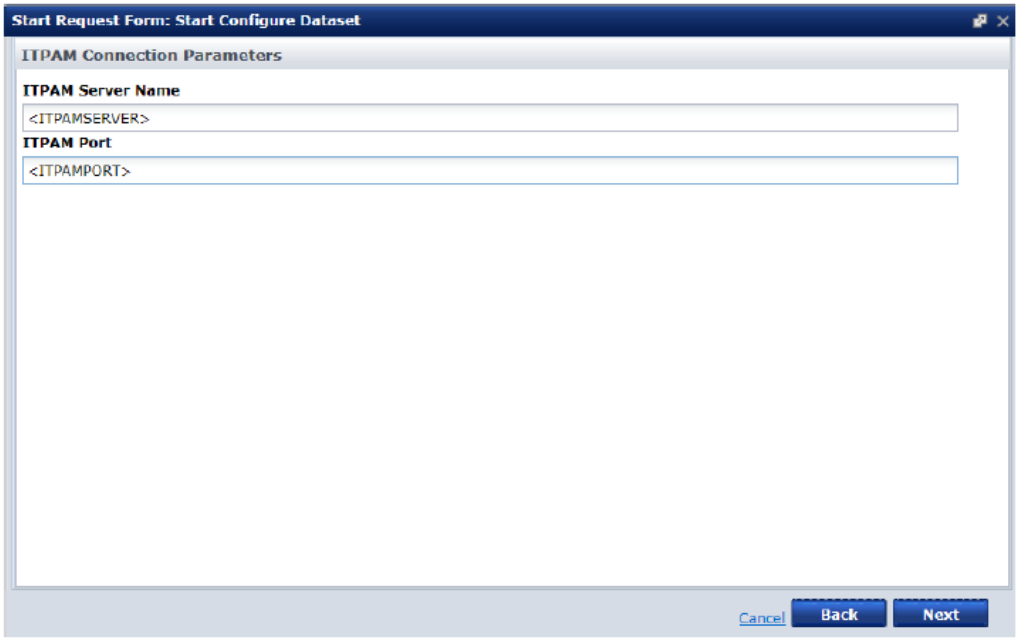
3. Verify the path to the Global Dataset (where all of the following data will be saved for other sample processes to leverage), and hit 'Next'.



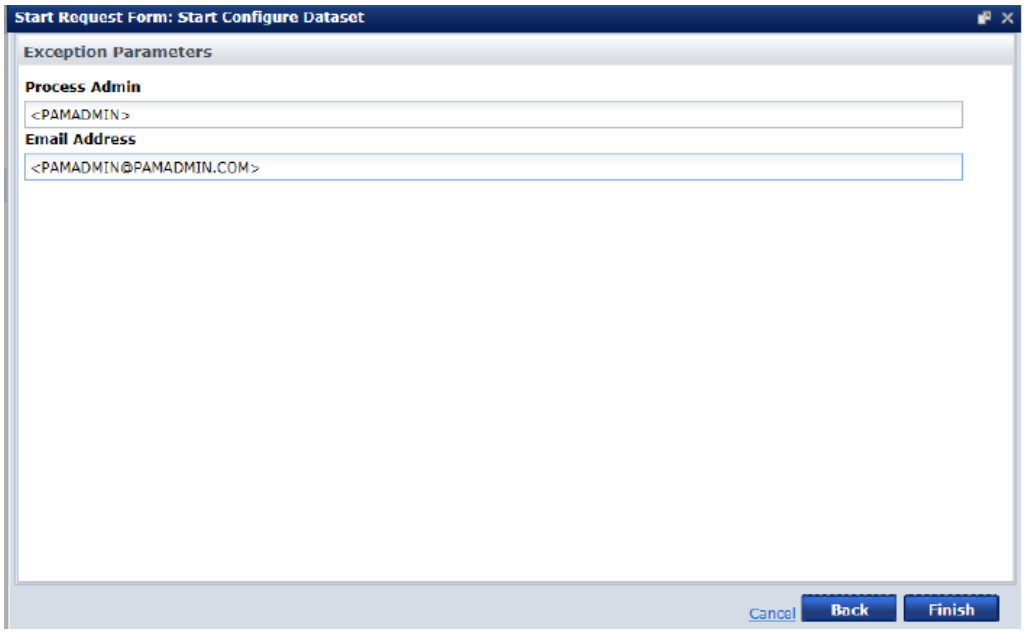
4. Enter in the values for the CA SDM server, port, Administrative Username and Password (replace what is shown here with your own data):



5. Enter in the values for the CA Process Automation server, and port (replace what is shown here with your own data):



6. Enter in the value for Process Admin and an email address (replace what is shown here with your own data):



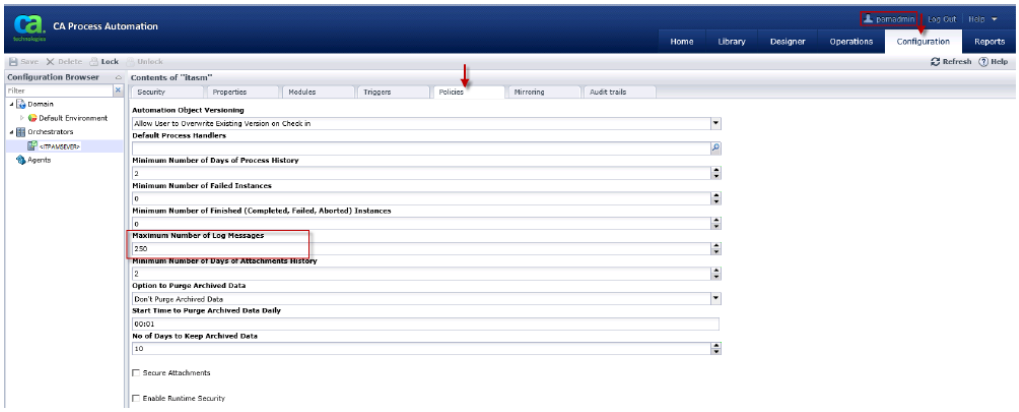
7. Hit Finish. Your CA Process Automation integration settings are now complete. All data resulting from this process definition are saved to the CA SDM Dataset.

Increase 'Maximum Number of Log Messages' in CA Process Automation

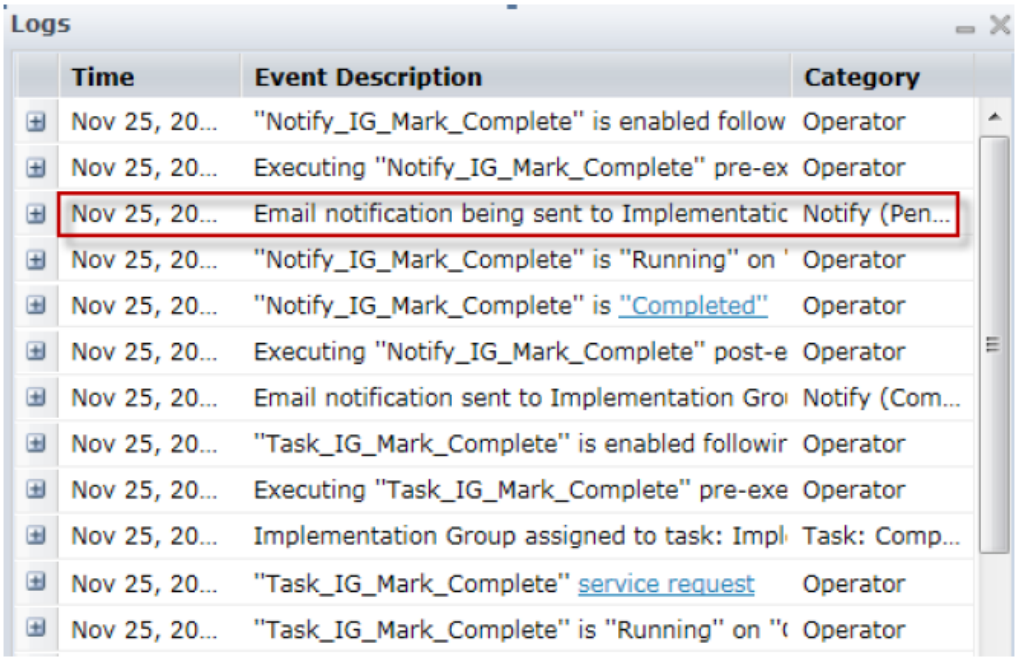
Follow these steps:

1. In the CA Process Automation Client, navigate to Configuration, select your Orchestrator and hit the 'Policies' Tab.

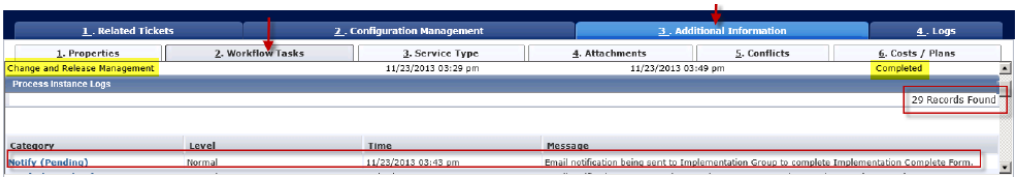
2. Increase 'Maximum number of Log Messages' to 250.



3. This number will ensure that all Process Instance Logs in CA Process Automation...



4. are carried over to the Workflow Tasks Tab in a CA SDM Problem, Request, or Change Order. If you do not increase this number, you will find that the Workflow Tasks Tab will not show the full list of Process Instance Logs, only the last 29 will be saved in cache and displayed:



Verify CA SDM Options Manager Options

Follow these steps:

1. Login to CA SDM by navigating to Start, Programs, CA, Service Desk Manager, Service Desk Web Client.

    a. Login as an Administrator, in our example we will be logging in as the 'ServiceDesk' user.

2. Install CA SDM Options Manager Options for CA IT PAM Workflow :

    a. Navigate to Administration, Options Manager, CA IT PAM Workflow

    b. Verify that all 7 options are installed according to the instructions in CA SDM 12.6 Integrations Greenbook, Volume 2, Chapter on CA Process Automation (https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/common/greenbooks.html).

i. All are applicable with the exception of the caextwf_eem_hostname option. This may not be applicable if you are not running EEM in your environment and instead are running Active Director.

c. Assume here that:

i. CAEEMSERVER = Name of your EEM server.
1. Should match what is returned by running 'hostname' in DOS

ii. CAITPAMSERVER = Name of your CA Process Automation server.
1. Should match what is returned by running 'hostname' in DOS

iii. CAITPAMPORT: CA Process Automation Tomcat port

CASDM Options Manager Option	Value
Caextwf_eem_hostname	<CAEEMSERVER>
Caextwf_endpoint	http://<CAITPAMSERVER>:<CAITPAMPORT>/itpam/soap
Caextwf_log_categories For more information, see CA SDM 12.6 Integrations Greenbook, Volume 2, Chapter on CA Process Automation (https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/common/greenbooks.html).	Notify (Pending), Notify (Complete), Task: Complete Form (Pending), Task: Complete Form (Complete), Task: Approve/Reject (Pending), Task: Approve/Reject (Complete), Status Change (Pending), Status Change (Complete), Task: Other (Pending), Task: Other (Complete), Closure Code Change (Pending), Closure Code Change (Complete), Create Incident (Pending), Create Incident (Complete), Create Change Order (Pending), Create Change Order (Complete), Process Form Data
Caextwf_processdisplayurl	http://< CAITPAMSERVER>:<ITPAMPORT>/itpam/JNLPRequestProcessor?processType=startUI&roid=
Caextwf_worklist_url	http://< CAITPAMSERVER >:<ITPAMPORT>/itpam?webPage=mytaskfilter&view=tasklist
Caextwf_ws_password	<Encrypted password>
Caextwf_ws_user	Itpamadmin <for an upgraded instance of CA Process Automation, 'pamadmin' on a fresh install

3. Recycle the CA SDM Services for changes to Options Manager Options to take effect.

Troubleshooting: Fields of type Text Area Render Without Word Wrap

Valid on IE 11

Problem:

When executing the CA Process Automation Workflows, it is found that IRF's that have fields of type 'Text Area' render without word wrap on the forms.

Solution:

Currently no solution exists. Visit the CA Process Automation Home Page on support.ca.com (http://support.ca.com) for more information.

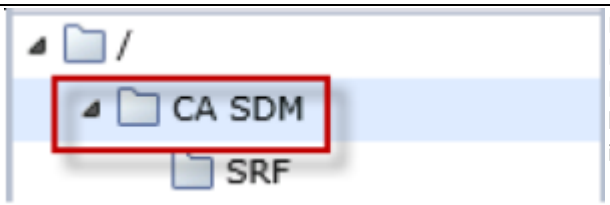
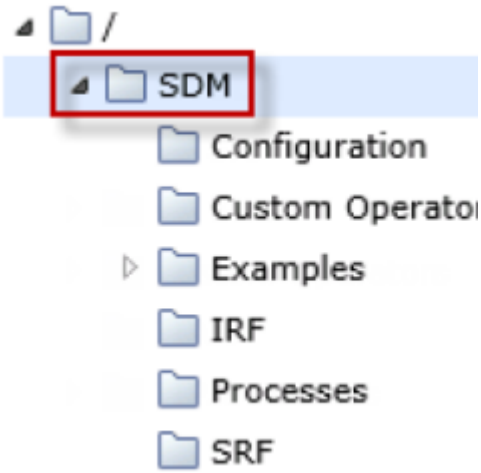
CA Process Automation Process Definitions for CA Service Desk Manager

This topic covers steps to import and configure the sample CA SDM CA Process Automation process definitions provided with the Content Pack for ITIL for the current release of CA SDM. Before we get started, let's discuss some of the CA Process Automation content that either is currently available, or has been available with previous versions of CA SDM, and how that content relates to the Content Pack for ITIL for the current release of CA SDM which we are focusing in on in this document.

Other CA Process Automation Content for CA SDM

This section describes additional CA Process Automation Content that either is currently available, or has been available with previous versions of CA SDM, and how that content relates to the Content Pack for ITIL for the CA SDM Release 14.1.

ITIL Content Pack	CA Process Automation Sample Process Defi CA SDM
Available Out-of-box in CA SDM	Yes, with a caveat. The original ITIL Content Pack was shipped with CA Process Automation Process Definitions and documentation, however what we provide out-of-box in the current release of CA SDM is the corresponding documentation only. - The Process Definitions are no longer supported or available for download.	Yes. These have also been referred to as the Out-of-box CA Workflow Samples Converted Process Automation.' The Process Definition available out-of-box in the directory below, they need to be manually imported into CA Automation.

	ITIL Content Pack	CA Process Automation Sample Process Defi CA SDM
Release?		
Where to get it	$NX_ROOT/samples/Sample_ITIL_Content	$NX_ROOT/samples/CA_PAM_Workflows
What it includes	Documentation Only. The original ITIL Content Pack was shipped with Process Definitions and documentation, however what we provide out-of-box in CA SDM 14.1 is the corresponding documentation only. The Process Definitions are no longer supported or available for download.	The following CA Process Automation (Full) I Definitions and corresponding documentatio - Order PC - Problem Analysis - Change Management
Where to check if you have imported this c		Note that this is the same directory that the Process Automation Process Definitions in th Pack for ITIL for CA SDM are imported to, be builds upon and enhanced this content. Mor information on this to follow later in this doc 

	ITIL Content Pack	CA Process Automation Sample Process Defi CA SDM
ontentintoCAProcessAutomation?		
Supported?	No	Yes…but is replaced with the Content Pack f CA SDM.
Replaced with Content Pack for IT	Yes, however note that the Content Pack for ITIL for CA SDM is not related to the ITIL Content Pack.	Yes, builds upon and enhances this content.

ITIL Content Pack	CA Process Automation Sample Process Defi CA SDM
IL fo r C A S D M C A Pr o c es s A ut o m at io n Pr o c es s D ef in iti o n s?	

Prerequisites

This document is meant to be used in addition to the information provided in the CA SDM 12.6 Integrations Greenbook, Volume 2, Chapter on CA Process Automation (https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/common/greenbooks.html).

This document assumes that the following applications have been installed and are operational:

- CA EEM 12.0.6.56 and above
- CA SDM 14.1
  - Email is configured and tested for CA SDM outbound email notifications
- CA Process Automation 4.1 SP1 and above

- This document also assumes that CA EEM, CA Service Desk Manager, and CA Process Automation have been integrated according to the instructions provided in the CA SDM 12.6 Integrations Greenbook, Volume 2, Chapter on CA Process Automation (https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/common/greenbooks.html)

> **Important!** This document will walk you through importing the CA Process Automation Process Definitions which are available with the 'Content Pack for ITIL for CA SDM 14.1'. In order for these process definitions to run successfully, you must have already installed the 'Content Pack for ITIL for CA SDM', as outlined in Install the ITIL Content for CA Service Desk Manager (see page 4819), which installs schema and HTMPL modifications, as well additional Administrative Data. The process definitions which we will walk though throughout this document rely heavily on this content.

Where to Find Future Updates to the CA SDM CA Process Automation Process Definitions

You can find any available updates on the CA SDM Homepage on support.ca.com (http://support.ca.com), please be sure to check this location regularly.

CA SDM CA Process Automation Process Definitions Defined

Following are the process names:

Process Name	Building Block or Full Process Definition	New with Content Pack for ITIL for CA SDM, Updated, or Existing?	What it does
Close Ticket	Building Block	Existing	Closes a Request, Incident, Problem, Change Order or Issue.
Exception Handling	Building Block	Existing	Exception handling template which can be called from within any CA Process Automation process definition
Get Group Mem and Notify	Building Block	Existing	This building block is passed a group UUID and notify flags as input, and as a result returns a list of all group members, group manager, and notifications to these users dependent upon flags passed.
Template Process	Building Block	Existing	Template which can be used to create your own CA Process Automation Process definition.

Order PC	Full Process Definition	Existing	The goal of this process is to walk through an end user ordering a new PC and the subsequent approval steps in order to fulfill or reject this order. Should be called from a Change Category.
Problem Analysis	Full Process Definition	Existing	The goal of this process is to decide if an RFC/Change should be created for a given Problem. Once the problem assignee has finished researching the problem and has a suggested solution, they will fill out this problem survey and provide a recommendation. The survey should give the approver a good idea of the impact of the problem and if it is necessary to resolve it through Change Management. The idea of Problem Pain/Value Analysis comes from ITIL 2011. Should be called from within a Problem Area.
Request Fulfillment	Full Process Definition	New	The goal of this process is to provide a foundation for Request Fulfillment which aligns to ITIL 2011.
Change and Release Management	Full Process Definition	Updated	This process definition adds Release and Deployment Management to the existing Change Management process included in the 'CA Process Automation Sample Process Definitions for CA SDM'. The goal of this process is to provide a foundation for Change and Release and Deployment Management which aligns to ITIL 2011. Provides the ability to manage a Change Management process for all Standard, Normal or Emergency Changes from the initial Request for Change through to its deployment and Post Implementation Review. It analyzes the 'Type' of Change Order and associated 'Risk' Level to determine what level of approvals are necessary for Change implementation. Should be called from a Change Category.

Note: The difference between a 'full process definition' and a 'building block' is that full process definition can is designed to be attached to a change category or macro directly to be instantiated. A building block is designed to be invoked from within another process definition.

CA SDM CA Process Automation Custom Operators Defined

Following are the process names:

Process Name	New with Content Pack for ITIL for CA SDM, Updated, or Existing?	Process or Soap Operator?	CA SDM Web Service Invoked	Input Parameters	What it does
Attach Change Order to Request	Existing	Soap	attachChangeToRequest	Assignee Handle Request Handle Description	Attaches a Change Order to a Request
Change Status	Existing	Soap	changeStatus	Creator Handle Ticket Handle New Status Code Comments	Updates the status of a ticket
Close Ticket	Existing	Soap	closeTicket	Persid Description	Closes a ticket
Close Ticket & Logout	Existing	Process	Via Close Ticket Process	Ticket Handle Initial Delay Comments Ticket Number	Invokes Close Ticket Process which closes a ticket and logs out CA SDM Web Services
Create Request	Existing	Soap	createRequest	Creator Handle Parent Change Handle Request Type Description Customer Handle Parent Request Handle Template	Creates a new Request/Incident/Problem, dependent upon the 'type' parameter passed.
Exception Handling	Existing	Process	Via Exception Handling Process	Ticket Handle Exception Type Process Name Process ID Node Name Touchpoint Name	Dependent upon the error message received, the exception handler will determine if the system should skip the operation, try and obtain a new Session ID (SID), try the operation again, or notify the System Administrator.

Process Name	New with Content Pack for ITIL for CA SDM, Updated, or Existing?	Process or Soap Operator?	CA SDM Web Service Invoked	Input Parameters	What it does
				Agent Name Error Message Operation Name Fault Response	
Get Assignee Handle	Existing	Soap	doSelect	Ticket Type Ticket Handle	Gets handle of ticket assignee
Get Contact Info	Existing	Soap	getContact	Contact ID	Retrieves attributes of a contact
Get Group Mem and Notify	Existing	Process	Via Get Group Mem and Notify Process	Creator Handle Ticket Handle Group Handle Notify List Message Title Message Body Urgency Internal Only	Invokes the Get Group Mem and Notify Process, which is passed a group UUID and notify flags as input, and as a result returns a list of all group members, group manager, and notifications to these users dependent upon flags passed.
Get Group Members	Existing	Soap	getGroupMemberListValues	Group Handle	Retrieves members of a group.
Get Handle for UserID	Existing	Soap	getGroupMemberListValues	User ID	Retrieves handle for a given user ID.
Get Object Values	Existing	Soap	getObjectValues	Object Handle Attributes	Retrieves all attributes for a Request /Incident/Problem/Change Order. The return is a UDSObject (XML); retrieve data with XPATH.
	Existing	Soap	getRelatedListValues	Object Handle List Name	

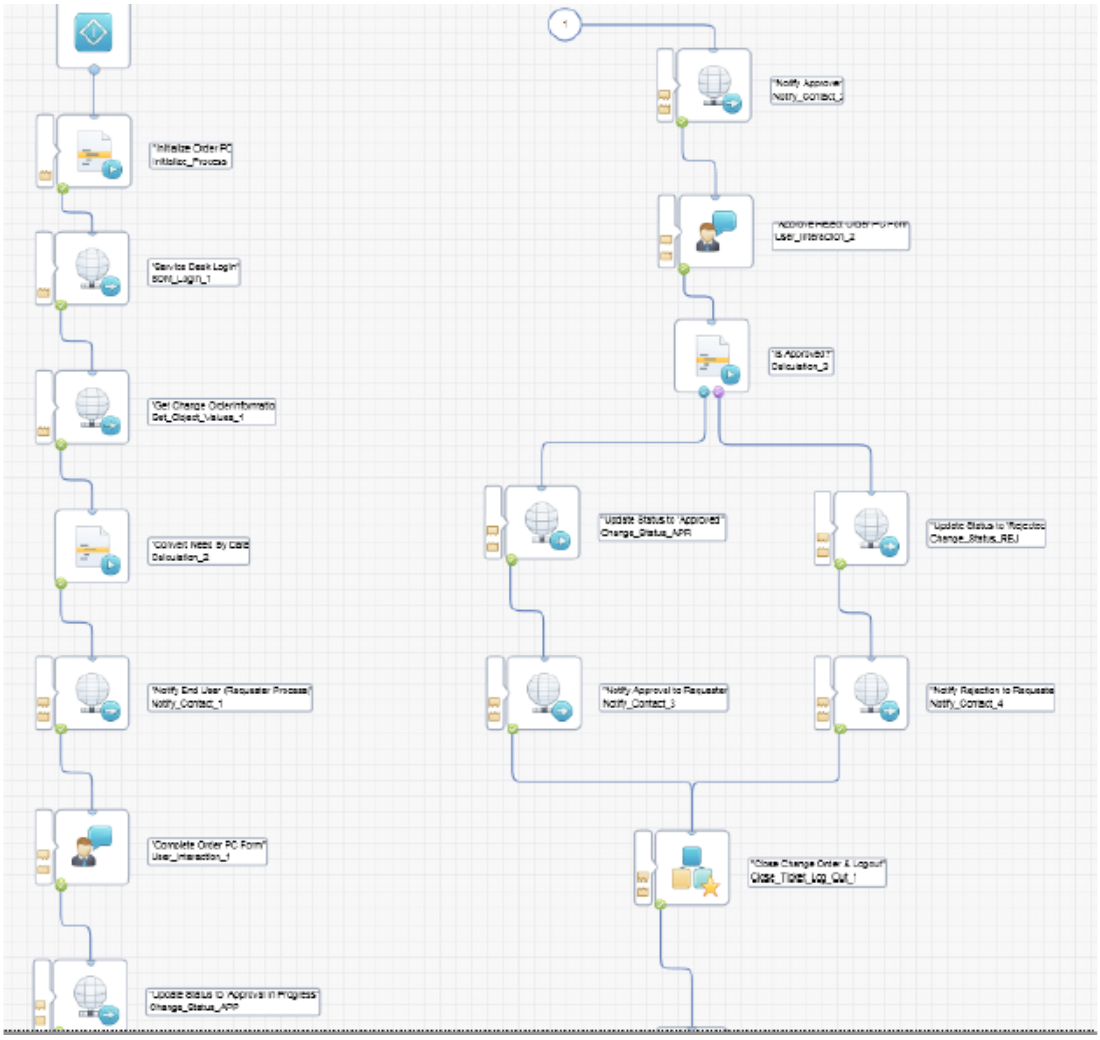
Process Name	New with Content Pack for ITIL for CA SDM, Updated, or Existing?	Process or Soap Operator?	CA SDM Web Service Invoked	Input Parameters	What it does
Get Related List Values					Returns values for lists related to a specific object. The lists must be defined as a QREL or BREL. Use the LREL methods to query LREL types.
Get Status Handle	Existing	Soap	doSelect	Ticket Type New Status Code	Retrieves the handle for a given status code, to be passed to the Update Status Method.
Initialize Process	Existing	Process	Via SDM Dataset		Initializes variables in the SDM Dataset to be used in the sample process definitions.
Link Asset	Existing	Soap	createLrelRelationships	Object Handle Asset Handle	Links an Asset to a Request, Incident, Problem, Change Order or Issue.
Link Request to Change	Existing	Soap	update Object	Request Handle Change Handle	Links a Request/Incident/Problem to a Change Order.
Notify Contact	Existing	Soap	notifyContact	Creator Handle Ticket Handle Contact Handle Message Title Message Body Urgency Internal Only	Sends a notification.
SDM Login	Existing	Soap	login	Soap Request File Soap Response File	Performs a Service Desk Web Service login and returns the SID
SDM Logout	Existing	Soap	Transfer	Creator Handle Ticket Handle Activity Log New	Transfers ownership of a Request, Incident, Problem, Change Order or Issue.

Process Name	New with Content Pack for ITIL for CA SDM, Updated, or Existing?	Process or Soap Operator?	CA SDM Web Service Invoked	Input Parameters	What it does
				Assignee Handle New Group Handle New Organization Handle	
Transfer Ticket	Existing	Soap	Transfer	Creator Handle Ticket Handle Activity Log New Assignee Handle New Group Handle New Organization Handle	Transfers ownership of a Request, Incident, Problem, Change Order or Issue.
Update Object	Existing	Soap	update Object	Ticket Handle Attribute New Value	Update any single attribute in an object. This supports fields that are NOT LREL's such as asset (CI). If you want to update an SREL field like priority ensure to pass the handle (persid).
Update Status & Comment	Existing	Process	Via Update Status	Creator Handle Ticket Handle New Status Code Comments	Updates ticket status and logs a comment in the ticket.

Order PC Workflow

This topic contains the following information

Design View in CA Process Automation



How Configure the Order PC Workflow

There is data which is a pre-requisite for running this Process Definition, which you must manually configure. It is listed in the following table. Note that there is 'Example Data' specified in the middle column of the chart below which indicates the name of the Contacts/Categories, etc that we used as a part of our walk-through, these of course can be changed to Contacts/Categories, etc for your own environment.

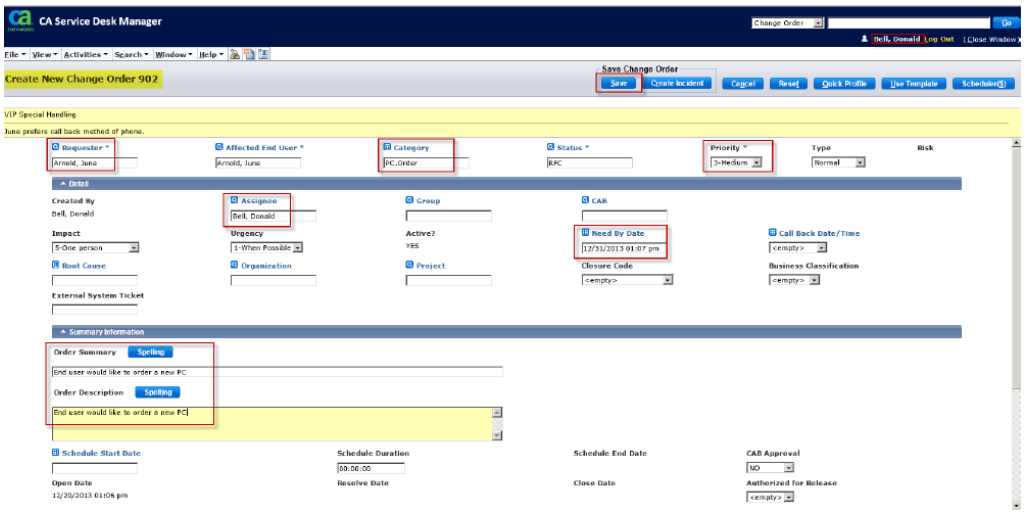
CA SDM Object /Option	Example Data	Notes
Add contact (Employee)	June Arnold	

CA SDM Object /Option	Example Data	Notes
		June will be the end user who requests the PC. 1. Must be defined as a contact in CA SDM as well as CA EEM, if you are leveraging EEM for authentication. 2. Must have an email address defined in the CA SDM contact record. 3. Must have a notification method set to 'Email' in the CA SDM contact record.
Add contact (Analyst)	Donald Bell	Donald will be the Analyst creating the Change Order. He will also be the Approver assigned to the Change Order Category, and thus assigned to the Change Order (through Category_Defaults Option, see below for details) 1. Must be defined as a contact in CA SDM as well as CA EEM, if you are leveraging EEM for authentication. 2. Must have an email address defined in the CA SDM contact record. 3. Must have a notification method set to 'Email' in the CA SDM contact record.
Add contact (Analyst)	John McCarthy	John will be the approver assigned to the Change Order Category, and thus assigned to the Change Order (through Category_Defaults Option, see below for details) 1. Must be defined as a contact in CA SDM as well as CA EEM, if you are leveraging EEM for authentication. 2. Must have an email address defined in the CA SDM contact record. 3. Must have a notification method set to 'Email' in the CA SDM contact record.
Create Change Order Category	PC. Order	This category will have the following values set: 1. Assignee: Donald Bell 2. <in the 'Workflow' Tab> CA IT PAM Process Name: 'Order PC'
Install 'Category_Defaults' Option	Yes	This option needs to be installed so that the information from the PC.Order Change Category is pulled over to the Change Order once it is created. Recycle CA SDM services for changes to take effect.

Order PC Workflow in Action

1. Login to CA SDM as Donald Bell, create a new Change Order, either from scratch or based on an existing Incident.

2. Fill out all of the fields highlighted in red below, also including 'Backout Plan' on the 'Cost /Plans' Tab. (There is a status transition in place such that this field must not be NULL in order for Change Order to move from status 'Approval in Progress' to 'Approved'.) Then hit save.



3. Click on the Additional Information Tab, and then drill down to the Workflow Tasks Tab. Scroll down through the tasks. You will see a notification has gone out to the requester (June Arnold) to complete the 'Order PC' Form. To complete this task June can either click on the link provided via email, or alternatively, she can scroll to the next pending task in the Workflow and click on the hyperlink for 'Task: Complete Form (Pending)':

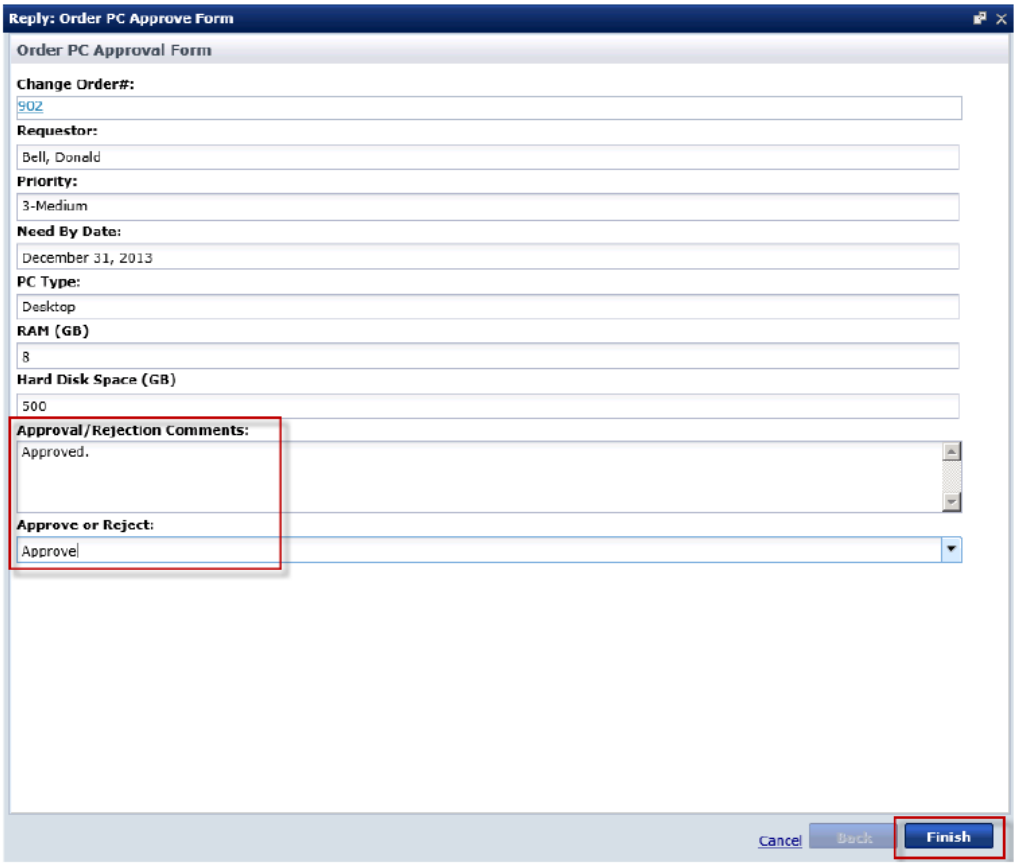
4. Once logged in to CA Process Automation as June, you should see one pending task to 'Complete the 'Order PC Form'. RMC on the task, and select 'Reply':

5. Complete the information in the Order PC Form. Hit 'Finish',

6. Navigate back to the Change Order. The status of the Change Order is now 'Approval in Progress'. Click on the Additional Information Tab, and then drill down to the Workflow Tasks Tab. Scroll down through the tasks. You will see a notification has gone out to the approver (assignee of the Change Category) to Approve/Reject, which in our case is John McCarthy. To complete this task John can either click on the link provided via email, or alternatively, he can scroll to the next pending task in the Workflow and click on the hyperlink for 'Task: Approve /Reject (Pending)':

7. Once logged in as John, you should see one pending task to 'Approve/reject the PC Order'. RMC on the task, and select 'Reply'.

8. All of the information that had been initially filled out by Donald remains in this form for John to review. Either approve, reject, or mark as incomplete. In this example we will be approving this order. Hit finish.



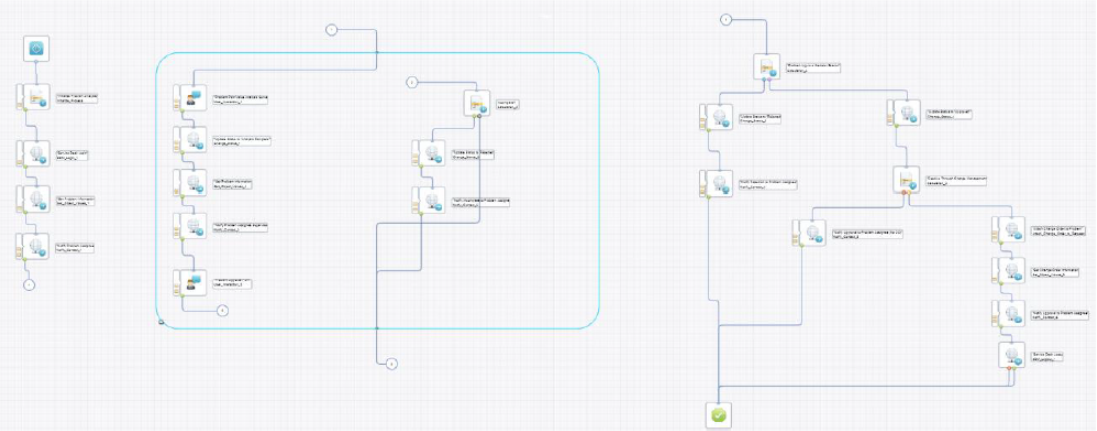
9. Navigate back to the Change Order. The status of the Change is now 'Approved'. Click on the Additional Information Tab, and then drill down to the Workflow Tasks Tab. Scroll down through the tasks. You can see that an email notification has one out to the Requester saying it has been approved.

10. Refresh the Change Order. Scroll further down in the Workflow Tasks. You will see that the status has changed to 'Closed'.

Problem Analysis Workflow

This topic contains the following information:

Design view in CA Process Automation



How to Configure the Problem Analysis Workflow

There is data which is a pre-requisite for running this Process Definition, which you must manually configure. It is listed in the following table. Note that there is 'Example Data' specified in the middle column of the chart below which indicates the name of the Contacts/Problem Areas, etc that we used as a part of our walk-through, these of course can be changed to Contacts/Problem Areas, etc for your own environment.

CA SDM Object /Option	Example Data	Notes
Add contact (Employee)	June Arnold	June will be the end user who creates the initial Incident, that leads to the creation of the Problem. If a Problem is created directly, she will be the end user requesting the problem. 1. Must be defined as a contact in CA SDM as well as CA EEM, if you are leveraging EEM for authentication. 2. Must have an email address defined in the CA SDM contact record. 3. Must have a notification method set to 'Email' in the CA SDM contact record.
Add contact (Analyst)	Donald Bell	Donald will be the Analyst creating/assigned to the Change Order resulting from the Problem. 1. Must be defined as a contact in CA SDM as well as CA EEM, if you are leveraging EEM for authentication. 2. Must have an email address defined in the CA SDM contact record. 3. Must have a notification method set to 'Email' in the CA SDM contact record.
Add contact (Analyst)	Marc Craigie	Marc will be Donald's supervisor, and as such, will be the approver of the Problem. 1. Must be defined as a contact in CA SDM as well as CA EEM, if you are leveraging EEM for authentication. 2. Must have an email address defined in the CA SDM contact record. 3. Must have a notification method set to 'Email' in the CA SDM contact

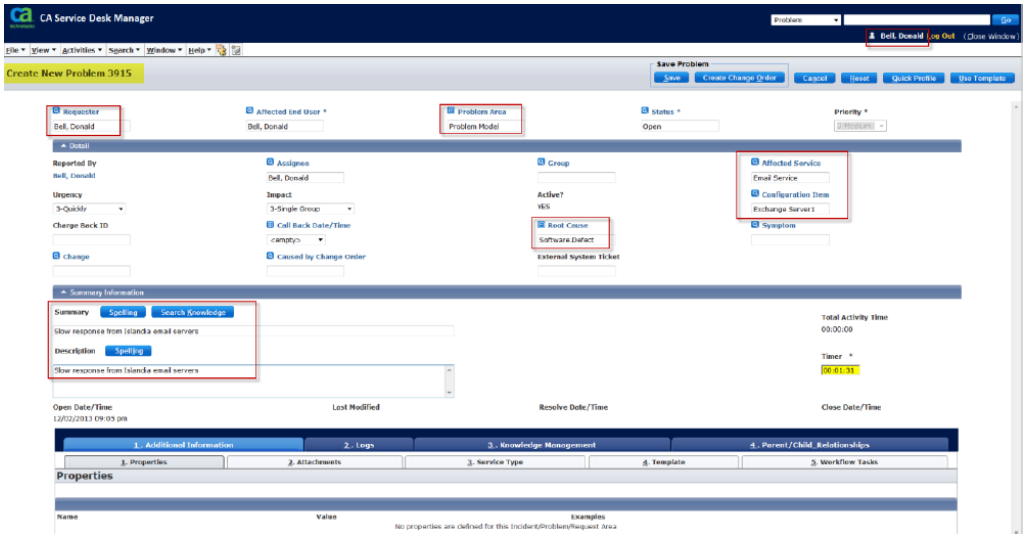
CA SDM Object /Option	Example Data	Notes
		record. 4. Assign Marc as Donald's Supervisor by going to Donald's contact record, and navigating to the Organization Tab, and entering in Marc as Donald's supervisor.
Create Problem Area	Problem Model	This Problem Area will have the following values set: 1. Assignee: Donald Bell 2. <in the 'Workflow' Tab> CA IT PAM Process Name: 'Problem Analysis'
Create CI's	Email Service Exchange Server1	Create two new configuration items (Service Desk Tab->File->New Configuration Item), which we will assign to the Problem as we go through the demo: 1. Email Service 2. Exchange Server
Create root cause	Software Defect	Create a root cause (Administration Tab->Service Desk->Application Data->Codes->Root Cause), which we will assign to the Problem as we go through the demo: 1. Software Defect
Install 'Category_Defaults' Option	Yes	This option needs to be installed so that the information from the 'Problem Model' Problem Area is pulled over to the Problem once it is created. Recycle CA SDM services for changes to take effect.

Problem Analysis Workflow in Action

Follow these steps:

1. Login to CA SDM as Donald Bell, create a new Problem, either from scratch or based on an existing Incident.

2. Fill out all of the fields highlighted in red below, then hit save.



3. Click on the Additional Information Tab, and then drill down to the Workflow Tasks Tab. Scroll down through the tasks. You will see a notification has gone out to the assignee (Donald Bell) to complete the Problem Pain/Value Analysis Form. To complete this task Donald can either click on the link provided via email, or alternatively, he can scroll to the next pending task in the Workflow and click on the hyperlink for 'Task: Complete Form (Pending)':

4. Once logged in to CA Process Automation as Donald, you should see one pending task to complete the 'Problem Pain/Value Analysis Survey'. You will also see an 'I' flashing in the lower right hand side of the screen, indicating user interaction is pending. RMC on the task, and select 'Reply':

5. Complete the information in the Problem Analysis Survey. Be sure to respond to the last question 'Should this Problem be resolved through Change Management?' as 'Yes'. Hit 'Finish',

6. Navigate back to the Problem. The status of the Problem is now 'Analysis Complete'. Click on the Additional Information Tab, and then drill down to the Workflow Tasks Tab. Scroll down through the tasks. You will see a notification has gone out to the assignee (Donald Bell's) supervisor to Approve/Reject , which in our case is Mark Craigie. To complete this task Marc can either click on the link provided via email, or alternatively, he can scroll to the next pending task in the Workflow and click on the hyperlink for 'Task: Approve/Reject (Pending)':

7. Once logged in as Marc, you should see one pending task to 'Approve/reject the Problem Pain/ Value Analysis Survey'. RMC on the task, and select 'Reply':

8. All of the information that had been initially filled out by Donald remains in this form for Marc to review. Scroll down to the bottom of the form. Either approve, reject, or mark as incomplete. In this example we will be approving this Problem to be resolved through Change Management. Hit finish, and then 'sign out' of CA Process Automation as Marc.

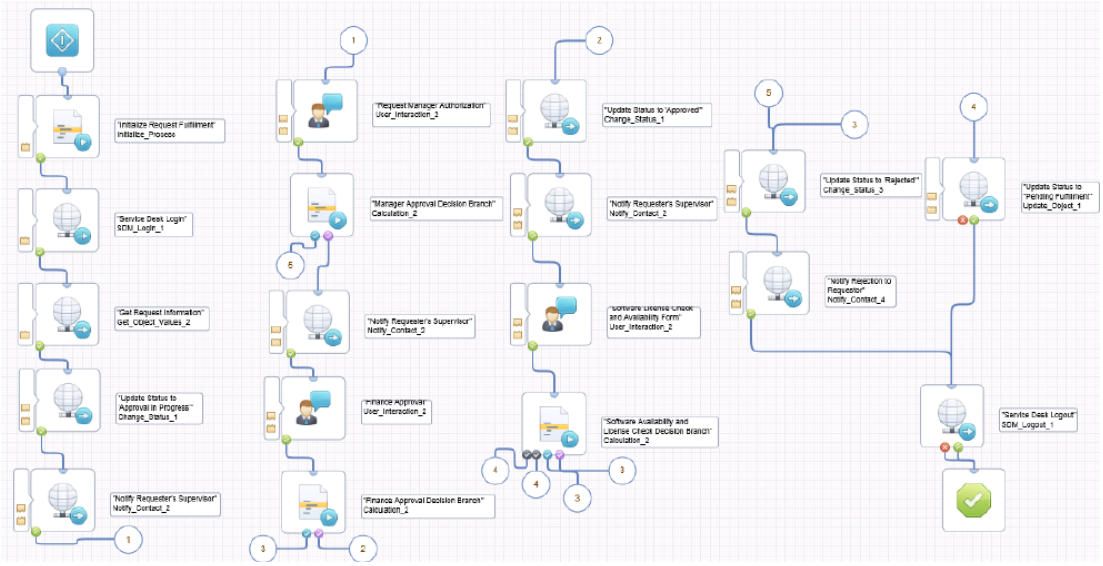
9. Navigate back to the Problem. The status of the Problem is now 'Approved'. Click on the Additional Information Tab, and then drill down to the Workflow Tasks Tab. Scroll down through the tasks. You will see that a Change Order has been opened and attached to the Problem, an email notification has gone out to the assignee (Donald Bell) indicating the same.

10. Click on the link for the Change Order to view details.

Request Fulfillment Workflow

This topic contains the following information:

Design View in CA Process Automation



How to configure the Request Fulfillment Workflow

There is data which is a pre-requisite for running this Process Definition, which you must manually configure. It is listed in the following table. Note that there is 'Example Data' specified in the middle column of the chart below which indicates the name of the Contacts/Request Areas, etc that we used as a part of our walk-through, these of course can be changed to Contacts/Request Areas, etc for your own environment.

CA SDM Object /Option	Example Data	Notes
Add contact (Analyst)	June Arnold	June will be the Analyst creating/assigned to the Request. 1. Must be defined as a contact in CA SDM as well as CA EEM, if you are leveraging EEM for authentication. 2. Must have an email address defined in the CA SDM contact record. 3. Must have a notification method set to 'Email' in the CA SDM contact record.
Add contact (Analyst)	Donald Bell	Donald will be June's supervisor, and as such, will be the approver of the Request. 1. Must be defined as a contact in CA SDM as well as CA EEM, if you are leveraging EEM for authentication. 2. Must have an email address defined in the CA SDM contact record. 3. Must have a notification method set to 'Email' in the CA SDM contact record. 4. Assign Donald as June's Supervisor by going to June's' contact record, and navigating to the Organization Tab, and entering in Donald as June's supervisor.
Create Request Area	SW	

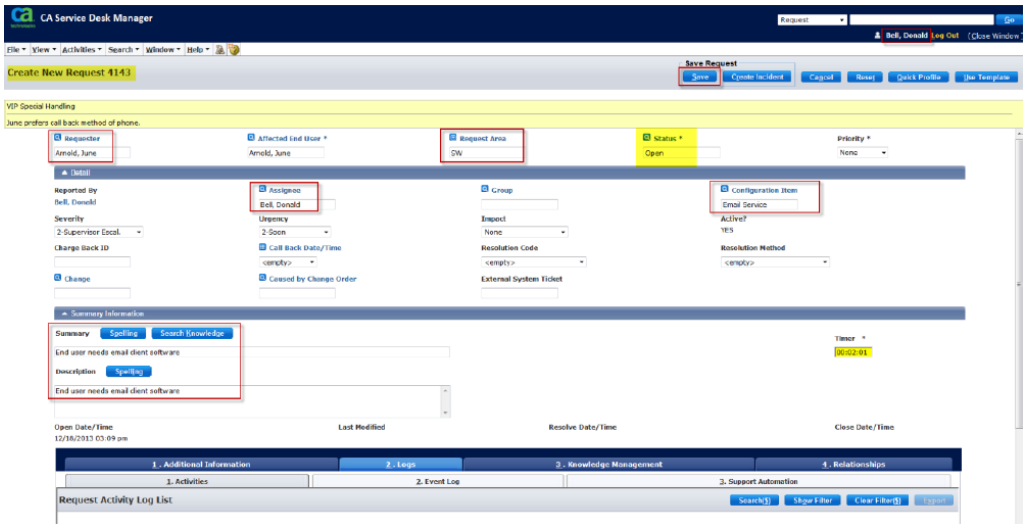
CA SDM Object /Option	Example Data	Notes
		This Request Area will have the following values set: 1. Assignee: June Arnold 2. <in the 'Workflow' Tab> CA IT PAM Process Name: 'Request Fulfillment'
Create CI	Email Service	Create a new configuration item, (Service Desk Tab->File->New Configuration Item), which we will assign to the Problem as we go through the demo. 1. Email Service
Install 'Category_Defaults' Option.	Yes	This option needs to be installed so that the information from the SW Request Area is pulled over to the Request once it is created. Recycle CA SDM services for changes to take effect

Request Fulfillment Workflow in Action

Follow these steps:

1. Login to CA SDM as Donald Bell, create a new Request.

2. Fill out all of the fields highlighted in red below, then hit save.



3. Click on the Relationships tab, then drill down to the Workflow Tasks Tab. Scroll down through the tasks. You will see the status has changed to 'Approval in Progress'.

4. Continue to scroll through the tasks. You will see a notification has gone out to the approver (Donald Bell) to authorize end user access. To complete this task Donald can either click on the link provided via email, or alternatively, he can scroll to the next pending task in the Workflow and click on the hyperlink for 'Task: Approve/Reject (Pending)'.

5. Once logged in to CA Process Automation as Donald, you should see one pending task to complete the 'Request Manager Authorization Form'. RMC on the task, and select 'Reply'.

6. Complete the information in the Request Manager Authorization Form. In this case, approve the request.

7. Navigate back to the Request. Click on the Relationships Tab, and then drill down to the Workflow Tasks Tab. Scroll down through the tasks. You will see a notification has gone out to the assignee (June Arnold's) supervisor for Financial Approval, which in our case is Donald Bell. To complete this task Donald can either click on the link provided via email, or alternatively, he can scroll to the next pending task in the Workflow and click on the hyperlink for 'Task: Approve/Reject (Pending)'.

8. Once logged in to CA Process Automation as Donald, you should see one pending task to complete the 'Finance Approval Form'. RMC on the task, and select 'Reply'.

9. Complete the information in the Financial Approval Form. In this case, approve the request.

10. Navigate back to the Request. The status of the Request is now 'Approved'. Click on the Relationships Tab, and then drill down to the Workflow Tasks Tab. Scroll down through the tasks. You will see a notification has gone out to the requestor (June Arnold's) supervisor (Donald Bell) to confirm license check and availability of software. To complete this task Donald can either click on the link provided via email, or alternatively, he can scroll to the next pending task in the Workflow and click on the hyperlink for 'Task: Approve/Reject (Pending)'.

11. Once logged in to CA Process Automation as Donald, you should see one pending task to 'Confirm software license and availability'. RMC on the task, and select 'Reply'.

12. Confirm software license and availability, and hit 'Finish':

13. Navigate back to the Request. The status of the Request is now 'Pending Fulfillment'.

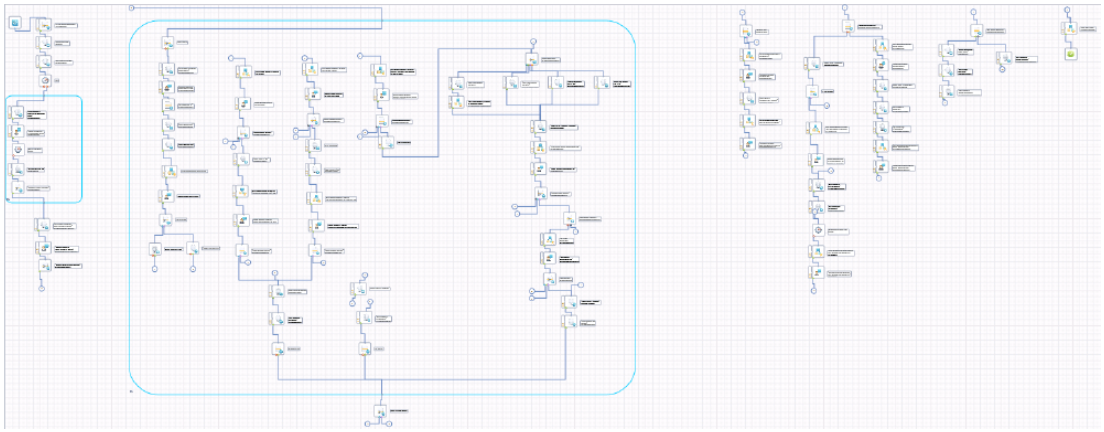
14. The workflow is now complete.

Change and Release Management Workflow

This topic contains the following information:

Important! If you are using only Change Management, and not Release Management, you can leverage this workflow process from a Change Management perspective. The process looks for a user-defined flag indicating whether the Change is a release. If the RFC is solely managing Change, then the process moves from Change Analysis directly to Change Manager and CAB Approvals. If it is a Release, then the process moves from Change Analysis through to Release approvals, then merges with Change at the Change Manager Approvals step. Any task that is specific to RDM only is delimited in the following steps with 'RDM'.

Design View in CA Process Automation



How to configure the Change and Release Management Workflow

The following table lists the prerequisites for running this Process Definition.

> **Note:** Example Data indicates the examples of Contacts or Change Categories. You can change according to your organization.

Note that there is

CA SDM Object/Option	Example Data	Notes
Add contact (Analyst)	Donald Bell	Donald is the Requester of the Change Order and also a member of both the CAB and Implementation Groups. 1. Must be defined as a contact in CA SDM and also in CA EEM, if you are leveraging CA EEM for authentication. 2. Must have an email address defined in the CA SDM contact record. 3. Must have a notification method set to 'Email' in the CA SDM contact record.
Add contact (Analyst)	Kevin Smith	Kevin is a member of both the CAB and Implementation Groups. 1. Must be defined as a contact in CA SDM and also in CA EEM, if you are leveraging EEM for authentication. 2. Must have an email address defined in the CA SDM contact record. 3. Must have a notification method set to 'Email' in the CA SDM contact record.
Add contact (Analyst)		

CA SDM Object/Option	Example Data	Notes
	John McCarthy	John is a member and manager of both the CAB and Implementation Groups. 1. Must be defined as a contact in CA SDM and also in CA EEM, if you are leveraging EEM for authentication. 2. Must have an email address defined in the CA SDM contact record. 3. Must have a notification method set to 'Email' in the CA SDM contact record.
Add an Implementation Group	Implementation Group	Following is the group that implements the Change Order. 1. Group must be defined in CA SDM and also in CA EEM, if you are leveraging EEM for authentication. 2. When creating this group in EEM, the 'Group Name' in CA SDM must match the 'Principal Name' in EEM.
Add users to Implementation Group	John McCarthy Donald Bell Kevin Smith	1. This group must have more than one member 2. The members must be added to the group in CA SDM, and CA EEM if using EEM for authentication. 3. To add the user to the Group in CA EEM, go to Manage Identities->Users. Run a search. Highlight the user to view details. Navigate to the 'Global Group Membership' box. Under 'Available Global User Groups', search, and highlight the group that you would like to add the user to. Hit the right arrow, so that the group name is populated under 'Selected Global User Groups.'
Make one of the users previously added to the Implementation Group the Manager	John McCarthy	The group must have only one manager, this contact must be defined in CA SDM group record as the manager. This user is the Change Manager. 1. To make a contact a manager in the group record, navigate to the 'Members, Service Contracts, Auto Assignment' Tab, then drill down to 'Members' Tab
Add CAB Group	CAB	The CAB (Change Advisory Board) serves as approval group for the Change Order. This group implements the Change Order. 1. Group must be defined in CA SDM and CA EEM, if you are leveraging EEM for authentication. 2. When creating this group in EEM, the 'Group Name' in CA SDM must match the 'Principal Name' in EEM.
Add users to CAB Group	John McCarthy Donald Bell Kevin Smith	1. This group must have more than one member 2. The members must be added to the group in CA SDM and CA EEM, if using EEM for authentication. 3. To add the user to the Group in CA EEM, go to Manage Identities->Users. Run a search. Highlight the user to view details. Navigate to the 'Global Group Membership' box. Under 'Available Global User Groups', search, and highlight the group that you would like to add the user to. Hit the right arrow, so that the group name is populated under 'Selected Global User Groups.'
Make one of the users previously added to the CAB Group the Manager	John McCarthy	This user is the CAB Manager. 1. The group must have only one manager, this contact must be defined in CA SDM group record as the manager. This user

CA SDM Object/Option	Example Data	Notes
		is the Change Manager. 2. To make a contact a manager in the group record, navigate to the 'Members, Service Contracts, Auto Assignment' Tab, then drill down to 'Members' Tab
Create Change Order Category	Change and Release Mgmt	This Change Category has the following values set: 1. Assignee: John McCarthy 2. Risk Survey: General 3. CAB: CAB 4. Implementation Group: Implementation Group 5. <in the 'Workflow' Tab> CA IT PAM Process Name: 'Change and Release Management'
Create at least two new CI's, that have pre-existing relationships established and Change Orders already opened against them during the same scheduled timeframe.	TIXCHANGE TIXCHANGE Web Application	1. Create at least two new Configuration Items (Service Desk Tab->File->New Configuration Item) which we associate to the Change Order. 2. These CIs must all have relationships established with other CIs, so that a good view of the CA CMDB Visualizer (see page 2613) can be displayed. 3. These CIs must have pre-existing Change Orders opened against them which can be shown as a part of Conflict Analysis. In order for pre-existing Change Orders to appear during Conflict Analysis (see page 2245) step in the Workflow, they must be opened against the same CI, during the same scheduled timeframe.
Install Category_Defaults Option	Yes	This option must be installed so that the information from the Change and Release Model Category is pulled over to the Change Order once it is created. Recycle CA SDM services for changes to take effect
Modify Change Order Status	Check 'Make Change Order Active'	Use Administration, ServiceDesk, Change Orders, Status to check 'Make Change Order Active', so that when a Change Order enters the Backed Out status as a part of this workflow, it remains active.

Change and Release Management Workflow in Action

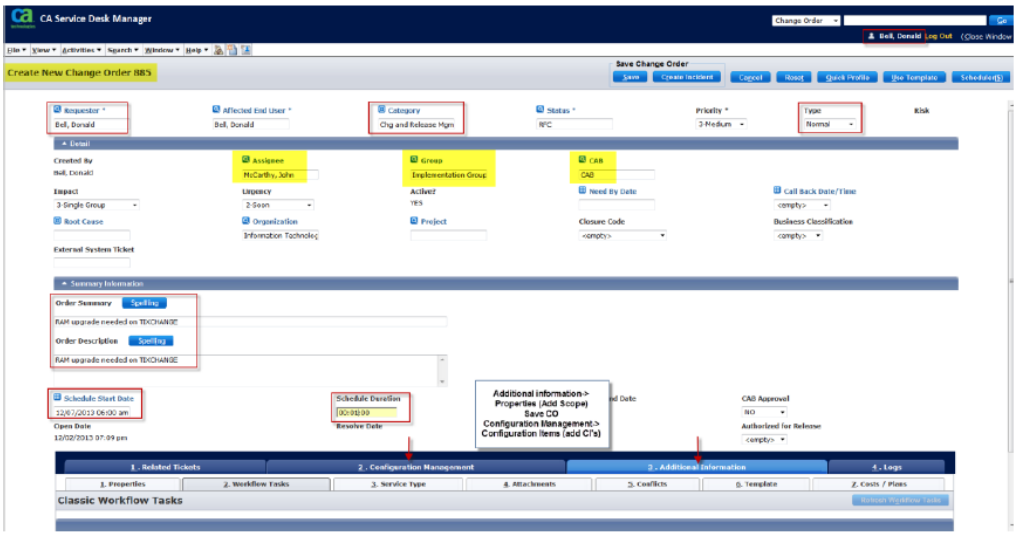
Important! Logic built into many of the IRFs (Interaction Request Forms) such that a response of 'no' when a 'yes' is expected result in an automatic 'rejection' of the Change Order or Release.

Follow these steps:

1. Log in to CA SDM as Donald Bell. Create a Change Order.

2. Fill out all of the highlighted fields including 'Backout Plan' on the 'Cost/Plans' Tab. For the Change Order to move from status 'Approval in Progress' to 'Approved', a status transition ensures that this field must not be NULL.

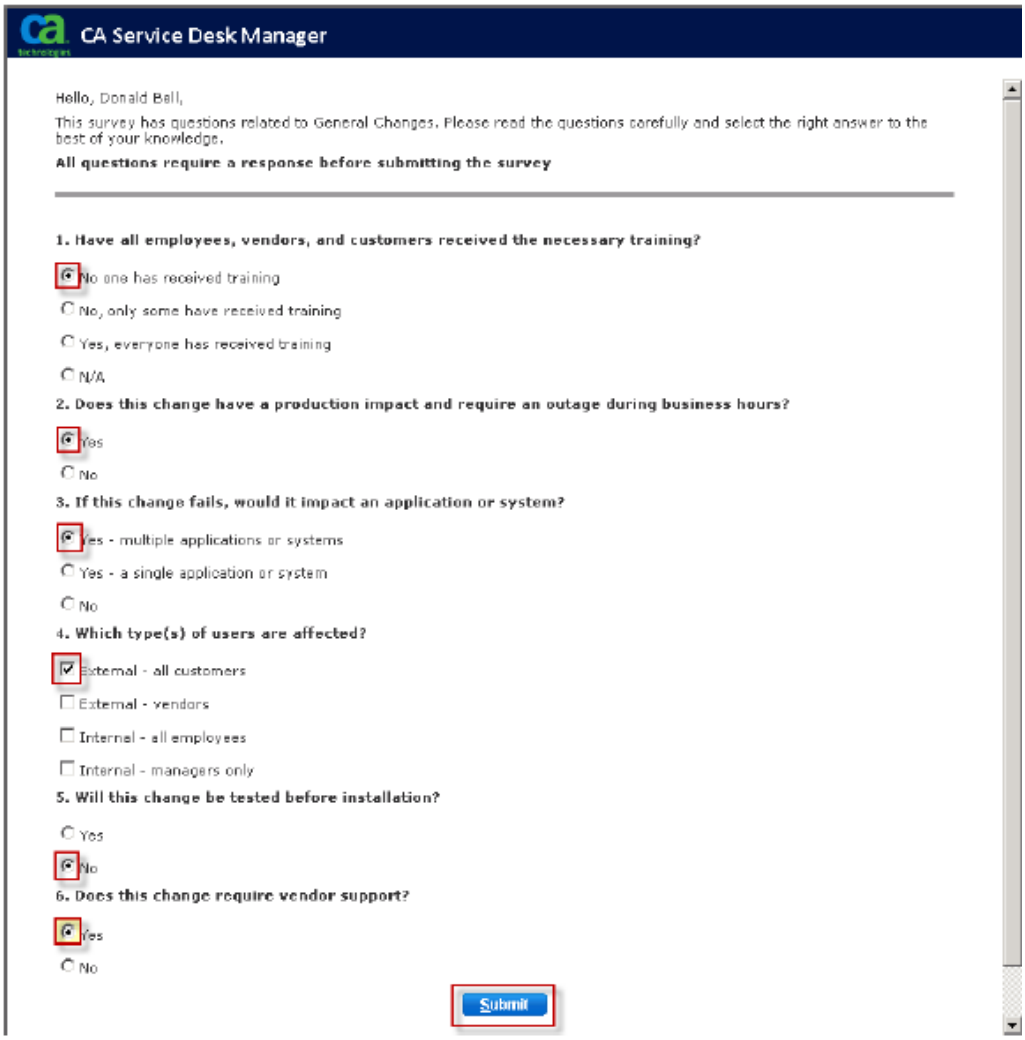
> **Note:** When you select the Category, and tab out of the field, the 'Assignee', 'Implementation Group' and 'CAB' are filled in, because the category_defaults option is turned on. You will not be able to add CI until after you save the Change order.



3. Select Additional Information, Workflow Tasks and scroll down through the tasks.
   You will see a notification has gone out to the requester (Donald Bell) to complete the Risk Assessment Survey. There is currently no Risk value assigned to the Change Order.

4. To complete this task, Donald can either click on the link provided in the email, or can scroll to the next pending task in the Workflow and click on the Task: Other (Pending) hyperlink. Clicking on the hyperlink will automatically log Donald into his tasklist.

5. RMC on the task and then click Reply.
   Donald is prompted to complete the Risk Assessment Survey. He clicks on the Risk Assessment Survey link. The link brings Donald in context to the Risk Assessment Survey. The survey which we have assigned to the Change Category is the default 'General' Risk Survey. Complete the Risk Survey, answering questions in such a way that it will generate high risk:



6. Once the Risk Survey is complete, navigate to CA Process Automation in context of the task and click Finish on the Risk Assessment task. You can remain logged into CA Process Automation as Donald.

7. Navigate back to the Change Order. Select Additional Information, Workflow Tasks and scroll down through the tasks.
   You will see a notification has gone out to the requester (Donald Bell) to complete Impact and Conflict Analysis. To complete this task Donald can either click on the link provided via email or scroll to the next pending task in the Workflow and click on the Task: Other (Pending) hyperlink.

8. Navigate back into CA Process Automation as Donald.
   You will see one pending task for Impact and Conflict Analysis.
   RMC on the task and click reply.

9. Clicking on the link to Impact and Conflict Analysis brings you in context to the Change Order where Impact and Conflict Analysis must be instantiated manually. The first step is to perform Impact Analysis. Impact Analysis will show which CI is impacted if the TIXCHANGE Servers are temporarily down for the RAM upgrade. There are two ways to run Impact Analysis. You can either run it through Impact Explorer which is accessible using the Additional Information,

Configuration Items tab within a Change Order. Or you can use CA CMDB Visualizer. You can filter the Visualizer for Impact Analysis. Once Impact Analysis is complete, the next step is Conflict Analysis, which is also run within context of a Change Order, from Additional Information, Conflicts Tab. Conflict Analysis shows if there are any Change Orders open for the same CI in the same timeframe, thus generating conflict. If there are any conflicts they must be resolved before proceeding further with the Change Order.

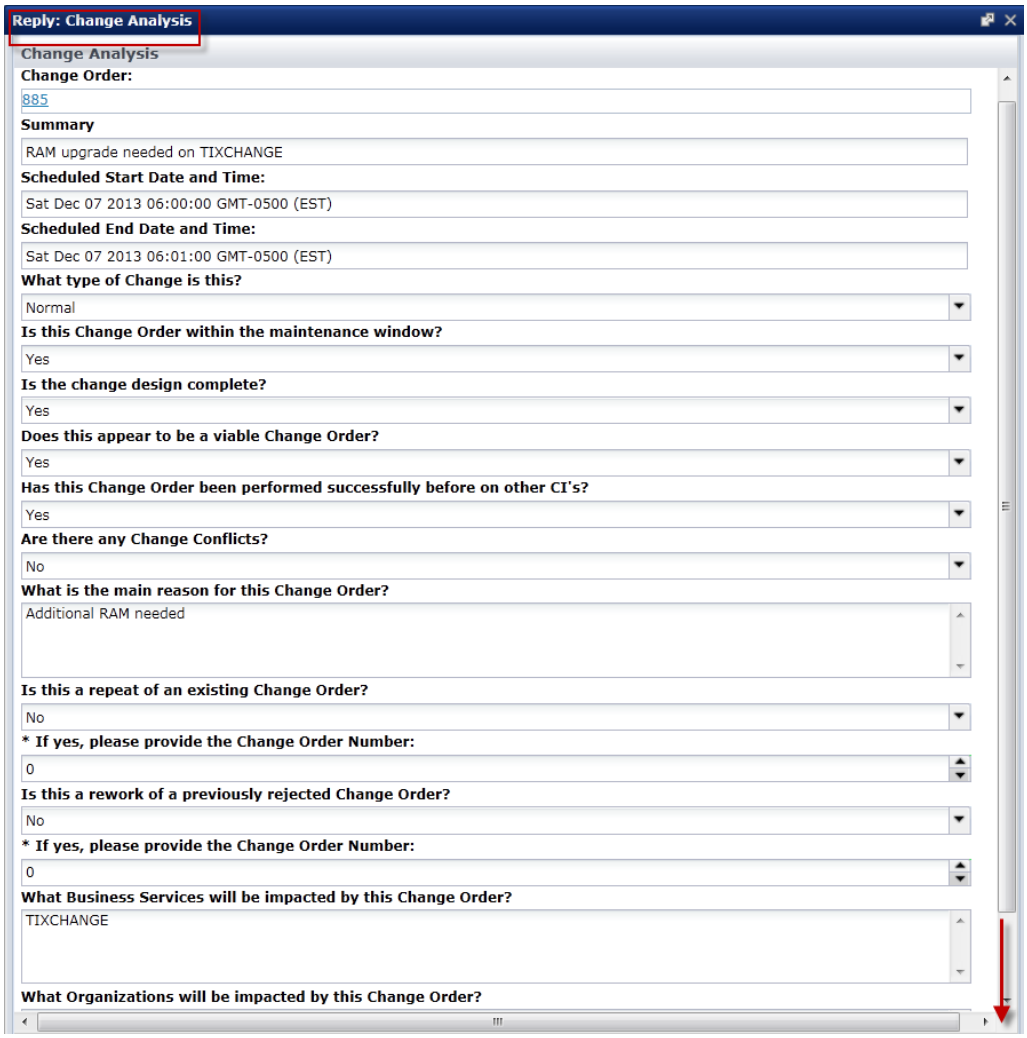
10. Finish the CA Process Automation task. You can remain logged in as Donald Bell.

11. Navigate to the Change Order. Click Additional Information, Workflow Tasks and scroll down through the tasks.
    You will see a notification has gone out to the requester (Donald Bell) to complete Change Analysis. To complete this task Donald can either click on the link provided in the email or scroll to the next pending task in the Workflow and click on the Task: Complete Form (Pending) hyperlink.

12. Navigate to CA Process Automation as Donald Bell. You will see one pending task for Change Analysis. If any of the form data indicates that any step is not complete or not done, the workflow takes different paths. We assume everything is complete.

13. RMC on the task and click Reply.

14. Complete the information in the Change Analysis form click finish. Following is an example of an IRF where an answer of ‘no’ to questions where a ‘yes’ is expected result in an automatic rejection of the Change Order:



15. Navigate to the Change Order. Select Additional Information and Workflow Tasks.
    You will see that the information from the Change Analysis form has been saved to the Change Order.

16. Scroll down through the tasks.
    You will see a notification has been sent to the Change Manager, Donald Bell. Donald must verify if this Change is going to be a Release. To complete this task Donald can either click on the link provided in the email or scroll to the next pending task in the Workflow and click on the Task: Approve/Reject (Pending) hyperlink.

17. Navigate to CA Process Automation as Donald Bell.
    You will see one pending task for Release Verification.

18. RMC on the task and click Reply.

19. Donald specifies that this is a Release, and then click Finish. Setting this to 'Yes' guides the user through the Release portion of this process.

    a. Navigate to the Change Order.

The ‘Authorized for Release’ Flag is set to ‘Yes’.

b. Scroll through the tasks.

You will see a notification has been sent to the Change Manager, Donald Bell. Donald must authorize Plan and Build Release. To complete this task Donald can either click on the link provided in the email or scroll to the next pending task in the Workflow and click on the Task: Complete Form (Pending) hyperlink.

c. Navigate to CA Process Automation as Donald Bell.

You will see one pending task for Authorize Plan and Build Release.

d. RMC on the task and click Reply. Complete the information in the Authorize Plan and Build Release form, scroll down and click finish. If any tasks are ‘Rejected’ or marked ‘Incomplete’, the workflow takes different paths. We will approve all tasks.

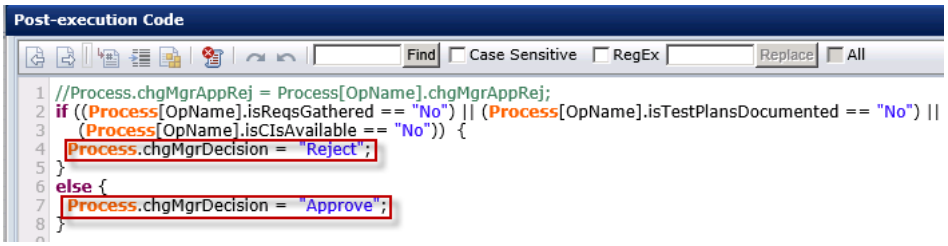
e. Navigate to the Change Order.

The status has changed to ‘Build’.

f. Scroll through the tasks.

You will see a notification has been sent to the Change Manager, Donald Bell. Donald must complete the Release and Deployment Plan and Build form. To complete this task Donald can either click on the link provided in the email or scroll to the next pending task in the Workflow and click on the Task: Complete Form (Pending) hyperlink.

g. Navigate to CA Process Automation as Donald Bell. You will see one pending task for to complete the Release and Deployment Plan form. RMC on the task and click Reply. Complete the information in the Plan and Build Release form. responding ‘no’ to some of the questions automatically result in the Change Order being rejected. Following is an example of the Operator’s Post Execution Code.



h. Complete the form, scroll down and click finish.

i. Navigate to the Change Order and scroll through the tasks.

You will see a notification has one out to the Change Manager, Donald Bell. Donald must Authorize Build and Test Release. To complete this task Donald can either click on the link provided in the email or can scroll to the next pending task in the Workflow and click on the Task: Complete Form (Pending) hyperlink.

j. Navigate to CA Process Automation as Donald Bell. You will see one pending task to Authorize Build and Test Release. RMC on the task and click Reply. Complete the information in the Build and Test Release form and click finish.

k. Navigate to the Change Order.
The status has changed to 'Test'.

l. Scroll through the tasks.
You will see a notification has one out to the Change Manager, Donald Bell. Donald must complete the Release and Deployment Test form. To complete this task Donald can either click on the link provided in the email or scroll to the next pending task in the Workflow and click on the Task: Complete Form (Pending) hyperlink.

m. Navigate to CA Process Automation as Donald Bell.
You will see one pending task to complete Release and Deployment Build and Test form.

n. RMC on the task and click Reply. Complete the information in the Release and Deployment Build and Test form and click finish.

o. Navigate to the Change Order and scroll through the tasks.
You will see a notification has one out to the Change Manager, Donald Bell. Donald must authorize checkin of baselined release package into the DML. To complete this task Donald can either click on the link provided in the email or scroll to the next pending task in the Workflow and click on the Task: Approve/Reject (Pending) hyperlink.

p. Navigate to CA Process Automation as Donald Bell.
You will see one pending task to authorize checkin of baselined release package into DML. RMC on the task and hit 'Reply'. Authorize checkin of baselined release package into DML by SACM, scroll down and hit finish.

20. Navigate to the Change Order. Change Manager and CAB Approval is required as the 'type' and level of 'risk' is associated with the Change. The status has changed to 'Approval in Progress' and the 'CAB Approval' flag is set to yes. Scroll through the tasks.

    You will see a notification has one out to the Change Manager, who is the manager of the Implementation Group, Donald Bell. Donald must approve or reject the Change Order. To complete this task Donald can either click on the link provided in the email or scroll to the next pending task in the Workflow and click on the Task: Approve/Reject (Pending) hyperlink.

21. Navigate to CA Process Automation as Donald Bell.

    You will see one pending task to approve/reject Change Order.

22. RMC on the task and click Reply.

23. Complete the Approval/Rejection comments. Dependent upon whether the Change Manager Approves, Rejects, or marks the Change Order Incomplete, the Workflow takes different paths. Mark it as 'Approved'.

24. Navigate to the Change Order. Select Additional Information, Workflow Tasks, and scroll down through the tasks. You will see a notification has gone out to the CAB, including the CAB Manager, who incidentally is also Donald Bell. The CAB Manager, Donald, needs to Approve or Reject the Change Order on behalf of the CAB. To complete this task John can either click on the link provided in the email or scroll to the next pending task in the Workflow and click on the Task: Approve/Reject (Pending) hyperlink.

25. As Donald, you see one pending task for CAB Approval. RMC on the task and hit 'Reply'.

26. Complete CAB Date/CAB Chair, and the CAB Approval/Rejection comments. Dependent upon whether the CAB Manager Approves, Rejects, or marks the Change Order Incomplete, the Workflow will take different paths. In this case mark it as 'Approved'.

27. Navigate back to the Change Order. The status of the Change Order is now 'Approved'. Click on the WF Tasks Tab. Scroll down through the tasks. You will see a notification has gone out to the Implementation Group, of which John McCarthy is a member. The Implementation Group is now responsible for implementing the RAM upgrade on TIXCHANGE.

28. To complete this task Donald can either click on the link provided via email, or alternatively, he can scroll to the next pending task in the Workflow and click on the hyperlink for 'Task: Other (Pending)'. As Donald, you will need to click on 'Group Tasks' on the left hand side of the pane since this task of Implementing the Change Order is assigned to the full Implementation Group. RMC on the Implementation task and hit 'Reply'.

29. The link in this task will bring you directly into CA SDM in context of the Change Order. Once the Implementation Group begins the RAM upgrade, Donald can hit Finish to complete the task.

30. Navigate back to the Change Order. The status has changed from 'Approved' to 'Implementation in Progress'. Click on the WF Tasks Tab. Scroll down through the tasks. You will see a notification has gone out to all of the members of the Implementation Group, of which Donald Bell is a member. The Implementation Group is now responsible for confirming the successful implementation of the patches. To complete this task Donald can either click on the link provided via email, or alternatively, he can scroll to the next pending task in the Workflow and click on the hyperlink for 'Task: Complete Form (Pending)'.

31. As Donald, you will again need to click on 'Group Tasks' on the left hand side of the pane since this task of confirming implementation of the Change Order is assigned to the full Implementation Group. RMC on the Implementation Complete task and hit 'Reply'. Implementation Status as 'Complete' or 'Incomplete' and as a result the Workflow will take different paths. In our case we will mark it as 'Complete'.

32. Navigate back to the Change Order. Navigate back to the Change Order. The status has changed to Deployed.

> **Note:** The workflow will proceed to this step if you answered 'Yes' to Release Verification. Otherwise skip to step 33.

a. Click on the WF Tasks Tab. Scroll down through the tasks. You will see a notification has gone out to the Change Manager, Donald Bell, who needs to update the release number of all records of all Service CI's associated with this Release. To complete this task Donald can either click on the link provided via email, or alternatively, he can scroll to the next pending task in the Workflow and click on the hyperlink for 'Task: Approve/Reject (Pending)'.

b. As Donald, you will again need to click on 'Group Tasks' on the left hand side of the pane since this task of confirming implementation of the Change Order is assigned to the full Implementation Group. RMC on the Implementation Complete task and hit 'Reply'. Donald updates the release number of all Service CI's associated with the Release.

c. Once complete he can hit 'Finish' on the task.

33. Navigate back to the Change Order. The closure code has been set to 'successful'. Click on the WF Tasks Tab. Scroll down through the tasks. You will see a notification has gone out to all of the members of the Implementation Group, of which Donald Bell is a member. The Implementation Group is now responsible for doing a Post Implementation Review (PIR). To complete this task John can either click on the link provided via email, or alternatively, he can scroll to the next pending task in the Workflow and click on the hyperlink for 'Task: Complete Form (Pending)'.

34. As John, you will again need to click on 'Group Tasks' on the left hand side of the pane since this task of confirming implementation of the Change Order is assigned to the full Implementation Group. RMC on the Post Implementation Review task and hit 'Reply'.

35. Complete the Post Implementation Review Form, and once complete hit 'Finish'.

36. Navigate back to the Change Order. The status of the CO is set to 'Closed' as all steps in the Workflow are now complete and the RAM upgrade was successful.

CA Service Management Reports

This section lists the out-of-the-box CA Business Intelligence reports:

CA Asset Portfolio Management Reports

The following table lists the CA Business Intelligence reports available with CA Asset Portfolio Management:

Report Name	Report Description	Used By Role
	Report of billed assets not matched to any discovery record	

Billed Assets not matched to any discovery record		Administrator
Discovered assets not matched to any owned asset	List of discovered assets not reconciled to any owned asset	Administrator
Discovered assets not processed due to missing or invalid data	This report shows the list of discovered assets not processed because of missing or invalid data	Administrator
Discovered inventory records matched with network discovery data	List of matches between network data and discovery data	Administrator
In-scope owned assets matched to discovery records	Report of in-scope owned assets matched to discovery records	Administrator
In-scope owned assets not matched to discovery records	Report of in-scope owned assets not matched to discovery records	Administrator
Lost Revenue Report	Report identifying potential lost revenue,which includes assets in a non-active status but discovered, as well as assets in an active status, but not billing	Executive, Administrator
Network Discovery Exception Report	List of network discovery records that have not been matched to any corresponding discovered inventory	Administrator
Owned assets matched with discovered assets	Report of owned assets reconciled to discovered assets - either discovered inventory or network discovery or both	Administrator

CA Service Desk Manager Reports

The following table lists the CA Business Intelligence reports available with CA Service Desk Manager:

Report Name	Folder Name (Public Folders > CA Reports > CA Service Management > CA Service Desk)	Report Description	Report Type
Overall Summary	Aggregate	Shows the count of Requests and Change Orders created and closed, between the start and end dates, as well as the average time to close. Also contains a report of the Top5 Request Areas associated with Requests and a report of the Top 5 Categories for Change Orders	Crystal Reports

Asset List	Asset	Shows the Resource Family (Hardware, Software etc.), the type of Asset (keyboard, modem etc.), the serial number for that Asset and a more detailed description of the Asset.	Crystal Reports
Active Change Orders Aging	Change Order\Aging	Shows count of all open Change Orders by the number of weeks open	Crystal Reports
Active Change Orders Aging for Categories		Shows count of open Change Orders by the number of weeks open. User must input a Category name for a search of Change Orders in that Category	Crystal Reports
Active Change Orders Aging for Groups		Shows count of open Change Orders by the number of weeks open. The see results for a specific Group(s), user must select the Group Name(s).	Crystal Reports
Active Change Orders Aging for Priority		Shows count of open Change Orders by the number of weeks open. Adjacent bars break up counts by Priorities.	Crystal Reports
Active Change Orders Aging by Priority for Categories		Shows count of open Change Orders by the number of weeks open. Adjacent bars break up counts by Priorities. User must input Category name for a search of Change Orders in that Category.	Crystal Reports
Active Change Orders Aging by Priority for Groups		Shows count of open Change Orders by the number of weeks open. Adjacent bars break up counts by Priorities. User must input a Group name for a search of Change Orders in that Group.	Crystal Reports
Active Change Orders Aging by		Shows count of open Change Orders by the number of weeks open. Adjacent bars break up counts by Priorities. User must input a Status for a search of Change Orders with that Status.	Crystal

Priority for Status			Reports
Active Change Orders Aging for Status		Shows count of open Change Orders by the number of weeks open. User must input a Status for a search of Change Orders with that Status.	Crystal Reports
All Rejected Change Orders	Change Order\Compliance	Shows total number of Change Orders, number of rejected Change Orders, % of Change Orders rejected during approval phase, group by Change Category, Change Group, for the specified period.	Crystal Reports
Average duration of Change Orders		Shows total number of Change Orders, average duration for Change Order completion, group by Change Category, Change Group, for the specified period.	Crystal Reports
Change Order implementation Cost Details		Shows the associated costs for Change Order for each Change Category, group by Change Group, Change Category, No. of Change Order, Actual Cost and Estimated Cost for all Change Orders, for the specified period.	Crystal Reports
Change Order in Detail		Shows complete details of the Change Order(s).	Crystal Reports
Change Orders by Change Type		Shows total number of completed Change Orders and % of Change Orders for each Change Type, group by Change Group and Change Category for the specified period.	Crystal Reports
Change Orders by Closure Code		Shows total number of Change Orders and % of Change Orders for each Closure Code, group by Change Group and Change Category for the specified period.	Crystal Reports
Change Orders Initiated		Shows total number of Change Orders, Change Orders initiated by Incident /Problem and % of Change Orders initiated by Incident/Problem, group by Change Group and Change Category for the specified period.	Crystal

by Problem /Incident			Reports
Change Orders outside Blackout Window		Shows total number of Change Orders, number of Change Orders scheduled outside Blackout Window and % of Change Orders scheduled outside the Blackout Window, group by Change Group and Change Category for the specified period.	Crystal Reports
Change Orders outside Maintenance Window		Shows total number of Change Orders, number of Change Orders scheduled outside Maintenance Window and % of Change Orders scheduled outside the Maintenance Window, group by Change Group and Change Category for the specified period.	Crystal Reports
Configuration Items Associated to Change Order		Shows Configuration Items, number of associated Change Orders, group by Change Group and Change Category for the specified period.	Crystal Reports
Change Orders Approved and Scheduled for Implementation	Change Order\Forecast	Shows Change Order number, Change Group, Change Category, Priority, Risk Level, Status and Planned Implementation Date of all Change Orders that are approved and planned for implementation.	Crystal Reports
Change Order Waiting for CAB approval		Shows Change Orders waiting for CAB Approval, Change Order number, Change Category, Priority, Risk Level, Status, Planned Implementation Date & Time and number of elapsed days since opened.	Crystal Reports
Analyst Count by Priority of Open Change Orders	Change Order\Resource	Shows open Change Orders counts that are displayed by Analyst assigned to the Change Orders and broken up by Priority.	Crystal Reports
Change Orders by Failed Service Type for Groups		Shows % of each Service Type failure based on the total Service Type failures in one Group, in specific Groups or in ALL Groups.	Crystal Reports

Workflow Tasks Pending		Shows list of Workflow Tasks that are in a Pending Status and the duration (within Workshift hours) that it has been in Pending Status from the time the Workflow Task started.	Crystal Reports
Trend Report by Group	Change Order\Trend	Shows historical data of % of Change Orders for each Closure Code grouped by Change Group for specified Change Groups.	Crystal Reports
Active Change Orders at Weeks End	Change Order\Volume	Shows counts of opened Change Orders for today, 7 days ago, 14 days ago and so for a 5 week period.	Crystal Reports
Change Order Totals by Assignee		Shows total number of Change Orders assigned to each Assignee. A start and end date must be entered. Also, User ID and the analyst(s) last name needs to be specified or ALL for a list of all analysts. Estimate Time and Cost are shown, plus the Total Time and Cost and average Time to Close.	Crystal Reports
Change Orders by Failed Service Type for Change Categories		Shows the % of each Service Type failure based on the total Service Type failures in a particular Change Category, or a group of specific Change Categories, or in ALL Change Categories.	Crystal Reports
Change Orders by Failed Service Type for Statuses		Shows the % of each Service Type failure based on the total Service Type failures in a particular Change Status, or a group of specific Change Statuses, or in ALL Change Statuses.	Crystal Reports
Change Categories Currently Active		Shows count of open Change Orders by Change Category.	Crystal Reports
Total No. of Change Orders implemented		Shows number of Change Orders which are closed in the specific period for each Change Group.	Crystal Reports

Total Volume of Change Orders		Shows counts of both opened and closed Change Orders for today, 7 days ago, 14 days ago and so for about a 5 week period.	Crystal Reports
Total Volume of Change Orders by Interface		Shows counts of both opened and closed Change Orders by interface for today, 7 days ago, 14 days ago and so for about a 5 week period.	Crystal Reports
Workflow Task Aging		Shows a list of Workflow Tasks and duration (within Workshift hours) it took to complete one task to another per Change Order.	Crystal Reports
Properties Values by Property	Change Order\Volume\Properties	Shows a list of Change Order properties based on the open date range selected. The list shows each Property and all the responses to that Property.	Crystal Reports
Change Properties by Category		Shows a list of all Change Order and their Properties with an open date in the selected date range, grouped by Change Category.	Crystal Reports
Mean Time To Acknowledge & Mean Time To Resolve	Incident and Problem Management \Effectiveness	Shows annual trend of mean time to acknowledge (MTTA) and the mean time to resolve (MTTR) requests against the current month and the previous 3 months.	Crystal Reports
SLA Violation	Incident and Problem Management\SLA	Shows annual trend on % of SLA violation against the opened requests volume.	Crystal Reports
Incident Traceability Matrix	Incident and Problem	Shows a list of the Incidents and related Problems and Change Orders. Hyperlink on the Incident number opens a sub-report showing the brief details of the Incidents, Problems and Change Orders.	Crystal Reports

Problem Traceability Matrix	Management \Traceability Matrix	Shows a list of the Problems that have relationships with Incidents and Change Orders. Hyperlink on the Problem number opens a sub-report showing the brief details of the Problems, Incidents and Change Orders.	Crystal Reports
Volume Trend	Incident and Problem Management\Count	Shows annual trend of opened and closed requests based on selected annual trending parameter.	Crystal Reports
Active Issues Aging	Issue\Aging	Shows count of all open Issues by number of weeks open.	Crystal Reports
Active Issues Aging for Priority		Shows count of all open Issues by number of weeks open. Adjacent bars break up counts by Priorities.	Crystal Reports
Active Issues Aging by Priority for Categories		Shows count of all open Issues by number of weeks open. Adjacent bars break up counts by Priorities. User must input a Category name for a search of Issues in that Category.	Crystal Reports
Active Issues Aging by Priority for Groups		Shows count of all open Issues by number of weeks open. Adjacent bars break up counts by Priorities. User must input a Group name for a search of Issues in that Group.	Crystal Reports
Active Issues Aging by Priority for Status		Shows count of all open Issues by number of weeks open. Adjacent bars break up counts by Priorities. User must input a Status.	Crystal Reports
Active Issues Aging for Categories		Shows count of Issues by number of weeks open. User must input a Category name for a search of only Issues in that Category.	Crystal Reports

Active Issues Aging for Groups		Shows count of all open Issues by number of weeks open. User must input a Group(s).	Crystal Reports
Active Issues Aging for Status		Shows count of all open Issues by number of weeks open. User must input a Status.	Crystal Reports
Analyst Count by Priority of Active Issues	Issue\Resource	Shows active Issue counts by Analyst assigned to the Issue and broken up by Priority.	Crystal Reports
Issues by Failed Service Type for Groups		Shows % of each Service Type failure based on the total Service Type failures in one Group, in specific Groups or in ALL Groups.	Crystal Reports
Plan Task Pending		Shows list of Plan Tasks that are in a Pending Status and the duration (within Workshift hours) that is has been in Pending Status from the time the Plan Task started.	Crystal Reports
Active Issues at Weeks End	Issue\Volume	Shows count of opened Issues for today, 7 days ago, 14 days ago, and so on for 5 weeks. Counts are shown on the bars for each week ending date. The opened Issue counts, for each week ending date, include the previous 6 days up to and including the 7th day (week ending date).	Crystal Reports
Issues Categories Currently Active		Shows count of open Issues by Category.	Crystal Reports
Issue Totals		Start and end date must be entered. Analyst(s) last name needs to be specified or ALL for a list of all Analysts. Estimated Time and Cost are shown, plus the Total Time and Cost and average Time to Close.	Crystal Reports

Issues by Failed Service Type for Categories		Shows % of each Service Type failure based on the total Service Type failures in a particular Change Category, or a group of specific Change Categories or in ALL Change Categories.	Crystal Reports
Issues by Failed Service Type for Status		Shows % of each Service Type failure based on the total Service Type failures in a particular Status, or a group of specific Statuses or in ALL Statuses.	Crystal Reports
Plan Task Aging		Shows list of Plan Tasks and the duration (within Workshift hours) it took to complete one task to another, per Change Order.	Crystal Reports
Total Volume of Issues		Shows count of both opened and closed Issues for today, 7 days ago, 14 days ago and so on for about 5 weeks.	Crystal Reports
Total Volume of Issues by Interface		Shows count of both opened and closed Issues by Interface for today, 7 days ago, 14 days ago and so on for about 5 weeks.	Crystal Reports
Issue Properties by Category	Issue\Volume\Properties	Shows list of all Issues and their Properties with an open date in the selected date range, grouped by Category.	Crystal Reports
Issue Property Values		Shows list of all values for each Issue Property with an Issue open date in the selected date range.	Crystal Reports
Service Desk Application-Level Transaction Measurements	Key Performance Indicator	Produces graphs showing a comparison of transaction processing times for a chose system type KPI over a specified period of time.	Web Intelligen

			ce Report
Service Desk Application-Level Transaction Rates of Change		Produces a line graph showing the rate of change for a selected system activity during a selected time frame. Information displayed is derived from data gathered over time by active KPIs of type system.	Web Intelligence Report
Service Desk SQL and Stored Query KPI Values		Produces a line graph showing values collected by a selected KPI over a selected time frame. Information displayed is derived from data gathered over time by active KPIs of type SQL and Stored Query.	Web Intelligence Report
Document Usage by Contact	Knowledge Management\Contact Activity	Shows how Knowledge Documents have been utilized and is sorted by Contact.	Crystal Reports
Searches by Contact		Shows Knowledge Tools searches by Contact.	Crystal Reports
System Usage by Contact		Shows Knowledge Tools session and search information sorted by Contact.	Crystal Reports
User Sessions - Visits to Site		Shows Knowledge Tools session and search information sorted by Contact.	Crystal Reports
		Shows Issues opened without searching Knowledge.	

Users Opening Issues without Searching Knowledge			Crystal Reports
Users Opening Requests without Searching Knowledge		Shows Requests opened without searching Knowledge.	Crystal Reports
Comments by Contact		Shows Comments on Knowledge Documents sorted by Contact.	Crystal Reports
Document FAQ Rating	Knowledge Management\Knowledge Document Effectiveness	Shows Knowledge Documents sorted by FAQ Rating.	Crystal Reports
Comments by Document		Shows Comments sorted by Knowledge Document.	Crystal Reports
Document Ratings		Shows a list and pie chart of Knowledge Document Ratings.	Crystal Reports
Documents Viewed Detail		Shows details about the viewing of a specific Knowledge Document.	Crystal Reports
		Shows Knowledge Documents viewed least frequently.	Crystal

Least Frequently Viewed Documents			Reports
Most Frequently Viewed Documents		Shows Knowledge Documents viewed most frequently.	Crystal Reports
Knowledge Feedback		Shows Knowledge Documents feedback.	Crystal Reports
Knowledge Usage for Issues		Shows information about the number of sessions where users do not open Issues, % of Self Service, the total number of Solutions, the number of Issues opened over a time frame.	Crystal Reports
Knowledge Usage for Requests		Shows information about the number of sessions where users do not open Requests, % of Self Service, the total number of Solutions, the number of Requests opened over a time frame.	Crystal Reports
Poor Votes		Shows a list of Knowledge Documents with a 'Not Helpful at All' rating.	Crystal Reports
Candidate Documents for Retirement	Knowledge Management\Knowledge Document Status	Shows a list of Knowledge Documents that are candidates for retirement.	Crystal Reports
Documents by Status		Shows Knowledge Documents grouped by Status.	Crystal Reports
		Shows Knowledge Documents created via Knowledge Categories or via Submit Knowledge and assigned to the Category Owner.	

Documents Created Via Knowledge Categories		Crystal Reports
Documents Published	Shows Knowledge Documents that have been published.	Crystal Reports
Documents Scheduled for Expiration	Shows Knowledge Documents that are scheduled to expire within the specified time frame.	Crystal Reports
Documents with Inactive Assignees	Shows Knowledge Documents with Inactive Assignees.	Crystal Reports
Documents with Inactive Owners	Shows Knowledge Documents with Inactive Owners.	Crystal Reports
Expired Documents	Shows Knowledge Documents that have expired.	Crystal Reports
Submitted Knowledge	Shows Knowledge Documents submitted via the Submit Knowledge link in the Customer, Employee UI.	Crystal Reports
Unpublished Documents	Shows Knowledge Documents that have been unpublished.	Crystal Reports

Contact FAQ Ratings	Knowledge Management\Knowledge Team Productivity	Shows summary of Knowledge Document FAQ Ratings by Contact.	Crystal Reports
Contact FAQ Ratings Detail		Shows detail of Knowledge Document FAQ Ratings by Contact.	Crystal Reports
Contact Information		Shows a list of all Contacts, with name, login, role, status, email address, last login date and Groups the Contact is a member of.	Crystal Reports
Documents Solving Issues by Contact		Shows Knowledge Documents that have solved Issues.	Crystal Reports
Documents Solving Requests by Contact		Shows Knowledge Documents that have solved Requests.	Crystal Reports
Issues solved by Document		Shows details Knowledge Documents that have solved Issues. Information about the number of Issues that were resolved by Knowledge Document are also listed.	Crystal Reports
Requests solved by Document		Shows details Knowledge Documents that have solved Requests. Information about the number of Requests that were resolved by Knowledge Document are also listed.	Crystal Reports
Knowledge Initiators Detail		Shows details of Knowledge Documents grouped by the Contact who created them.	Crystal Reports

Knowledge Initiators Summary		Shows a summary line for each Contact, how many Knowledge Documents and a % of the total number of Knowledge Documents that were created by the Contact.	Crystal Reports
Noise Words	Knowledge Management\Search Administration	Shows Knowledge Document Noise Words.	Crystal Reports
Synonyms		Shows Knowledge Document Synonyms.	Crystal Reports
Special Terms		Shows Knowledge Document Special Terms.	Crystal Reports
Issues Closed Without Knowledge	Knowledge Management\Search Effectiveness and Usage	Shows list of Issues that have not been resolved by any Knowledge Documents.	Crystal Reports
Requests Closed Without Knowledge		Shows list of Requests that have not been resolved by any Knowledge Documents.	Crystal Reports
Most Frequent Searches		Shows most frequent Knowledge Tools searches.	Crystal Reports
Searches		Shows Knowledge Tools searches for a specific date range, Search Source and Search Type.	Crystal Reports
Requests Avoided		Shows details of Requests avoided.	

			Crystal Reports
Issues Closed with Knowledge		Shows information of Issues closed with Knowledge Documents.	Crystal Reports
Requests Closed with Knowledge		Shows information of Requests closed with Knowledge Documents.	Crystal Reports
Issues Avoided		Shows details of Issues avoided.	Crystal Reports
Knowledge Documents Created from Requests	Knowledge Management\Service Desk Integration	Shows proportion of Requests to generate a Knowledge Document.	Crystal Reports
Documents Solving Requests		Shows Knowledge Documents that have solved Requests.	Crystal Reports
Documents Solving Issues Detail		Shows details of the Issues that have a specific Knowledge Document as a solution.	Crystal Reports
Documents Solving Requests Detail		Shows details of the Requests that have a specific Knowledge Document as a solution.	Crystal Reports
		Shows proportion of Issues to generate a Knowledge Document.	

Knowledge Documents Created from Issues		Crystal Reports
Documents Solving Issues	Shows Knowledge Documents that have solved Issues.	Crystal Reports
Issues Created Based on Knowledge Documents	Shows Issues created when the link "New Issue based on this Document" is selected.	Crystal Reports
Requests Created Based on Knowledge Documents	Shows Requests created when the link "New Request based on this Document" is selected.	Crystal Reports
Time to Issue Resolution	Shows average time to resolve Issues when Knowledge is used or accepted as a solution.	Crystal Reports
Time to Request Resolution	Shows average time to resolve Requests when Knowledge is used or accepted as a solution.	Crystal Reports
Linked Knowledge To Issues	Shows linked Knowledge to Issues.	Crystal Reports
	Shows linked Knowledge to Requests.	Crystal

Linked Knowledge To Requests			Reports
Knowledge Management Metrics	Knowledge Management\System Reports	Shows various Knowledge Management metrics about Searches, Knowledge Life Cycle Management and others.	Crystal Reports
CI Maintenance Windows Conflict	MSP Reports	Shows the CIs that are linked to scheduled change and have conflicting maintenance windows.	Crystal Reports
Created Configuration Items Report		Shows all newly created CIs within the specified date range.	Web Intelligence Report
Deleted Configuration Items Report		Shows all CIs deleted within the specified date range.	Web Intelligence Report
Detailed Incident Source		Shows list of Incidents recorded in order to demonstrate the added value of service.	Web Intelligence Report
Incident Categories		Shows closed Incidents that do not have an associated Service Type.	Web Intelligence

without Service Type Report		ence Report
Incident Resolution Method	Shows Incidents that could have been resolved by lower level support groups for training purposes and to provide additional value to customer service packages.	Web Intelligence Report
Incident Resolution Report	Shows list of all the resolution codes used within the specified time period.	Web Intelligence Report
Incident Source Report	Shows total number of Incident requests by source.	Web Intelligence Report
Incidents by Category	Shows major Incidents for contract purposes, process performance, billing and compliance.	Web Intelligence Report
Incidents by Hardware Model	Shows count of total and closed Incidents associated with a CI by Hardware Model.	Web Intelligen

			ce Report
Incidents without associated Asset or CI		Shows list of Incidents recorded without an associated Asset or CI in order to demonstrate the added value of service.	Web Intelligence Report
Re-Categorized Incidents		Shows Incidents that required re-categorization upon resolution for billing and training purposes.	Crystal Reports
Reassigned Incidents Report		Shows Incidents that required to be re-assigned upon resolution for billing and training purposes.	Crystal Reports
Detail Incident Source	MSP Reports\Dashboards	Multi-tenancy required	Dashboard
Incident Resolution Dashboard		Multi-tenancy required	Dashboard
Incidents by Category		Multi-tenancy required	Dashboard
Incidents by Hardware Model		Multi-tenancy required	Dashboard
Re-Categorized Incidents		Multi-tenancy required	

			Dashboard
Reassigned Incidents Report		Multi-tenancy required	Dashboard
Created Configuration Items Report-Detail (Multi-Tenancy Required)	MSP Reports\Detail	Shows all newly created CIs within specified date range.	Web Intelligence Report
Dashboard Re-Categorized Incidents (Multi-Tenancy Required)		Shows Incidents that required re-categorization upon resolution for billing and training purposes.	Crystal Reports
Dashboard Detailed Incident Source (Multi-Tenancy Required)		Shows list of Incidents recorded in order to demonstrate the added value of service.	Crystal Reports
Deleted Configuration Items Report-Detail (Multi-Tenancy Required)		Shows details of deleted (marked Inactive) CIs within specified date range.	Crystal Reports
Detailed Incident Source		Shows list of Incidents recorded for each Category in order to demonstrate the added value of service.	Crystal

for Category (Multi-Tenancy Required)		Reports
Detailed Incident Source (Multi-Tenancy Required)	Shows list of Incidents recorded in order to demonstrate the added value of service.	Crystal Reports
Detailed Incident (Multi-Tenancy Required)	Shows lists of Incidents recorded in order to demonstrate the added value of service.	Crystal Reports
Detailed Resolution Report (Multi-Tenancy Required)	Shows lists of Resolutions recorded in order to demonstrate the added value of service.	Crystal Reports
Incident by Category Dashboard components (Multi-Tenancy Required)		Crystal Reports
Incident by Hardware Model-Detail (Multi-Tenancy Required)	Shows details of all closed Incidents.	Crystal Reports
Incident Categories without Service	This report cannot be viewed independently as this is a detail report.	Crystal

Type-Detail (Multi-Tenancy Required)			Reports
Incident Resolution Report Dashboard (Multi-Tenancy Required)			Crystal Reports
Incident Resolution Report Details Dashboard (Multi-Tenancy Required)			Crystal Reports
Incidents by Hardware Model - DB (Multi-Tenancy Required)			Crystal Reports
Incident by Category Dashboard Details Report (Multi-Tenancy Required)			Crystal Reports
Service Desk Manager Daily Operations	Operational Dashboard		

Active Request by Priority-Detail	Operational Dashboard \Request		Dashboard
Active Request by Priority-Main			Dashboard
Active Requests by Analyst			Dashboard
Active Requests by Category			Dashboard
Active Requests by Group			Dashboard
Active Incident by Priority-Detail	Operational Dashboard \Incident		Dashboard
Active Incident by Priority-Main			Dashboard
Active Incidents by Analyst			Dashboard
Active Incidents by Category			Dashboard
Active Incidents by Group			

			Dashboard
Active Problem by Priority-Detail	Operational Dashboard \Problem		Dashboard
Active Problem by Priority-Main			Dashboard
Active Problems by Analyst			Dashboard
Active Problems by Category			Dashboard
Active Problems by Group			Dashboard
Active Change Order by Priority-Detail	Operational Dashboard \Change Order		Dashboard
Active Change Order by Priority-Main			Dashboard
Active Change Orders by Analyst			Dashboard

Active Change Orders by Category			Dashboard
Active Change Orders by Group			Dashboard
Active Issue by Priority-Detail	Operational Dashboard\Issue		Dashboard
Active Issue by Priority-Main			Dashboard
Active Issues by Analyst			Dashboard
Active Issues by Category			Dashboard
Active Issues by Group			Dashboard
Service Desk Manager Daily Operations	Operational Dashboard		
Active Requests Aging by Priority for Groups	Request\Aging	Shows count of open Requests by the number of weeks open. Adjacent bars break up counts by Priorities. User must input a Group name for a search of Requests in that Group.	Crystal Reports

Active Requests Aging by Priority for Request Areas		Shows count of open Requests by the number of weeks open. Adjacent bars break up counts by Priorities. User must input a Request Area for a search of Requests in that Request Area.	Crystal Reports
Active Requests Aging by Priority for Status		Shows count of open Requests by the number of weeks open. Adjacent bars break up counts by Priorities. User must input a Status name for a search of Requests in that Status.	Crystal Reports
Active Requests Aging		Shows count of all open Requests by number of weeks open.	Crystal Reports
Active Requests Aging for Groups		Shows count of all open Requests by number of weeks open. User must input a Group Name for a search of only Requests in that Group.	Crystal Reports
Active Requests Aging for Priority		Shows count of open Requests by the number of weeks open. Adjacent bars break up counts by Priorities.	Crystal Reports
Active Requests Aging for Request Areas		Shows count of open Requests by the number of weeks open. User must input a Request Area for a search of Requests in that Request Area.	Crystal Reports
Active Requests Aging for Status		Shows count of open Requests by the number of weeks open. User must input a Status name for a search of Requests in that Status.	Crystal Reports
Volume and Trend	Request\Count	Shows annual trend of opened and closed Requests based on a user selected annual trending parameter.	Crystal Reports

Mean Time To Acknowledge & Mean Time To Resolve	Request\Effectiveness	Shows annual trend of mean time to acknowledge (MTTA) and the mean time to resolve (MTTR) requests against the current month and the previous 3 months.	Crystal Reports
Analyst Count by Priority of Active Requests	Request\Resource	Shows open Request counts by Priority grouped by Analyst.	Crystal Reports
Analyst Summary		Shows the number of Analysts assigned to Requests by Status.	Crystal Reports
Request Aging Detail by Organization and Analyst		Shows detailed summary of all currently opened Requests by Organization and Analyst and the last activity that occurred and by whom. Sorted descending on time open.	
Request List by Analyst		Shows a list of Requests assigned to each Analyst.	Crystal Reports
Violated SLA for Groups		Shows the number of Requests violated by the number of time violated. Requires a start and end date, and Group name for a search of only Requests opened during that date range and assigned to that Group or all Groups.	Crystal Reports
Requests by Failed Service Type for Groups		Shows % of each Service Type failure based on the total Service Type failures on one Group, in certain Groups or in all Groups.	Crystal Reports
SLA Violation	Request\SLA	Shows annual trend on % of SLA violation against the opened requests volume.	Crystal Reports
		Shows a list of active Requests grouped by Analyst.	

Active Request List	Request\Volume		Crystal Reports
Active Requests at Weeks End		Shows count of opened Issues for today, 7 days ago, 14 days ago, and so on for 5 weeks. Counts are shown on the bars for each week ending date. The opened Request counts, for each week ending date, include the previous 6 days up to and including the 7th d	Crystal Reports
Activity of Requests		Shows a list of activities for all Requests, grouped by Request.	Crystal Reports
Analyst List by Organization		Shows a list of Analysts organized by their Organization.	Crystal Reports
Key Organization Summary		Shows detail of all the active Requests by Organization.	Crystal Reports
Open /Closed Call Analysis by Analyst		Shows a count of Requests active at the start date, new Requests entered during the period, Requests closed during the period, the number of active Requests at the end of the period and the change in the number of active Requests over the period.	Crystal Reports
Request Activity Counts by Customer Organization		Shows a count of Request Activities by type, sorted by Customer Organization. The counts are based on Requests that were opened between the Start and End Dates.	Crystal Reports
Request Aging Detail		Shows a detailed summary of all currently opened Requests by Organization and the last Activity that occurred and by whom.	Crystal Reports

Request Areas Currently Active		Shows the count of open Requests by Request Area.	Crystal Reports
Request List		Shows a list of Requests.	Crystal Reports
Request List by Organization		Shows a list of Requests grouped by Customer Organization.	Crystal Reports
Request List by Priority		Shows a list of Requests grouped by Priority.	Crystal Reports
Request List by Request Area		Shows a list of Requests grouped by Request Area.	Crystal Reports
Request Properties by Request Area	Request\Volume\Properties	Shows a list of all Requests and their Properties within the user selected date range, grouped by Request Area.	Crystal Reports
Request Property Values		Shows a list of Request Properties based on the Open Date range selected. The list shows each Property and all the responses to that Property.	Crystal Reports
Not Closed Requests by Priority	Request\Volume\By Customer Location	Shows a count of Requests with no Closed Date by Customer Location. The numbers are further broken down by Priority. Additionally, the report totals the number of Requests active, inactive and with a SLA violation.	Crystal Reports
		Shows a count of Requests with no Close Date and attached Change Orders. The numbers are grouped by Customer Location and Priority.	

Not Closed Requests by Priority with Attached Change Orders			Crystal Reports
Resolved Requests by Priority with Resolved Date		Shows a count of Requests that have been resolved but not yet closed. Requests are listed by Customer Location and Priority.	Crystal Reports
Analyst Logins	Support Automation	Shows detailed information for each analyst login.	Crystal Reports
Analyst Metrics		Shows summary information for each analyst, including KPI metrics. Data is for all sessions completed during the analyst login session where the login itself occurred in the date range.	Crystal Reports
Assistance Sessions		Shows detailed report of all assistance sessions.	Crystal Reports
Assistance Sessions Metrics		Shows summary data of the assistance sessions conducted by the help desk.	Crystal Reports
Tool Usage Summary		Shows summary information about which tools are being used for assistance sessions. For each tool, the number of session it was used in is shown, with the number sub-totaled by ticket category and with a grand total.	Crystal Reports
Queue Entries		Shows detailed metrics information for each queue entry.	Crystal

			Reports
Queue Entry Metrics		Shows summary data by queue about the queue entries.	Crystal Reports
Automated Task Execution		Shows detail information for each automated task (script) execution.	Crystal Reports
Automated Task Summary		Shows a summary for each script showing the number of times it has been executed and the status of those executions.	Crystal Reports
Active Queued End Users		Shows real time information about end users, placed in support queues.	Crystal Reports
Active Assistance Sessions		Shows real time data of currently active assistance sessions.	Crystal Reports
Survey Detail	Survey	Shows details of a given Survey name (or ALL) that lists the specifics of each Survey completed. It will look very similar to the actual Survey, but filled in with the Customer choices and comments.	Crystal Reports
Survey Summary		Shows a summary of a given Survey name (or ALL) that lists the % and counts of responses for each answer, per question, based on the total number of responses for this Survey.	Crystal Reports
Survey Summary with Comments		Shows a summary of a given Survey name (or ALL) that lists the % and counts of responses for each answer, per question, based on the total number of responses for this Survey. Includes Customer comments.	Crystal

			Reports
CI Maintenance Windows	CMDB	Shows the CIs that are linked to multiple services and have multiple maintenance windows.	Crystal Reports
CIs Added in Time Range Report		Shows a list of CIs added during the specified date range and for specified tenant(s). The report lets you view the related CI Name, Family, Class, Responsible Organization and Location.	Crystal Reports
CIs by MDR Report		Shows a list of all CIs for a specific Management Data Repository (MDR) name or grouped by all MDRs for the specific tenant(s). The report lets you view the related CI Name, Family, Class, Responsible Organization and Location.	Crystal Reports
CIs by Owner Report		Shows all the CIs for a specific Owner last name grouped by all Owners for the specific tenant(s). The report lets you view the related CI Name, Family, Class, Responsible Organization and Location.	Crystal Reports
CIs by Tenant Report		Shows all the CIs for a specific Tenant name grouped by all Tenant(s). The report lets you view the related CI Name, Family, Class, Responsible Organization and Location.	Crystal Reports
CIs Change Anomaly Report		Shows a list of all CIs to which changes have been made during the specified date range and tenant.	Crystal Reports
CIs Details Report		Shows a list of CIs for a specific Location or grouped by all Locations for the specific tenants. The report lets you view the related CI Name, Family, Class, and Responsible Organization. Can also view the assets if there are no CIs.	Crystal Reports
CIs Related to		Shows a list of all the CIs along with the Incident and the Problem count for specified tenant(s). The report lets you view the related CI Name, Family, Class, Responsible Organization and Location.	Crystal

Incidents and Problem Report			Reports
CIs Relationship Changes Report		Shows a list of all CIs for which the relationships have been changed or deleted for the specified date range and for the specified tenant.	Crystal Reports
CIs Scheduled Changes Report		Shows a list of all the CIs along with the related Change Orders and the RFC Scheduling details for specified tenant(s). The report lets you view the related CI Name, Family, Class, Responsible Organization and Location.	Crystal Reports
CIs Updated in Time Range Report		Shows a list of all the updated/modified CIs for the specified date range and for the specific tenant(s). The report lets you view the related CI Name, Family, Class, Responsible Organization and Location.	Crystal Reports
CIs With Change Orders Report		Shows a list of all CIs with the Change Order counts for the specified tenant (s). The report lets you view the related CI Name, Family, Class, Responsible Organization and Location.	Crystal Reports
All Change Impact Report	CMDB\SQL Server (These Reports will work on SQL Server only)	Shows a list of CIs which have a direct relationship with the specified CI for the specified tenants. Lets you view the CIs according to Family, Relation Type, CI Class, Responsible Organization and Location. Can view active and inactive CIs.	Crystal Reports
CIs Relationships Report		Shows a list of all the Dependent and Provider CIs for the specified tenants. Lets you view the CIs according to Family, Relation Type, CI Class, Responsible Organization and Location. Can view active	Crystal Reports
CIs Root Cause Analysis Report		Shows a list of all CIs that have been modified during the specified date range and have a direct or indirect relationship with the specified CI for the specified tenants. The report lets you view the CIs according to the user who modified the CI and the Relationship Type. You can also view the Dependent and Provider CIs for the specified CI, along with the old and new values.	Crystal Reports
All Change Impact Report		Shows a list of CIs which have a direct relationship with the specified CI for the specified tenants. Lets you view the CIs according to Family, Relation Type, CI Class, Responsible Organization and Location. Can view active and inactive CIs.	Crystal

	CMDB\Oracle (These Reports will work on Oracle Only)		Reports
CIs Relationships Report		Shows a list of all the Dependent and Provider CIs for the specified tenants. Lets you view the CIs according to Family, Relation Type, CI Class, Responsible Organization and Location. Can view active	Crystal Reports
CIs Root Cause Analysis Report		Shows a list of all CIs that have been modified during the specified date range and have a direct or indirect relationship with the specified CI for the specified tenants. The report lets you view the CIs according to the user who modified the CI and the Relationship Type. You can also view the Dependent and Provider CIs for the specified CI, along with the old and new values.	Crystal Reports
CACF Overview	CMDB\Configuration Audit & Control Facility	Shows the CACF overview within the selected time period. The report lets you view the number of Incidents that CACF created, Detected Rogue changes, Prevented Rogue changes, Variances detected, Variances prevented and Variances allowed.	Crystal Reports
CACF Policy Efficiency summary		Shows the efficiency summary of the selected policies according to the modification, activation, and deactivation dates of these policies. The report lets you view the Policy deactivation date, Policy description, number of Incidents that Policy created, rogue changes or inserts, rogue changes prevented, variances detected, variances prevented and variances allowed by the selected policies.	Crystal Reports
Change verification trending information		Shows the trends of the change verification for the selected time period. The report lets you view the number of Change Orders requiring manual verification, variances allowed by Policy, variances prevented by Policy, rogue changes and verified change specifications.	Crystal Reports
Number of Change Orders for the time period		Shows the number of Change Orders within the selected time period. The report displays the number of Change Orders with or without the Change Specifications, Change Orders where all Change Specifications were closed automatically, Change Orders where at least one Change Specification needed manual intervention and Change Orders with no associated CIs. The reports let you view the Change Orders according to the selected Categories, Assignees, Change Organizations, Requestors, Priorities, CIs, CI Classes, Contact Names, CI Locations and CI Service Organizations.	Crystal Reports
Number of CIs for the time period		Shows the number of different CIs within the selected time period. The report displays the CIs with Rogue Changes, CIs with Variances, CIs with Unverifiable Changes and CIs with verified Change Specifications. The report lets you view the CIs according to the selected CI Classes, CI Locations, Contact Names and CI Service Organizations.	Crystal Reports
		This dashboard provides insight into metrics surrounding productivity of Groups of Teams that address the request and incident demand coming from business users.	

Operational Effectiveness	CA Service Management\Scheduled Dashboard	
Service Demand - Incidents		This dashboard provides insight into incident demand from business users to IT, and supports analysis of data through various time-periods, location, tenant or service.
Operational Effectiveness	CA Service Management\View on Demand Dashboard	This dashboard provides insight into metrics surrounding productivity of Groups of Teams that address the request and incident demand coming from business users.
Service Demand - Incidents		This dashboard provides insight into incident demand from business users to IT, and supports analysis of data through various time-periods, location, tenant or service.

CA Service Catalog Reports

The following table lists the CA Business Intelligence Reports available with CA Service Catalog:

Report Name	Folder Name (Public Folders > CA Reports > CA Service Management > CA Service Catalog)	Report Description
User Requests	User Reports	Provides the details of the requests raised, approved or fulfilled by a specific user between the specific periods of time.
Account Details	Admin Reports	Shows the accounts in a BU and the details of those accounts
Adjustment Details		Provides the details of the various adjustments provided to a tenant.
Invoice Details		Provides the details of the invoices raised for a particular business unit / tenant.
Ongoing Subscription to Services		Provides the details of the active subscriptions for a user.
Payment Details		Provides the details of the payments posted to various accounts for the chosen tenant.
Request Fulfillment Details		Shows time taken to Approve, Fulfill and Complete all requests which fall within the specified date range. This Report will have the requests that are already completed.
		Report providing the details of the assets associated with various requests.

Requests - Assets Association	
Requests - Change Orders - CI Associations	Provides the details of the Change Orders and the CIs associated with the requests for a Business Unit and can be further limited to the specified User in that BU.
Requests in Specified State For More Than Threshold Duration	Provides the list of orders from tenants that have been in the specified state for more than specified duration.
Requests Overview	Provides the details of the requests by period,tenant and status.
Service Catalog for a Tenant	Provides the Catalog of various services available for the Tenant users.
Service Level Agreement Report	Report of defined service request SLAs and their associated metrics. This report acts as a tool for monitoring all SLAs for a particular tenant. ''#/#'' is defined as ''# out of #''.
Service Options Not Requested	Provides the details of the offerings that haven't been ordered by the users of the chosen tenant in the specified period of time.
Service Request Fulfilment Report	High-level report detailing service request fulfillment, including average fulfillment times. This report provides a high-level review of Service Request Fulfillment activity.''#/#'' is defined as ''# out of #''.
Service Request Lifecycle Expectations Report	Report to track and monitor end-to-end expectations of service requests within a specified date range. This report acts as a tool for viewing SLA compliance of a complete Service Request from an overarching "end-to-end" perspective, as well as broken down into its constituent components. ''#/#'' is defined as ''# out of #''.
Services - Assets Association	Report providing the Services/Service Options associated with the Asset types.
Services - CMDB Associations	Provides the associations of Services with CMDB CI's.
Services Becoming Unavailable	Provides the details for the services that are becoming unavailable in the selected time frame.
Service Usage	Report detailing the usage of various services and service options by the tenants. This report provides a tool for monitoring and determining the number of times a service / service option is used by the users.
	This report provides the details of the requests for the specified service offerings that are in various stages of the service life cycle.

Service Usage - Open Requests		
Tenant Hierarchy Information		Provides a hierarchical view of the tenants in a MSP installation.
Tenant User Information		Provides the details of the users belonging to a specific tenant and their roles in the respective tenant.
Tenant's Services Consumption		Provides the details of the costs and services consumed by the tenant between specific periods of time.
Users Requests		Provides the details of the requests raised, approved or fulfilled by a specific user between the specific periods of time.
Violated SLA Report		Report of violated service request SLAs. This report acts as a tool for monitoring and determining which SLAs have not been met. ''# /#'' is defined as ''# out of #''.
Service Level Agreement Report (CSV Export)	Admin Reports\Flat File Reports	Report of defined service request SLAs and their associated metrics. This report acts as a tool for monitoring all SLAs for a particular tenant. ''#/#'' is defined as ''# out of #''.
Service Request Fulfillment Report (CSV Export)		High-level report detailing service request fulfillment, including average fulfillment times. This report provides a high-level review of Service Request Fulfillment activity.''#/#'' is defined as ''# out of #''.
Service Request Lifecycle Expectations Report (CSV Export)		Report to track and monitor end-to-end expectations of service requests within a specified date range.This report acts as a tool for viewing SLA compliance of a complete Service Request from an overarching “end-to-end” perspective, as well as broken down into its constituent components. ''#/#'' is defined as ''# out of #''.
Violated SLA Report (CSV Export)		Report of violated service request SLAs. This report acts as a tool for monitoring and determining which SLAs have not been met. ''# /#'' is defined as ''# out of #''.
Request Details Report	Admin Reports\Dashboard Reports	
Request Details Report by MonthYear		
Request Details Report by Service		

Option, Service Name and Status		
Request Details Report by Tenant		
Service Level Agreement Dashboard		Report of defined service request SLAs that are defined from Submitted to Completed State and their associated metrics. This report acts as a tool for monitoring all SLAs for a particular tenant.
Service Request Fulfillment Dashboard		High-level report detailing service request fulfillment, including average fulfillment times. This report provides a high-level review of Service Request Fulfillment activity.
Service Request Lifecycle Expectations Dashboard		Report to track and monitor end-to-end expectations of service requests within a specified date range. This report acts as a tool for viewing SLA compliance of a complete Service Request from an overarching “end-to-end” perspective, as well as broken down into its constituent components.
SLA Dashboard by SLA		Report of service request SLAs. This report acts as a tool for monitoring and determining the SLA Compliances for each tenant.
SLA Dashboard by Tenant		Report of service request SLAs. This report acts as a tool for monitoring and determining SLA compliances for the tenant.
SLA Detail Report		Report of defined service request SLAs that are defined from Submitted to Completed State and their associated metrics. This report acts as a tool for monitoring all SLAs for a particular tenant.
SLCM Admin Dashboard		
Violated SLA Dashboard		Report of defined service request SLAs that are defined from Submitted to Completed State and their associated metrics. This report acts as a tool for monitoring all SLAs for a particular tenant.
Violated SLA Dashboard by SLA		Report of violated service request SLAs. This report acts as a tool for monitoring and determining which SLAs have not been met.
Violated SLA Dashboard by Tenant		Report of violated service request SLAs. This report acts as a tool for monitoring and determining which SLAs have not been met.
Service Demand - Requests	CA Service Management\Scheduled Dashboard	This dashboard provides insight into request demand from business users to IT, and supports analysis of data through various time-periods, location, tenant or service.
Service Demand - Requests	CA Service Management\View on Demand Dashboard	This dashboard provides insight into request demand from business users to IT, and supports analysis of data through various time-periods, location, tenant or service.

Connect

Connect with the CA Service Management community using the following links:

- Join the CA Service Management Community (https://communities.ca.com/community/ca-service-management) and collaborate with a strong community of CA Service Management users and experts.
- Subscribe to Flipboard (https://flipboard.com/section/ca-service-desk-manager-cookbook-bq2BGC) to get your copy of How-to articles and tips.
- Subscribe to our YouTube channel (https://www.youtube.com/user/catechnologies) to view the videos.
- Follow us (http://CAInc) on twitter.

TechDocs, Courses, Greenbooks

- **TechDocs** (https://support.ca.com/irj/portal/newhome)
  Access the TechDocs from CA's support.
- Education Courses (http://www.ca.com/us/ca-education.aspx)
  View and sign up for the education courses that are available for CA Service Management products.
- Green Books and Green Papers (https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=%7BF1A711CF-D358-4DB6-9518-138D19D73CBE%7D)
  Access the Green Books and Green Papers for CA Service Management products.

Pre-Built CA Process Automation Workflows

This section provides the steps required to integrate the pre-built CA Process Automation workflows with CA Service Catalog. It is assumed that each CA Service Management product in the solution has been appropriately installed in a certified architecture.

Ensure that the following products are installed before you proceed with the integration:

- CA EEM
- CA Process Automation
- CA Service Catalog
- Java Runtime Environment is

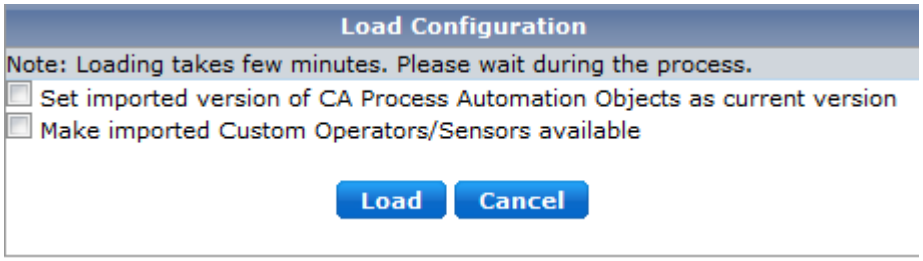
Important! Take a back up of the custom process files before you upgrade with the latest CA Process Automation Content files.

Follow these steps:

Step 1 - Load Pre-Built CA Process Automation Workflows for CA Service Catalog

Follow these steps:

1. Log in to CA Service Catalog as the Service Delivery Administrator (spadmin)
2. Click **Administration**, **Configuration**.
3. Click the link for CA Service Desk and edit each property with the appropriate value.
4. Click **Test**. If you do not receive a “Connection Test is Successful” message, modify your settings again.
5. Click the link for the CA Process Automation option.
6. Edit each property with the appropriate value, and then click **Test**.
   If you do not receive a “Connection Test is Successful” message, modify your settings again.
7. Click **Load** and select both check boxes that appear.



Load Configuration

8. Click **Load** button.
9. Click **Configure**, once the load completes.

Step 2 - Configure the pre-built CA Process Automation Workflows for CA Service Catalog

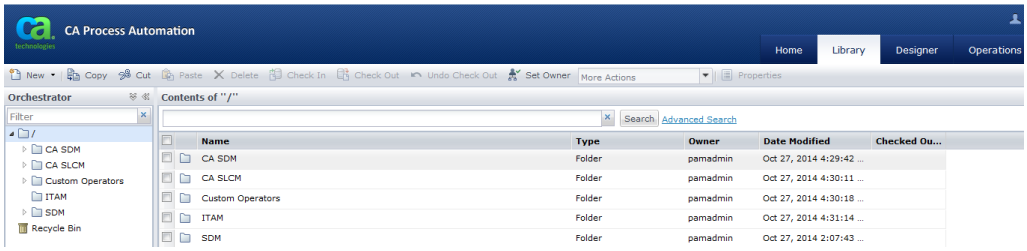
1. Log in to CA Service Catalog as the Service Delivery Administrator (spadmin).

2. Click **Administration**, **Configuration**.

3. Go to **CA Process Automation** section, and then click the **Launch** button to initiate CA Process Automation.

4. Enter the CA Process Automation Administrator username and password, and click **Log in**.

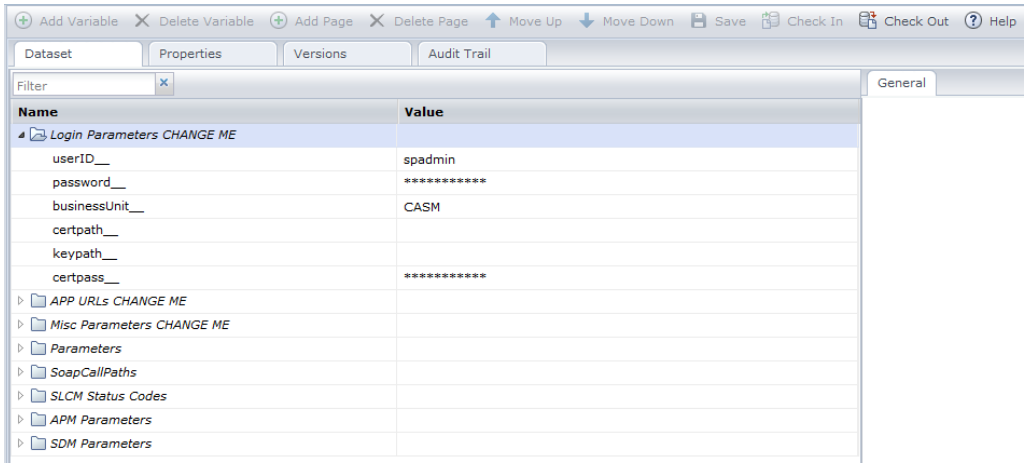
5. Click the **Library** tab.
   The following screen appears:



Library

6. Click the CA SLCM folder to open it.

7. Double-click SLCM_GlobalDataset.



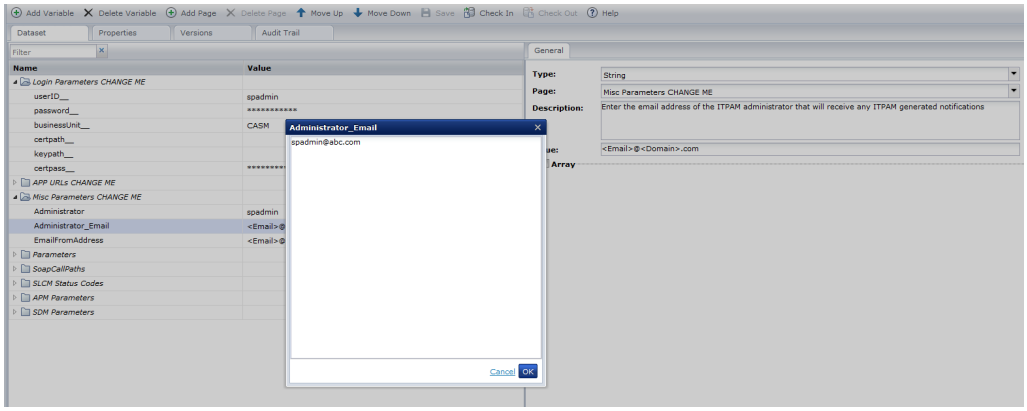
Login Parameters

8. Click the Checkout icon  in the SLCM_GlobalDataset screen.
   In the Login Parameters Value Definition screen, provide the Service Delivery Administrator user ID, password, and business Unit from the CA Service Catalog installation.

9. Click the CA SLCM folder to open it.

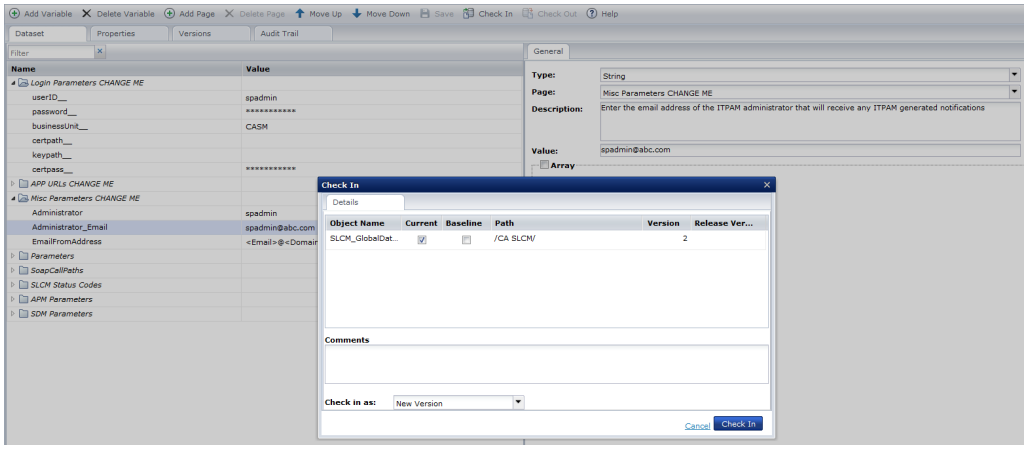
10. Double-click SLCM_GlobalDataset.

11. Click the Misc Parameters CHANGE ME section and modify the Administrator_Email and EmailFromAddress.



Misc Parameters

12. Click the **Save** icon, then click the **Check in** icon.
The following screen appears:



Check In Details

13. Enter any appropriate check-in comments and click OK.

14. Follow steps 4-8 for the SDM_GlobalDataset located in the CA SDM folder. Note that Administrator_Email and EmailFromAddress is located in the Parameters section.

15. Expand the CA SDM folder and click the SRF folder.

16. Right click the Service_Publishing Start Request Form and select Properties.

17. Click the **Tags** tab, then the **Edit** button.

18. Click in the text area and type chgcat then click **Save**.

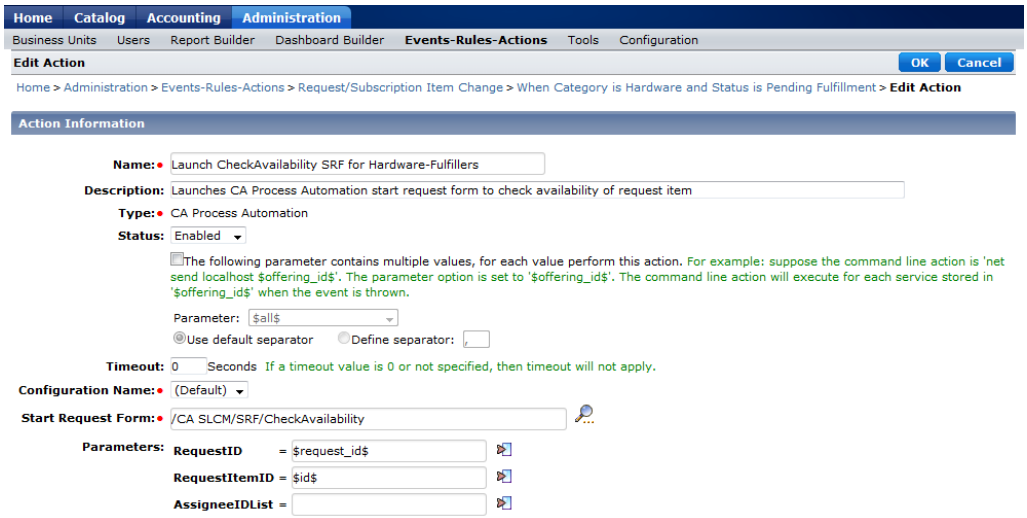
19. Follow steps 12-14 for the HWSW_FilledFromInventory Start Request Form.

20. Click the Configuration Browser tab
21. Click the Modules tab and double click the CA Service Desk Module.
22. Right-click and select Lock.
23. Update the Service Desk WebService URL, Service Desk Administrator User ID (ServiceDesk), and the Service Desk Administrator password. Click Apply.
24. Click the Modules tab again and double click the Alert Module.
25. Update the SMTP Server for Outgoing e-mail and the From Address for Outgoing e-mail. Click Apply.
26. Right-click and select Unlock. Click Ok to the confirmation popup.
27. Close CA Process Automation.

Step 3 - Copy and Modify Actions

Follow these steps:

1. Log into CA Service Catalog as an administrator.
2. Click **Administration**, **Events-Rules-Actions**.
3. Click **Request/Subscription Item Change**.
4. Click on the **When Category is Hardware and Status is Pending Fulfillment** rule.
5. Click the Copy icon for the **Launch CheckAvailability SRF for Hardware** action.
6. Type in the name **Launch CheckAvailability SRF for Hardware–Fulfillers Group** and click **OK**.
7. Check the action **Launch CheckAvailability SRF for Hardware** and click the Disable button.
8. Click the Edit icon for the **Launch CheckAvailability SRF for Hardware–Fulfillers Group** action.
9. Select Enabled from the **Status** drop-down box in the Action Information section.



Action Information

10. Type in Fulfillers in the text field for AssigneeIDList.
11. Click the **OK** button to save your changes.
12. Click the **Done** button.
13. Repeat Steps 1-12 for the all additional rules and actions.

Use the following table as a reference to add additional rules and actions:

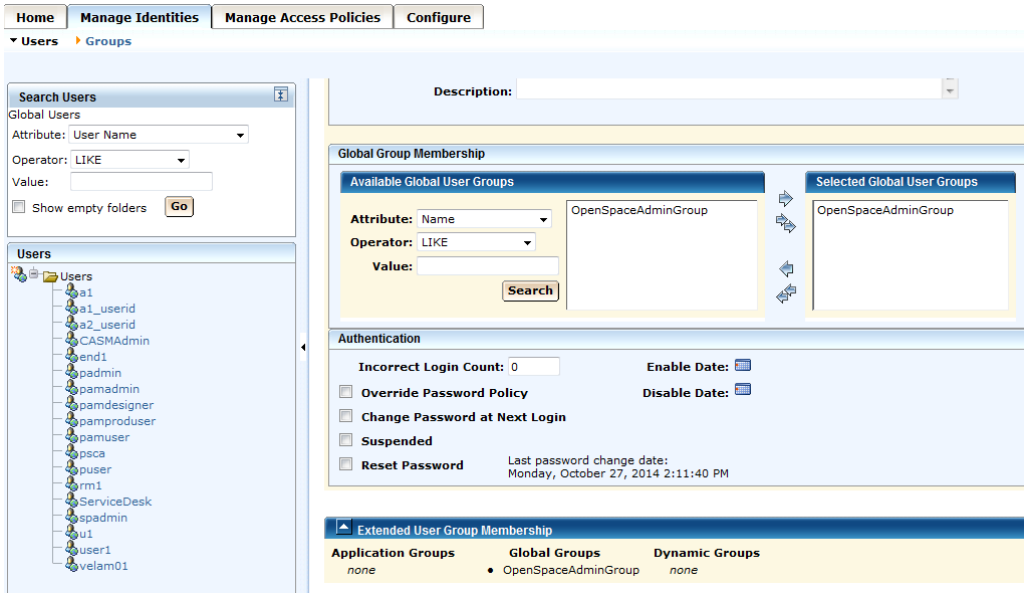
Rule Name	Action to Copy and Disable	New Enabled Action Name	How to Modify the Action
When Category is Software and Status is Pending Fulfillment	Launch CheckAvailability SRF for Software Availability	Launch CheckAvailability SRF for Software Availability–Fulfillers Group	AssigneeIDList = Fulfillers
When Category is Hardware and Status is Not Filled From Inventory	Launch SLCM_Fulfillment SRF	Launch SLCM_Fulfillment SRF–Procurement Group	AssigneeIDList = Procurement
When Category is Software and Status is Not Filled From Inventory	Launch SLCM_Fulfillment SRF	Launch SLCM_Fulfillment SRF–Procurement Group	AssigneeIDList = Procurement
When Category is Hardware and Status is Filled From Inventory	Launch HWSWFilledFromInv_SDM SRF	Launch HWSWFilledFromInv_SDM SRF–Change Analyst	AssigneeIDList = <SDM change analyst user id> SDM_Category = <tenanted category, ex. SLCM.HWFFI-A>
When Category is Software and Status is Filled From Inventory	Launch HWSWFilledFromInv_SDM SRF	Launch HWSWFilledFromInv_SDM SRF–Change Analyst	AssigneeIDList = <SDM change analyst user id>

Rule Name	Action to Copy and Disable	New Enabled Action Name	How to Modify the Action
			SDM_Category = <tenanted category, ex. SLCM.HWFFI-A>
When Category is Hardware and Status is Received or Order Cancelled	Launch Hardware CheckAvailability SRF	Launch Hardware CheckAvailability SRF–Fulfillers Group	AssigneeIDList = Fulfillers
When Category is Software and Status is Received or Order Cancelled	Launch CheckAvailability SRF for Software	Launch CheckAvailability SRF for Software–Fulfillers Group	AssigneeIDList = Fulfillers

Step 4 - Add Members to User Defined Group

Follow these steps:

1. Click **Manage Identities** tab, click the **Users** link in the CA EEM GUI.
2. Enter appropriate search criteria in the **Search Users** section, and click the Go button.
   Users appear in the Users section.
3. Select the user to add to the EEM group in the Users folder.
   The user details appear.
4. Search for the available global user groups in the Global Group Membership section.
5. Select the group(s) in the Global Group Membership section, to which the user must be added and move the selected groups into the **Selected Global User Groups** multi-select box.



Global Group Membership

6. Click **Save**.

7. Repeat steps 2 - 5 for each user that requires group membership.

Step 5 - Configure CA Service Desk Manager

Follow these steps to configure CA Service Desk Manager:

Step 5a - Configure Options Manager

You first configure the Options Manager in CA Service Desk Manager.

Follow these steps:

1. Log into the CA Service Desk Manager as a privileged user. For example, ServiceDesk

2. Click the **Administration** tab and navigate to **Options Manager**. Edit the following:

Sub Node	Options to Configure	Option Value / Action
CA Process Automation Workflow	caextwf_eem_hostname	CA EEM Server host name. Click Install.
	caextwf_endpoint	URL of the load balancer for the CA Process Automation server. Click Install.
	caextwf_log_categories	Enter **Process**. Click Install.
	caextwf_processdisplay_url	Replace <default hostname>: <port number> portion of the URL in the Option Value (in front of the "/itpam/JNLP") with the actual host name and port number of the load balancer for CA Process Automation server. Click Install.
	caextwf_worklist_url	Replace <default hostname>: <port number> portion of the URL in the Option Value (in front of the /itpam?webPage") with the actual host name and port number of the load balancer for CA Process Automation server. Click Install
	caextwf_ws_password	itpamadmin user's password in the Option Value field. Click Install.
	caextwf_ws_user	itpamadmin username in the Option Value field. Click Install.

Sub Node	Options to Configure	Option Value / Action
Change Order Manager	Category Defaults	Click Install.
Security	eiam_hostname	CA EEM Server host name. Click Install.
	Use_eiam_authentication	Click Install.

3. Close the CA Service Desk Manager GUI.
4. Restart the CA Service Desk Manager service.

Step 5b - Configure Web Screen Painter

You configure the Web Screen Painter now.

Follow these steps:

1. Open the Web Screen Painter and log in as a privileged user. For example, ServiceDesk
2. Open the Schema Designer and navigate to chg (Change Order).
3. Click **Add Column**.
4. Type usmrequestid in the pop up.
5. Click OK and set the Field Type to INTEGER.
6. Repeat steps 1-5 for usmrequestitemid, and then click the **Save** button.
7. Navigate to chgcat (Change Category).
8. Click **Add Column** and type implementors in the popup.
9. Click **OK** and set the Field Type to SREL. Then set the SRel Table to grp (Group Contacts).
10. Repeat steps 8 and 9 for change_manager.
11. Click Save and Publish. Then select **Yes** to the next 2 popups.
12. Stop the Service Desk services.
13. Run pdm_publish on the Service Desk server.
14. Start the Service Desk Manager services.
15. Open the Web Screen Painter and log in as a privileged user (e.g. ServiceDesk)

16. Click the **Open** icon.
17. Navigate to the detail_chgcat.htmpl file.
18. Click **Open**.
19. Right click the second row that has the field “Self-Service Include” and select Insert Row.
20. Right click the added row and select Insert Lookup.
21. Double-click the newly created field, click the Attribute row and select zchange_manager.
22. Repeat steps 20 and 21 for the Implementers field.
23. Click **File** and select **Save**.
24. Click **File** and select **Publish** and accept all confirmation popups.
25. Type pdm_webcache from a command prompt on the Service Desk server.

Step 5c - Add CA Service Desk Manager Groups

Use the following table to configure CA Service Desk Manager Groups:

Group Name	Group Manager	Group Members
Change Manager Group		*
IT Asset Management		*
Catalog Administrators		*

*Each group must contain at least one contact. Configure the contact as follows:

- Access type must be Analyst.
- Valid email address.
- Must exist in CA EEM.
- Belong to ITPAMUsers group within CA EEM.
- Select Email for all the Notification Methods.

Follow these steps to configure the CA Service Desk Manager Groups:

1. Open the CA Service Desk Manager and log in as a privileged user. For example, ServiceDesk
2. Click the **Administration** tab and navigate to **Security and Role Management**, **Groups**.
3. Click the **Create New** button.
4. Type Change Manager Group in the Group Name field.

5. Click the **Members** tab and click **Update Members** to add users to this group.
6. Repeat steps 3-5 for each group in the table above.

Step 5d - Add Status

Follow these steps:

1. Open CA Service Desk Manager and log in as a privileged user. For example, ServiceDesk
2. Click the **Administration** tab and navigate to **Service Desk**, **Change Orders**, **Status**.
3. Click the **Create New** button.
4. Type Complete in the Symbol field.
5. Type COMP in the Code field.
6. Click the **Save** button.
7. Click the **Update Transitions** button and check the following Statuses:
   - Cancelled
   - Closed
   - Customer Hold
   - Implementation in progress
   - Vendor Hold
   - Verification in progress
8. Click **Save**.

Step 5e - Add Change Categories

Use the following table to configure CA Service Desk Manager Change Categories:

Symbol	Code	Groups	Workflow SRF
SLCM.Hardware Filled From Inventory	SLCM. HWFFI	**Group**: IT Asset Manager	HWSW_FilledFromInventory
SLCM.Software Filled From Inventory	SLCM. SWFFI	**Group**: IT Asset Manager	HWSW_FilledFromInventory
SLCM.Service Publishing	SLCM. CN0	**Group**: IT Asset Manager **Change Manager**: Change Manager Group **Implementers**: Catalog Administrators	Service_Publishing

Follow these steps:

1. Open the CA Service Desk Manager and log in as a privileged user. For example, ServiceDesk
2. Click the **Administration** tab and navigate to **Service Desk**, **Change Orders**, **Categories**.
3. Click the **Create New** button.
4. Type SLCM.Hardware Filled From Inventory in the Symbol field.
5. Type SLCM.HWFFI in the Code field.
6. Select IT Asset Manager in the Group field.
7. Click the 2. Workflow tab.
8. Click the **Use CA IT PAM** button.
9. Choose **HWSW_FilledFromInventory Start Request** Form.
10. Click the **Save** button.
11. Repeat steps 3-10 for each change category in the table above.

Third-Party License Acknowledgments

This section contains all third-party software license agreements for applications that are included as part of the current release of CA Service Management. All third-party software has been used in accordance with the terms and conditions for use, reproduction, and distribution as defined by the applicable license agreements.

The following license agreements are available as an attachment:

Component	TPSR ID
.NET Framework 4.5	00001055_2
apache commons csv 1.1	00001327_2
BSAFE Crypto-J 3.6	P02258_1
Commons Cli 1.1	P05003_10
Commons Cli 1.2	05819_6
Commons Codec 1.4	08051_2
Commons Codec 1.9	13073_20
Commons IO 2.4	11999_1
Commons Lang 2.6	00000379_47
Commons Logging 1.1.1	11958_25
ESAPI 2.1.0	11353_42
iText 2.1.7	00001327_28

jackson 2.5.0	00001164_2
jackson-core 2.5.4	00001327_11
jackson-databind 2.5.4	00000773_8
jackson-dataformat-xml 2.5.4	00001327_10
jackson-module-jaxb-annotations 2.5.4	00000717_42
JNA 3.3.0	00001092_70
JDBC 11.2.0.3	0378_1
Log4j 1.2.15	P02272_7
Log4j 2.3	00001182_17
Oracle Java Runtime Environment (JRE) 1.8.0_45	12130_12
ODP.NET 12.1.22	1055_1
Stax2-api 3.1.4	00001327_15
SQL Server JDBC Driver 4.1	00001182_20
7Zip 9.2	00001327_26

Click here to download the license agreements.

CA SDM Connector Glossary

The following list contains concepts and terms that are useful if you are integrating a CA Catalyst Connector with CA Catalyst.

- **Connectors**
  Connectors are the links from products that consume data from external products, referred to in this document as domain managers. Each connector retrieves information from its domain manager and transmits the information through the connector framework to the consuming product for visualization and analysis. Connectors can also enact inbound operations on data in the source domain manager, such as object creation.

- **USM**
  The *Unified Service Model* (USM) is a schema of common object types and properties to which data from all connectors is converted. The USM schema enables data analysis from all domain managers on a common interface with identical formatting.

- **Configuration Items (CIs)**
  Configuration items (CIs) represent IT elements that the domain manager manages. Each CI belongs to a *type* (defined in the USM schema) such as ComputerSystem, Database, Process, BinaryRelationship, and so on.
  Connectors transform managed objects from domain managers to adhere to the USM schema and import the objects to the consuming products as CIs.

- **Services**
  Services represent discrete business functions that can contain configuration items that multiple domain managers manage. For example, a payroll service contains an Active Directory database managed by which the Microsoft SCOM manages, user store manages by security product, batch

jobs managed by mainframe product, router managed by network product, applications managed by application management product, and so on. You can do the following actions in consuming products, such as CA SOI:

- Detect the root cause of service degradation quickly and navigate to the appropriate product to resolve problems
- Model services based on imported CIs or import existing service models from integrated products to construct a comprehensive and service-centric model of your enterprise

- **Alerts**
  Alerts are the CA SOI mechanism for reporting fault conditions and service degradation. *Infrastructure alerts* are fault conditions originally reported by one of the domain managers (such as a CA NSM event or CA Spectrum alarm). An alert is associated with a corresponding CI and associated alert severities determine CI condition, and ultimately, service impact. *Service alerts* are conditions generated by CA Spectrum SA based on analysis of a modeled service. Service alerts result when the condition of one or more CIs combines to impact the overall quality or risk level associated with the service.

- **Outbound from connector operations**
  Outbound from connector operations are operations that a connector invokes to import data from domain managers into consuming products such as CA Catalyst and CA Spectrum SA. All connectors support outbound operations.

- **Inbound to connector operations**
  Inbound to connector operations invoke changes to the domain manager data store as a result of changes to the imported data in the consuming product. For example, CI reconciliation in CA Catalyst can change the values of CI properties. Connectors that support inbound operations can then enact that change in the source domain manager so that its data matches the reconciled data. Or if a CI is deleted in a domain manager that CA Catalyst defines as a source of truth, connectors that support inbound operations can delete the CI in other domain managers with a record of that CI.

- **ServiceDeskManagerConnector.conf**
  ServiceDeskManagerConnector.conf file is the configuration file for CA Catalyst Container r3.1 and r3.2. This file stores the configuration information (node and module information) needed for the CA Catalyst server and other peers. CA SDM Connector r2.5 framework does not have the ServiceDeskManagerConnector.conf file.

- **ServiceDeskManagerConnector.xml**
  ServiceDeskManagerConnector.xml is the configuration file for CA SDM Connector r3.1 and r3.2. For CA SDM Connector r2.5, the equivalent configuration file is ServiceDeskManager_<ComputerName>.xml where ComputerName is the name of the computer server where the CA SDM Connector resides. These files contain the configuration properties to help the connector operations. For example, toggling the Use Transaction Work Area, changing the configured username and password, excluding CI or relationship types, and so on.

- **USM-CMDB.xml**
  USM-CMDB.xml file contains the mapping information of the USM entities and CMDB families. Based upon this mapping the CA SDM Connector performs necessary actions.
  Example: The ServiceDeskObject.xml object lists the attributes to query while querying the CIs from CMDB. This information helps the CA SDM Connector to query CMDB with only those attributes which are mapped to USM attributes rather than querying all the attributes.

- **ServiceDeskManager_policy.xml**
  ServiceDeskManager_policy.xml file contains the outbound USM transformation policy information which transforms the incoming CIs from CMDB to USM entity.

- **ServiceDeskManager_policy.en**
  ServiceDeskManager_policy.en is the localization file for outbound policy. Change this file information to map with new values of CMDB families or attributes if you want to support CA SDM in a language other than English.

- **ServiceDeskManager_policySB.xml**
  ServiceDeskManager_policySB.xml file contains the inbound transformation policy information which transforms the incoming USM entity to CMDB CI before providing it to the CA SDM Connector.

- **ServiceDeskManager_policySB.en**
  ServiceDeskManager_policySB.en is the localization file for inbound policy. Change this file information to map with new values of CMDB families or attributes if you want to support CA SDM in a language other than English.