

CA TECHNOLOGIES GREEN BOOKS

# CA Service Desk Manager Integrations

Integration Best Practices

Volume 3

- CA ASSET PORTFOLIO MANAGEMENT
- CA CLIENT AUTOMATION
- CA PATCH MANAGER
- CA CONFIGURATION AUTOMATION
- CA ECOMETER
- CA NETWORK AND SYSTEMS MANAGEMENT
- CA SPECTRUM



## LEGAL NOTICE

This publication is based on current information and resource allocations as of its date of publication and is subject to change or withdrawal by CA at any time without notice. The information in this publication could include typographical errors or technical inaccuracies. CA may make modifications to any CA product, software program, method or procedure described in this publication at any time without notice.

Any reference in this publication to non-CA products and non-CA websites are provided for convenience only and shall not serve as CA's endorsement of such products or websites. Your use of such products, websites, and any information regarding such products or any materials provided with such products or at such websites shall be at your own risk.

Notwithstanding anything in this publication to the contrary, this publication shall not (i) constitute product documentation or specifications under any existing or future written license agreement or services agreement relating to any CA software product, or be subject to any warranty set forth in any such written agreement; (ii) serve to affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (iii) serve to amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this publication remain at CA's sole discretion.

The information in this publication is based upon CA's experiences with the referenced software products in a variety of development and customer environments. Past performance of the software products in such development and customer environments is not indicative of the future performance of such software products in identical, similar or different environments. CA does not warrant that the software products will operate as specifically set forth in this publication. CA will support only the referenced products in accordance with (i) the documentation and specifications provided with the referenced product, and (ii) CA's then-current maintenance and support policy for the referenced product.

Certain information in this publication may outline CA's general product direction. All information in this publication is for your informational purposes only and may not be incorporated into any contract. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "AS IS" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, lost investment, business interruption, goodwill or lost data, even if CA is expressly advised of the possibility of such damages.

### **COPYRIGHT LICENSE AND NOTICE:**

This publication may contain sample application programming code and/or language which illustrate programming techniques on various operating systems. Notwithstanding anything to the contrary contained in this publication, such sample code does not constitute licensed products or software under any CA license or services agreement. You may copy, modify and use this sample code for the purposes of performing the installation methods and routines described in this document. These samples have not been tested. CA does not make, and you may not rely on, any promise, express or implied, of reliability, serviceability or function of the sample code.

Copyright © 2012 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. Microsoft product screen shots reprinted with permission from Microsoft Corporation.

### **TITLE AND PUBLICATION DATE:**

*CA Service Desk Manager Integrations Green Book*  
Publication Date: September 24, 2012

# ACKNOWLEDGEMENTS

## Principal Authors

Tyson Bell

Amy Chenard

Richard Lankester

Reddy Mamidi

Raghu Rudraraju

Kirk O'Quinn

Richard Schneider

Steve Troy

Shawn Walsh

The principal authors and CA Technologies would like to thank the following contributors:

Gladys Beltran

Joseph Cabral

Kim Rasmussen

Barry Stern

Ramprasad Suthi

Malcolm Ryder

Neeraja Thota

David Vaughn

CA Technologies Support

## Third-Party Acknowledgements

Microsoft product screens reprinted with permission from Microsoft Corporation. Microsoft, SQL Server, and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Pentaho is a registered trademark of Pentaho Corporation.

## CA TECHNOLOGIES PRODUCT REFERENCES

This document references the following CA Technologies products:

- CA Application Performance Management
- CA Asset Portfolio Management (included with the CA IT Asset Manager solution)
- CA Business Intelligence
- CA Business Service Insight (CA BSI) – formerly known as CA Oblicore Guarantee™
- CA Clarity™ Project and Portfolio Manager (CA Clarity PPM)
- CA Configuration Automation – formerly known as CA Cohesion Application Configuration Manager (CA Cohesion ACM)
- CA Customer Experience Manager (CA CEM)
- CA ecoMeter
- CA Embedded Entitlements Manager (CA EEM)
- CA eHealth® (CA eHealth)
- CA Identity Manager
- CA Introscope
- CA IT Client Automation Manager (CA ITCM)
- CA Client Automation (includes CA IT Client Manager product)
- CA Management Database (CA MDB)
- CA Network and Systems Management (CA NSM)
- CA Process Automation (formerly CA IT Process Automation Manager, CA IT PAM)
- CA Role and Compliance Manager (CA RCM)
- CA Service Catalog (which includes CA Service Accounting)
- CA Service Desk Manager (CA SDM)
- CA Service Operations Insight (CA SOI)
- CA SiteMinder® (CA SiteMinder)
- CA Software Change Manager (CA SCM)

- CA Spectrum® (CA Spectrum)
- CA Service Operations Insight (CA SOI)
- CA Workflow

## FEEDBACK

Please email us at [greenbooks@ca.com](mailto:greenbooks@ca.com) to share your feedback on this publication. Please include the title of this publication in the subject of your email response. For technical assistance with a CA Technologies product, please contact CA Support at <http://ca.com/support>. For assistance with support specific to Japanese operating systems, please contact CA Technologies at <http://www.casupport.jp>.



# Contents

<b>Chapter 1: Introduction</b>	<b>11</b>
Who Should Read This Book .....	13
<b>Chapter 2: ITIL® V3 Service Lifecycle Support</b>	<b>15</b>
Service Strategy.....	15
Demand Management .....	15
Financial Management .....	16
Service Portfolio Management.....	17
Service Strategy.....	18
Service Design .....	19
Availability Management .....	19
Capacity Management .....	20
Information Security Management .....	22
IT Service Continuity Management .....	23
Service Catalog Management.....	24
Service Level Management .....	25
Supplier Management.....	26
Service Transition.....	27
Change Management .....	27
Evaluation.....	28
Knowledge Management .....	28
Release and Deployment Management .....	29
Service Asset and Configuration Management .....	30
Service Validation and Testing .....	32
Transition Planning and Support .....	33
Service Operation.....	34
Access Management .....	34
Event Management.....	34
Incident Management .....	35
Problem Management .....	36
Request Fulfillment .....	37
Continual Service Improvement.....	38
Seven-Step Improvement Process.....	38
<b>Chapter 3: CA Asset Portfolio Management</b>	<b>41</b>
CA Asset Portfolio Management Integration .....	41
What is CA Asset Portfolio Management .....	41
Integration Details.....	41
Integration Value.....	42
Integration Points Between CA APM and CA SDM .....	42
Configuring the Integration Between CA APM and CA SDM .....	43
Share Extended Fields Between CA APM and CA SDM.....	45
Launch CA APM in Context From CA SDM.....	59
Launch CA SDM in Context from CA APM .....	60

Including CA Service Catalog in the Solution .....	60
<b>Chapter 4: CA Client Automation Manager</b> .....	<b>61</b>
What is CA Client Automation Manager .....	61
Asset Management Functionality .....	62
Software Delivery Functionality .....	64
OS Installation Management .....	65
Remote Control Functionality .....	65
Windows New Desktop Migration .....	66
Path Research Management .....	67
Integration Details .....	69
Integration Points from CA Client Automation to CA SDM .....	70
Integration Points from CA SDM to CA Client Automation .....	70
Integration Points from CA Client Automation to CA SDM .....	70
Integration Value .....	71
How the Integration Works .....	72
Integration Scenario .....	73
Business Challenge.....	73
How the Integration with CA Client Automation Helps Overcome the Challenge.....	73
Configuring the Integration from CA SDM r12.6.....	74
Configure the Integration from CA Client Automation R12.5 .....	77
Testing the Integration .....	81
Integration Summary.....	85
<b>Chapter 5: CA Patch Manager</b> .....	<b>87</b>
CA Patch Manager Integration .....	87
Integration Details .....	87
Integration Points from CA SDM to CA Patch Manager .....	87
Integration Points from CA Patch Manager to CA SDM .....	87
Integration Value .....	88
How the Integration Works .....	88
Integration Example .....	89
Business Challenge.....	89
CA Approach .....	89
Configuring a Solution.....	90
Testing the Integration .....	97
Integration Summary.....	99
<b>Chapter 6: CA Configuration Automation</b> .....	<b>101</b>
CA Configuration Automation Integration.....	101
What is CA Configuration Automation.....	101
Integration Details .....	103
Integration Points and Functionality from CA SDM .....	103
Integration Points and Functionality from CA Configuration Automation.....	103
How the Integration Works .....	104
Prerequisites for Integration.....	105
Configure the Integration from CA SDM .....	106
Configure the Integration from CA Configuration Automation .....	109

Reconciling CIs to Avoid Duplicates .....	120
Reconciliation Approaches .....	121
Configure SSL Communication for CA Configuration Automation .....	128
Create Certificate .....	128
Add Certificate to Java Trusted Key Store .....	129
Pass the URL to GRLoader .....	129
Tips for Modifying the CMDB Attribute Mapping .....	130
Remove Model Attributes .....	131
Removing Redundant Software CIs .....	132
Tips for Modifying the CMDB Class Mapping .....	135
Reconciling Managed Hardware across Multiple Domains .....	137
Reconcile Discovered Servers .....	139
Reconcile Relationships .....	143
Integration Summary .....	146
<b>Chapter 7: CA ecoMeter</b> .....	<b>147</b>
CA ecoMeter Integration .....	147
What is CA ecoMeter .....	147
Integration Details .....	148
Integration Points and Functionality from CA SDM .....	148
Integration Points and Functionality from CA ecoMeter .....	148
Integration Value .....	148
Integration Example .....	149
Configure the Integration from CA SDM .....	149
Configure the Integration from CA ecoMeter .....	150
Testing the Integration .....	156
Troubleshooting the Integration .....	157
Integration Summary .....	157
<b>Chapter 8: CA NSM</b> .....	<b>159</b>
Integration Example- Service Desk and NSM .....	159
Business Challenges .....	159
CA Approach .....	159
Configuring a Solution .....	160
Best Practices .....	160
Configuring Alert Management to Work with Service Desk Example .....	161
Configuring MCC (Management Command Center) to Integrate with Service Desk Example .....	167
Testing Service Desk - NSM Integration .....	167
Testing Automatic Incident Creation .....	168
End-User Interactive Actions from Management Command Center .....	170
End-User Interactive Actions from 2D Map .....	174
Miscellaneous Integrations .....	175
Service Desk - NSM Integration Summary .....	180
<b>Chapter 9: CA Spectrum Infrastructure Manager Integrations</b> .....	<b>183</b>
Overview .....	183
CA Spectrum Infrastructure Manager Integration .....	184
Integration Points and Value .....	185

Integration Preparation .....	186
Use Fully Qualified Domain Names(FQDN) .....	187
Define Services in CA Spectrum IM .....	187
How the Integration Works .....	188
Prerequisites for Integration .....	190
Installation Documentation .....	191
Export and Import Options .....	192
Modify the CMDB Resource Mapping File .....	193
Configure CA SDM for the Integration .....	194
Define the CA Spectrum MDR .....	195
Use GRLoader to Copy Data from Remote MDRs .....	197
CI Import Notes .....	198
Troubleshooting .....	198
Introducing CA Service Operations Insight into the Solution .....	199
Integration Points and Value .....	200
CA SOI Integration Details .....	200
Prerequisites for Integration .....	201
Installation Documentation .....	201
CA Event Integration .....	202
Import Services to CA SOI .....	208
Introducing eHealth into the Solution .....	209
What is eHealth .....	209
Integration Value .....	209
Configuring the Integration .....	209
Introducing CA Application Performance Management into the Environment .....	210
What is CA Application Performance Management .....	210
Integration Value .....	210
Single Sign ON with CA Embedded Entitlements Manager .....	211
Summary .....	212

# Chapter 1: Introduction

The *CA Service Desk Manager Integration Best Practices Green Book* is comprised of three volumes. Each volume describes ways to improve the process maturity for various ITIL® processes when CA Service Desk Manager (CA SDM) 12.6 is integrated with other CA Technologies solutions. The following ITIL V3 IT Service Management processes are covered in this Green Book:

- Access Management
- Availability Management
- Capacity Management
- Change Management
- Continual Service Improvement
- Demand Management
- Evaluation
- Event Management
- Financial Management
- Incident Management
- Information Security Management
- IT Service Continuity Management
- Knowledge Management
- Problem Management
- Release and Deployment Management
- Request Fulfillment
- Service Asset and Configuration Management
- Service Catalog Management

- Service Level Management
- Service Portfolio Management
- Service Validation and Testing
- Supplier Management
- Transition Planning and Support

Chapter 2 highlights the key objectives and recommended product and solution integrations for each ITIL process. These integrations can help achieve and mature the process goals. Additional products are available that also add value to the ITIL processes. However, Chapter 2 discusses the product-to-process mappings for the product integrations that are described in this Green Book.

The remaining chapters in each volume describe how to integrate additional CA Technologies solutions with CA SDM. The integrations can help extend the capability of CA SDM and enhance the management and coordination of service management business processes. This Green Book uses a layered approach to technical integrations by starting with a point-to-point integration with CA SDM. This Green Book then includes instructions or recommendations for introducing one or more additional product solutions into the existing integration.

The following information is provided for each product integration:

- An overview that describes the benefits of the integration.
- Recommended best practices for the integration.
- Steps to set up, configure, test, and troubleshoot the integration.
- Steps to introduce additional solutions into the environment, if applicable.

The CA SDM integrations that are explained in this Green Book are divided into the following volumes:

- Volume 1
  - CA Service Catalog
  - CA Clarity™ Project and Portfolio Manager (CA Clarity PPM)
  - CA Business Service Insight (CA BSI)
  - CA Identity Manager
  - CA SiteMinder®

- Volume 2
  - CA Integration Platform
  - CA Process Automation
- Volume 3
  - CA Asset Portfolio Management
  - CA IT Client Manager
  - CA Patch Manager
  - CA Cohesion Application Configuration Manager (CA Configuration Automation)
  - CA ecoMeter
  - CA NSM
  - CA SOI

All three volumes include the following chapters:

- Introduction
- ITIL V3 Service Lifecycle Support

**Important!** Some of the product features and functions listed in this Green Book are not described in CA Technologies product documentation and CA Technical Support does not support them. While the integrations described have been tested in a limited test environment, these integrations are not fully supported. We recommend that you test the integrations carefully in a test environment before going into production.

## Who Should Read This Book

---

This Green Book provides the following types of users with the information necessary to integrate CA SDM with various CA Technologies solutions:

- Support technician
- Software architect

## Who Should Read This Book

- Software developer
- Software engineer
- System administrator

This Green Book is intended for highly technical users who have an advanced knowledge of CA SDM and require integration capabilities to configure and maintain their CA SDM environment successfully.

# Chapter 2: ITIL® V3 Service Lifecycle Support

CA Technologies integrated solutions support and align with the 24 processes and 4 functions in the Service Lifecycle of ITIL V3. This chapter lists the objectives for each process and the technologies that support them.

## Service Strategy

---

### Demand Management

#### Objectives

- Influence user and customer demand of IT services.
- Manage the impact on IT resources.
- Develop and maintain service packages and service level packages that are based on patterns of business activity.

#### How CA Technologies Solutions Help Meet the Objectives for Demand Management

The following process describes how CA eHealth, CA Clarity PPM, CA Service Catalog, and CA SDM integrate to help improve the Demand Management process:

1. CA eHealth provides a service provider with the metrics that can be used to model service demand. CA eHealth metrics can be tied to CA Service Catalog service offerings to enable reporting back to the customers on how their services are used. The reporting also identifies the costs that are associated with providing the service at the given demand.
2. When CA eHealth and CA Service Catalog are integrated with the CMDB component of CA SDM, the relationship between the services and their supporting infrastructure can be analyzed graphically with the CMDB Visualizer for actual and anticipated demand.
3. As improvements or details of a new service are defined, the Demand Manager documents the details in the service package of the portfolio within CA Clarity PPM.
4. As updates are approved, CA Clarity PPM creates requests for change (RFCs) in CA SDM to update the CA eHealth monitoring profiles and CA Service Catalog with changes to the service and its costs.

5. CA BSI integrates, at a service view, CA eHealth, CA Clarity PPM, CA Service Catalog, and CA SDM to enable a Demand Manager to review existing and anticipated patterns of business activity for the business.

### Other CA Technologies Products that Facilitate the Demand Management Process

Demand Management is also facilitated in other CA Technologies solutions.

- CA ecoMeter automates delivering green service and reports on green IT effectiveness. The reports from CA ecoMeter help IT to convey the savings of having well-defined demand back to the business.
- CA SOI provides infrastructure that is based on demand. Specific service level packages are modeled in CA SOI. Modeling in CA SOI helps simplify the deployment of the infrastructure that is based on demand. A Demand Manager can use the metrics that CA SOI gathers to model future service packages.
- CA SDM provides statistics of incident and change requests to understand customer patterns of business activity better.

### Financial Management

#### Objectives

- Quantify the value of IT services and their underlying assets by managing IT budgeting, accounting, and charging.

#### How CA Technologies Solutions Help Meet the Objectives for Financial Management

The following process describes how CA Asset Portfolio Management, CA Clarity PPM, CA Service Catalog, and CA SDM integrate to help improve the Financial Management process:

1. CA Clarity PPM helps a service provider manage the project and asset costs and evaluate how the services are budgeted and charged to the customer.
2. The integration of CA Clarity PPM with CA Service Catalog helps in managing finances efficiently. The accounting capabilities of CA Service Catalog provide the metrics useful to an IT Financial Manager. The IT Financial manager uses them to model which services are cost-effective, and to identify ways of gaining efficiencies in those services.

3. CA Clarity PPM provides the accounting capabilities of CA Service Catalog with up-to-date costs and services that a customer can request.
4. Each individual asset that is requested through the catalog is tracked through CA SDM as either a request or, if needed, a change order.
5. CA Asset Portfolio Management provides the cost of the assets, contracts, and vendor information. When CA Asset Portfolio Management is integrated with CA Service Catalog, a user sees currently available assets. An asset can be a configuration item (CI), an asset which is associated with a user, or both a CI and a user asset. If an asset is also a CI, the asset is managed under the full Change Process.
6. CA Asset Portfolio Management integrates into the Enterprise Resource Planning (ERP) solution of the service provider, strengthening the IT alignment to business budgeting, accounting, and charging.
7. CA Asset Portfolio Management provides details to CA Clarity PPM to enable up-to-date IT financial management decisions for services.

## Service Portfolio Management

### Objectives

- Provide a dynamic method for governing investments in service management across the enterprise and managing them for value.
- Define, analyze, approve, and offer services.

### How CA Technologies Solutions Help Meet the Objectives for Service Portfolio Management

The following process describes how CA Clarity PPM, CA Service Catalog, and CA SDM integrate to help improve the Service Portfolio Management process:

1. CA Technologies has an industry-leading Project and Portfolio Management solution, CA Clarity PPM. Native integration to other solutions such as CA SDM and CA Service Catalog provide three-direction feeds that provide current, planned, and historical data about how services are used.
2. When CA Clarity PPM receives request volumes from CA Service Catalog, CA Clarity PPM can track the frequency of a service is currently being requested, compared to the long-term usage of the service.

3. Incident and problem ticket volumes from CA SDM, together with relationships in the CA SDM CMDB component, enable analysis of how effectively a service delivers on its commitments.
4. The Portfolio Manager uses CA Clarity PPM to analyze all aspects of providing the service to justify further investment.
5. In CA Clarity PPM, the approval process is modeled in a way which allows the workflow and decision tree to retain, replace, rationalize, refactor, renew, or retire a service can be documented, assessed, and ultimately approved.
6. Most importantly, the integration helps ensure continuous improvement to the service without the need to recompile data that is natively integrated.
7. CA BSI provides the Service Level Management understanding that supports the Service Portfolio. CA BSI also helps ensure that the Service Level Agreements (SLAs), Operational Level Agreements (OLAs), and Underpinning Contracts (UCs) are being managed properly.

### Service Strategy

Define the best possible value that a service can create for a customer through analysis of competition, market space, asset use, and business capabilities.

### How CA Technologies Solutions Help Meet the Objectives for Service Strategy

The following process describes how CA Clarity PPM and CA SDM integrate to help improve the Service Strategy process:

1. CA Clarity PPM analyzes the key attributes with a number of scenarios such as comparisons over time, costing models, resource use, and others.
2. When CA Clarity PPM is integrated with CA SDM, detailed attributes of the CIs, organizations, resources, service use, and ties to other services are added to the analysis within the CMDB Visualizer.
3. With the solutions integrated, CA Clarity PPM and CA SDM provide the ability to analyze which combinations of investments provide the most benefit to the business.

## Service Design

---

### Availability Management

#### Objectives

- Produce and maintain an availability plan that reflects the current and future needs of the business.
- Provide advice and guidance on all availability-related issues.
- Help ensure that service availability achievements meet or exceed all their agreed targets by managing the performance of services and resource-related availability.
- Assist with the diagnosis and resolution of availability-related incidents and problems.
- Assess the impact of all changes on the availability plan and the performance and capacity of all services and resources.
- Help ensure that proactive measures to improve the availability of services are implemented, if the measures are cost-justifiable.

#### How CA Technologies Solutions Help Meet the Objectives for Availability Management

The following process describes how CA eHealth, CA CEM, CA NSM, CA Spectrum, and CA SDM integrate to help improve the Availability Management process:

1. CA CEM allows for real-time and historical views of the customer experience of the service, such as web page generation and data retrieval.
2. CA Introscope gathers back-end to front-end application performance metrics.
3. CA NSM provides agent level metrics on the operating system, database, and applications.
4. CA Spectrum provides the heuristic measurements of the network and system availability.
5. These four solutions provide details that are sent to CA eHealth for the baseline and real-time availability of the IT infrastructure.
6. The modeling of the infrastructure is maintained in the CMDB component of CA SDM. The CIs the infrastructure solutions manage are imported into the CMDB component, which is associated to a Management Database Repository (MDR), and visualized at a service layer.

7. Incident metrics are automatically created from the tools and manually created from customers and are added to the analysis within CA SDM.
8. The availability plans are documented as knowledge documents in the knowledge management function of CA SDM. Knowledge management has a flexible document lifecycle, which helps ensure that updates to the availability plan are properly managed.

### Other CA Technologies Products that Facilitate Availability Management

Other CA Technologies solutions also facilitate Availability Management. The solutions are added to the Availability Manager planning tools.

- CA BSI automates, activates, and accelerates the management, monitoring, and reporting of business and technology Service Level Agreements (SLAs) and service delivery agreements for enterprises and service providers.
- CA SOI gives a model-based view of critical application monitoring data. CA SOI pulls all the data from domain management systems, such as CA Application Performance Management, CA Spectrum, and CA eHealth, and presents it in a single view to end users. CA SOI provides service impact analysis, service visualization, and integration to service management through CA SDM.
- CA Patch Manager lists computers that are not patched, which enables Availability Management to identify potential threats to availability.

**Note:** CA Patch Manager uses the infrastructure and resources of the CA IT Client Manager solution.

### Capacity Management

#### Objectives

- Produce and maintain an up-to-date capacity plan, which reflects the current and future business needs.
- Provide advice and guidance to all business and IT departments on all issues that are related to capacity and performance.
- Help ensure that service performance achievements meet or exceed all of their agreed performance targets.
- Assess the impact of all changes on the capacity plan, and the performance and capacity of all services and resources.

## How CA Technologies Solutions Help Meet the Objectives for Capacity Management

Capacity Management relies on metrics from the infrastructure to plan, advise, and react to capacity needs. The metrics are used to analyze historical, current, and future availability through visualization, alerting, and reporting. CA Technologies solutions gather the metrics about a service provider infrastructure and add an integrated management layer to support mature Capacity Management.

1. CA CEM allows for real-time and historical views of the customer experience of the service, such as web page generation and data retrieval.
2. CA Introscope gathers back-end to front-end application performance metrics.
3. CA NSM provides agent-level metrics on the operating system, database, and applications.
4. CA Spectrum provides the heuristic measurements of the network and system availability.
5. These four solutions provide details that are fed to CA eHealth for baseline and real-time capacity of the IT infrastructure.
6. Final service modeling of the infrastructure is maintained in the CMDB component of CA SDM. The CIs that the infrastructure solutions manage, are imported into the CA SDM CMDB component. These components are associated to a Management Database Repository (MDR) and visualized at a service layer.
7. Incident metrics are automatically created from the tools or from customers and are added to the analysis within CA SDM.
8. The Capacity Plans are documented as knowledge documents in the knowledge management function of CA SDM. Knowledge management has a flexible document lifecycle to help ensure that updates to the plan are properly managed.

## Other CA Technologies Products that Facilitate Capacity Management

Other CA Technologies solutions also facilitate Capacity Management. These solutions are added to the Capacity Manager planning tools.

- CA BSI automates, activates, and accelerates the management, monitoring, and reporting of business and technology SLAs in addition to service delivery agreements for enterprises and service providers.
- CA SOI gives a model-based view of critical application monitoring data. CA SOI pulls all the data from domain management systems, such as CA Application Performance Management, CA Spectrum, and CA eHealth, and presents it in a single view to end users. CA SOI provides service impact analysis, service visualization, and integration to service management through CA SDM.
- CA Client Automation and CA Server Automation provide alerts and automated actions on desktops and servers that are running low on disk space. CA Client Automation provides a set of cross-platform product capabilities for Windows, Linux, UNIX, and MAC environments. While CA IT Client Manager was previously sold as a standalone product, it is now included as part of the CA Client Automation and also as part of CA Server Automation solutions. CA Client Automation has focus on managing end-user devices such as desktops, laptops, and end-point devices; while CA Server Automation has focus on managing servers. This document refers to the functionality of the CA Client Automation product capabilities.

## Information Security Management

### Objectives

- Help ensure availability, confidentiality, and integrity of data, systems, and the environments that contain them.
- Communicate, implement, and enforce the Information Security Policy.

### How CA Technologies Solutions Help Meet the Objectives for Information Security Management

1. CA Technologies IT Security Solutions manage the full scope of Information Security Management as it relates to implementing, evaluating, maintaining, and controlling access, identities, and information.
2. The Service Management solutions leverage and integrate with CA Technologies IT Security Solution enabling a service provider to plan and design an Information Security Policy.

3. CA SDM tracks security incidents, assets and locations, SLAs, UCs, and OLAs that are used to plan the security policy.
4. Information Security is published as a knowledge document in the CA SDM knowledge management feature. An enforced review cycle maintains the Information Security.
5. The service management solution supports implementation, evaluation, maintenance, and control through its technology stack. For example, CA EEM, a component within the IT Security Solutions, is a core component of the Service Management solution enabling service providers a central repository of service management application users. This solution is integrated using LDAP and provides access to features and data within the Service Management suite. This integration supports password reset through the CA SDM end-user self-service interface.
6. CA Client Automation, CA Server Automation, and CA Configuration Automation feed the infrastructure resources contained in the CMDB component of CA SDM. CA Client Automation and CA Server Automation identify changes to desktops and servers that can introduce security threats, such as unauthorized USB drives, inappropriate software installs, or changes to browser settings.
7. CA Configuration Automation baseline comparison lists changes to CIs that affect the availability of service. Moreover, CA Patch Manager (which feeds CA Client Automation and CA Server Automation) lists all desktops and servers that are not at the proper patch level. CA SDM integrates with CA Identity Manager to enable pass-through authentication in the most complex security architecture.

## IT Service Continuity Management

### Objectives

- Maintain a set of IT Service Continuity plans and IT Recovery plans that support the overall organizational business continuity plans.
- Complete regular business impact analysis exercises to help ensure that all continuity plans are maintained in line with changing business impacts and requirements.
- Assess the impact of all changes on the IT Service Continuity plans and IT Recovery plans.
- Negotiate and agree to the necessary supplier contracts for the provision of the recovery capability that supports the continuity plans with Supplier Management.

## How CA Technologies Solutions Help Meet the Objectives for IT Service Continuity Management

Helping ensure an effective IT Service Continuity Management (ITSCM) process requires a documented and executed continuity plan. CA Technologies integrated solutions leverage all of the solutions documented in this Green Book to provide inputs to defining the continuity plan. This plan is ultimately published in CA SDM and managed as an ongoing project with the business in CA Clarity PPM.

1. The integration of CA SDM with CA Process Automation can be used to automate recovery plans by notifying key personnel, initiating failover systems, and initiating monitoring of new facilities.
2. Functionally, CA Clarity PPM opens Change Orders in CA SDM to schedule recovery testing, which initiates the CA Process Automation process flow to begin a recovery process.
3. Leveraging the solutions in Capacity and Availability Management, a service provider can identify whether the service levels are being met. The service provider can then feed them back to CA SDM and ultimately back into the ITSCM design improvements.

## Service Catalog Management

### Objectives

- Provide a single source of consistent information about all the agreed services.
- Help ensure wide availability to users who have access.

## How CA Technologies Solutions Help Meet the Objectives for Service Catalog Management

The following process describes how CA SDM, CA Service Catalog, CA Clarity PPM, and CA Asset Portfolio Management integrate to help improve the Service Catalog Management process:

1. CA Service Catalog is a solution that supports all objectives of the Service Catalog Management process in Service Design.
2. CA SDM and CA Service Catalog share a repository of users, locations, organizations, tenants, and CA EEM for security.

3. RFCs that are created in CA SDM can be linked to CA Service Catalog requests. The assets in the CA SDM CMDB are managed in CA Asset Portfolio Management.
4. When fulfilling a request, a link directly into CA Asset Portfolio Management data is used to assign only available assets to the request. This link helps ensure immediate CA SDM CMDB updates on the asset or CI status for the request throughout its progress into a production state.
5. CA Clarity PPM contains the master portfolio and helps ensure that CA Service Catalog is given the proper service offerings and deactivates any inactive ones.

## Service Level Management

### Objectives

- Define, document, agree on, monitor, measure, report, and review the level of IT services provided.
- Help ensure the specific and measurable targets are developed for all IT services.
- Monitor and improve customer satisfaction with the quality of service delivered.
- Verify that IT and the customers have a clear and unambiguous expectation of the level of service that is delivered.

### How CA Technologies Solutions Help Meet the Objectives for Service Level Management

The following process describes how CA Clarity PPM, CA eHealth, CA BSI, and CA SDM integrate to help improve the Service Level Management process:

1. The defined and agreed levels of SLAs are developed in CA Clarity PPM and then documented and tracked in CA BSI.
2. The Service Level Manager publishes the details of the SLAs that are maintained in CA BSI or CA Clarity PPM as a CA SDM knowledge document. This document supports communication to the business about the expected levels of service.
3. CA BSI and CA eHealth enforce, alert, and report on the defined levels of service.
4. When there are agreed changes to the SLA, CA Clarity PPM initiates an RFC in CA SDM against the services. The RFC initiates a workflow in CA Process Automation to deploy the updated service levels to CA eHealth and CA BSI for monitoring.

## Supplier Management

### Objective

- Ensure the best value of service is obtained from suppliers and contracts.
- Ensure the underpinning contracts are aligned to business needs and SLAs.
- Manage supplier relationships and performance.
- Maintain a supplier and contracts database.

### How CA Technologies Solutions Help Meet the Objectives for Supplier Management

The following process describes how CA BSI, CA Clarity PPM, CA eHealth, CA Asset Portfolio Management, CA Client Automation, CA Server Automation, and CA SDM integrate to help improve the Supplier Management process:

1. A service provider uses CA Asset Portfolio Management as the supplier and contracts database (SCD) enabling centralized management of underpinning contracts. The database includes a list of the providers, their products and services, and the value they bring to the business.
2. When integrated with CA Client Automation, CA Server Automation, and CA SDM, CA Asset Portfolio Management is able to identify quantitatively the hardware, software, and system performance of the services that the suppliers provide. CA Client Automation and CA Server Automation provide up-to-date inventory in a service provider environment.
3. The CA Client Automation and CA Server Automation inventory is provided to CA Asset Portfolio Management and linked to the relevant contracts.
4. The CA SDM CMDB component and CA Asset Portfolio Management share the physical asset and CI records that are linked back to the Supplier in CA Asset Portfolio Management. Service contracts in CA BSI enforce service levels against the CIs that are associated to the suppliers through automated escalation and reporting.
5. The CA SDM CMDB component contains the relationships of the services to the CIs and assets that link to CA Asset Portfolio Management. Leveraging the integration of the CMDB component with CA eHealth provides the visibility to the overall health and performance of the services that a supplier provides.
6. CA Asset Portfolio Management and CA SDM ad-hoc reporting enables visibility into the number of incidents that are opened against supplier services. This visibility can be used to help manage supplier relationships and prove their performance.

7. CA Asset Portfolio Management and CA SDM are integrated with CA Clarity PPM, which provides the detailed costs that are associated to the service portfolio. This integration is then used to validate and analyze the value that a supplier provides to the service provider and business.
8. CA BSI consolidates the details from the other technologies to provide insight into how well suppliers are meeting SLAs.

## Service Transition

---

### Change Management

#### Objectives

- Help ensure that standardized methods and procedures are used for efficient and prompt handling of all changes.
- Record all changes to service assets and configuration items in the Configuration Management System and optimize the overall business risk.

#### How CA Technologies Solutions Help Meet the Objectives for Change Management

The following process describes how CA Configuration Automation, CA SOI, CA Client Automation, CA Server Automation, and CA SDM integrate to help improve the Change Management process:

1. RFCs are recorded, reviewed, assessed, and prioritized in CA SDM.
2. The approval process of the RFC is enforced using CA Process Automation for normal or emergency changes.
3. For standard changes, CA Process Automation automates the end-to-end approval and deployment, through CA Client Automation and CA Server Automation or CA SOI, of the requested change using the inventory in the CMDB component of CA SDM.
4. When CA Client Automation and CA Server Automation are integrated with CA SDM, RFCs of unauthorized changes are automatically logged as incidents or RFCs for further review.
5. The complex relationships of CIs and the recipients of their services are tracked in CA Configuration Automation. CA Configuration Automation baselines help ensure the complex interconnections of the infrastructure that supplies the service remain unchanged.
6. CA Configuration Automation is integrated into CA SDM through inventory importing, which helps ensure that the CA SDM CMDB is up-to-date with the latest relationships between CIs.

## Evaluation

### Objectives

- Evaluate the impact a new or changed service has on the customer perception of capacity, resource, and performance.
- Enable change management to be more effective in the decision about service changes.

### How CA Technologies Solutions Help Meet the Objectives for Evaluation

The following process describes how CA eHealth, CA CEM, and CA SDM integrate to help improve the evaluation process:

1. Integrating CA eHealth and CA CEM with the CA SDM CMDB and change management functions enables a service provider to compare previous and new performance metrics.
2. CA SDM surveys gather feedback from customers on the effectiveness of a new release.
3. CA CEM enables measurements from the customer perspective of the service.
4. Using the CMDB Visualizer, together with real-time statistics from CA CEM and performance trends of CA eHealth, a service provider can determine which portions of a change reduced the resource performance. CA Technologies integrated solutions enable this end-to-end visualization which facilitates effective management decisions.

## Knowledge Management

### Objectives

- Enable the service provider to be more efficient and improve quality of service, reduce the cost of service, and increase customer satisfaction.
- Help ensure that the service provider staff has a clear and common understanding of the following areas:
  - Value that the services provide to customers.
  - Benefits that are realized from the use of those services.

- Help ensure that at a given time and location, the service provider staff has adequate information about the following areas:
  - Who uses the services
  - Current states of consumption
  - Service delivery constraints
  - Difficulties that the customer faces.

### How CA Technologies Solutions Help Meet the Objectives for Knowledge Management

The following process describes how CA SDM helps improve the Knowledge Management process:

1. CA SDM Knowledge Management centralizes the administration and management of knowledge for service providers.
2. Integrations to other systems that can automate steps for the customer, such as CA Client Automation and CA Server Automation scripts or CA SDM Support Automation Automated Tasks scripts, can be called from Action Content in the knowledge document.

### Release and Deployment Management

#### Objectives

- Provide clear and comprehensive release and deployment plans to align with customer and business change project activities.
- Build, install, test, and deploy release packages efficiently and on schedule.
- Minimize unpredicted impact on the production services, operations, and support organization.
- Improve the satisfaction of customers, users, and service management staff with the service transition practices and outputs.

## How CA Technologies Solutions Help Meet the Objectives for Release and Deployment Management

The following process describes how CA Service Catalog, CA Clarity PPM, CA SCM, CA Client Automation, CA Server Automation, and CA SDM integrate to help improve the Release and Deployment Management process:

1. The Release and Deployment Management process is the culmination of the work from the strategy, design, and remaining transition processes.
2. The service portfolio in CA Clarity PPM initiates an RFC in CA SDM, where the requested change is classified, reviewed, and approved through a Change Management process.
3. CA Process Automation automates the process and creates the release package in CA SCM. The documents that are related to the release package are centrally controlled in CA SCM through approvals and a check-in and check-out process. Ultimately, the documents are promoted through the test to production. Throughout the process, status updates are provided to the project and the RFC.
4. CA SCM leverages its integration with CA Client Automation and CA Server Automation to initiate the deployment of the release package. This action ensures a consistent deployment, which results in a reduced impact to the service at the production roll-out.
5. When the release package is ready to be part of CA Service Catalog, CA SCM notifies the CA Clarity PPM project and portfolio that the service is ready to be promoted into CA Service Catalog.
6. When the RFC is closed, satisfaction surveys are sent to customers. Any incidents that are related to the release can be tied back to the RFC for future analysis and the change impact.

## Service Asset and Configuration Management

### Objectives

- Identify, control, record, report, audit, and verify service assets and configuration items, including their versions, baselines, constituent components, attributes, and relationships.
- Account for, manage, and protect the integrity of service assets and configuration items throughout the service lifecycle by ensuring that only authorized components are used and only authorized changes are made.
- Help ensure the integrity of the assets and configurations that are required to control the services and IT infrastructure by establishing and maintaining an accurate and complete Configuration Management System.

## How CA Technologies Solutions Help Meet the Objectives for Service Asset and Configuration Management

The following process describes how CA Service Catalog, CA Configuration Automation, CA Asset Portfolio Management, CA Client Automation, CA Server Automation, and CA SDM integrate to help improve the Service Asset and Configuration Management process:

1. CA Technologies solutions support the ability of the service provider to perform Service Asset and Configuration Management, which includes everything from procuring a new asset to providing final support for a service. The process helps ensure control through a centralized CMDB component.
2. An asset is procured and logged in CA Asset Portfolio Management with the associated contracts, licensing, and classifying attributes that enable it to be tracked throughout its life cycle.
3. When a CA Service Catalog request is initiated, the service provider leverages the CA Asset Portfolio Management and CA Service Catalog integration to retrieve a list of available assets to assign to the request. Unique attributes, such as which software to install, are also identified.
4. The CA Service Catalog request creates an RFC in CA SDM.
5. CA SDM and CA Asset Portfolio Management share the repository of assets and CIs. When an RFC is initiated from a CA Service Catalog request, it already has the approved linked assets, along with the desired software configuration.
6. The automation and integrated solutions help ensure that the status of the identified asset is updated and auditable by the service provider. The automation and integration also help ensure the continuity of the Release and Deployment Management process.
7. When an asset (for example, a server being provisioned for a particular service) is put onto the network, CA Client Automation and CA Server Automation discover the device. CA Client Automation and CA Server Automation deploy their agents to begin immediate management of the device and start the deployment of required software.
8. To add to the control of the server, CA Configuration Automation identifies which part of the service the server is providing (for example, a database server in a cluster). CA Configuration Automation identifies the relationship, which is then sent back to the CA SDM CMDB component. Change Manager validates the relationship on the RFC.

9. Baselines of the server are contained in CA Client Automation, CA Server Automation, and CA Configuration Automation, allowing a service provider to identify any unauthorized changes to the device.
10. Any updates of software or configuration are provided to CA Asset Portfolio Management by CA Client Automation and CA Server Automation or through updates of the CA SDM CMDB through CA Configuration Automation.
11. As the server depreciates in its ability to provide value to the service, an RFC is created in CA SDM to retire the device. Leveraging historical data from CA SDM (such as incidents, RFCs, performance statistics, and memory upgrades), the service provider can show a full audit trail for the CI over time.

## Service Validation and Testing

### Objectives

- Validate that a service is "fit for use" or Warranty.
- Validate that a service is "fit for purpose" or Utility.
- Provide confidence that a new or changed service delivers value to the customer.
- Confirm that the requirements for a service are correctly defined and remedy any errors or variances early in the service lifecycle.

### How CA Technologies Solutions Help Meet the Objectives for Service Validation and Testing

The following process describes how CA SCM, CA eHealth, CA SOI, and CA SDM integrate to help improve the Service Validation and Testing process:

1. Integrating CA Clarity PPM, CA SDM, and CA SCM enables a service provider to manage the documentation that is required to ensure a new or changed service is fit for use and fit for that purpose.
2. CA Clarity PPM contains the quantitative attributes of what is required for the portfolio.

3. CA SCM contains the documents that capture the requirements of the service as well as the testing strategy.
4. The CA SDM CMDB Visualizer enables modeling of the test environment for impact analysis.

**Note:** The service model is an abstraction that shows logical elements and their relationships. The service definition is the description of an implemented instance of a service that has been modeled. A service map is a selective view of a service showing desired elements and relationships from an explicit perspective. Different perspectives on a given service generate different maps.

5. CA eHealth measures the availability and capacity of the service.
6. CA SOI automates the deployment of the test environment and testing scripts. These integrated solutions share CI information, test plans, test package promotion and state, and the CA Business Intelligence centralized reporting solution.

## Transition Planning and Support

### Objectives

- Plan appropriate capacity and resource to package a release and to build, release, test, deploy, and establish a new or changed service into production.
- Provide support for the service transition teams and people.
- Help ensure that service transition issues, risks, and deviations are reported to the appropriate stakeholders and decision makers.
- Coordinate activities across projects, suppliers, and service teams when required.

### How CA Technologies Solutions Help Meet the Objectives for Transition Planning and Support

The following process describes how CA Clarity PPM, CA SCM, and CA SDM integrate to help improve the Transition Planning and Support process:

1. CA Technologies integrated solutions enable effective transition planning and facilitate support of new or changed services. For transition planning, resources are scheduled in CA Clarity PPM against a project.
2. In CA SDM, individual work tasks are created as RFCs, incidents, or requests from the CA Clarity PPM project workflow, depending on the work needed.

3. As work for developers and product teams begins, CA SDM initiates packages inside CA SCM. CA SCM helps ensure that activity is properly coordinated, approved, and promoted through a defined lifecycle.
4. In CA SDM, incidents are tracked against the projects providing visibility to management on the success of the transition as well as identifying areas that could require additional support.

## Service Operation

---

### Access Management

#### Objectives

- Provide the permission for users to access services based on policies and actions defined in security and availability management.

#### How CA Technologies Solutions Help Meet the Objectives for Access Management

The following process describes how CA SiteMinder, CA Identity Manager, CA Service Catalog, and CA SDM integrate to help improve the Access Management process:

1. From CA Service Catalog, an authorized user can request to change or add security rights as well as initiate approvals that are based on CA Process Automation workflows.
2. After a request is created, CA SDM generates an RFC so that the user profile can be updated in the CA SDM CMDB.
3. CA SDM then initiates a workflow in CA Identity Manager, where security administrators review and implement the security access.
4. CA SiteMinder, integrated with CA Identity Manager, helps ensure that only authorized systems are made available to the user.

### Event Management

#### Objectives

- Detect events, comprehend, and determine the appropriate control action; communicate operational information as well as warnings and exceptions.
- Automate routine operations management activities.

- Provide a way of comparing actual performance and behavior against design standards and Service Level Agreements.

### How CA Technologies Solutions Help Meet the Objectives for Event Management

The following process describes how CA NSM, CA Spectrum, CA eHealth, CA CEM, CA Introscope, and CA SDM integrate to help improve the Event Management process:

1. Event Management begins with determining the level of the service that a service provider intends to monitor.
2. CA CEM monitors the service from the customer perspective. For any breach of service level, CA CEM creates an incident in CA SDM.
3. As a service provider delves deeper into monitoring the application communications to back-end systems, CA Introscope generates incidents in CA SDM.
4. For events that occur inside the applications, CA NSM agent technology generates SNMP traps. These traps are used against a robust correlation engine, which determine whether it is necessary to open an incident.
5. If there is an event in the environment that results in a cascading failure to multiple users or service, CA Spectrum automatically creates a single incident in CA SDM instead of multiple individual incidents for each affected resource. This single incident helps the Service Desk to manage more effectively the queue and to stay focused on the user perception of service. Incidents are logged for each user and linked to the parent incident.
6. CA eHealth monitors the Systems-level SLAs. CA eHealth opens incidents that are based on general service degradation or potential service degradation. Application management and IT operations management functions use this set of integrated solutions to manage their responsibilities. Application managers use the metrics from these solutions to design better services for the customer. For IT Operations Managers, these tools offer the low-level metrics with alerting and automation to ensure day-to-day stability.

### Incident Management

#### Objectives

- Restore normal service operation as quickly as possible and minimize the adverse impact on business operations.
- Help ensure that the best possible service quality and availability are maintained.

## How CA Technologies Solutions Meet the Objectives for Incident Management

The following process describes how CA SDM, CA eHealth, CA Spectrum, CA Client Automation, and CA Server Automation integrate to help improve the Incident Management process.

1. CA SDM provides the front end to incident, problem, request, and change tickets as well as the Knowledge Documents. The CMDB function of CA SDM integrates into all aspects of IT operations to help ensure that CA SDM can gather facts to restore service quickly to the customer.
2. CA eHealth and CA SOI proactively generate Incidents as a result of potential service degradation.
3. Incidents can be analyzed against impact analysis using the CMDB Visualizer to plan availability and capacity better.
4. CA Client Automation and CA Server Automation can generate incidents in CA SDM based on policy violations that result in degradation of client/server ability to provide service.
5. CA Spectrum auto-generates incidents when there is a disruption of service.
6. The CA SDM web services application programming interface (API), email API, and native integration with various CA Technologies solutions enable bidirectional communication that is based on activities that are performed on the ticket. This communication helps ensure the most effective route to restoration of service to the end user.

## Problem Management

### Objectives

- Prevent problems and resulting incidents from happening.
- Eliminate recurring incidents and minimize the impact of incidents that cannot be prevented.

## How CA Technologies Solutions Help Meet the Objectives for Problem Management

The following process describes how CA Spectrum, CA NSM, CA Client Automation, CA Server Automation, CA Configuration Automation, and CA SDM integrate to help improve the Problem Management process:

1. CA SDM provides a robust Problem Management solution that enables a service provider to manage a problem throughout its lifecycle, from Incident creation and known error recording to initiation of an RFC.
2. By leveraging the native integration of CA Spectrum, CA NSM and other Infrastructure Management solutions, Problem Management can become proactive.
3. CA Spectrum and CA NSM monitor the infrastructure for the signs of service degradation that automatically opens problem tickets.
4. CA Client Automation and CA Server Automation, when integrated with the CA SDM CMDB, proactively create hardware and software based Incidents. The Problem Manager can leverage the Incidents to perform Root Cause Analysis (RCA) of the problem.
5. CA Configuration Automation integrates with CA SDM to enable a Problem Manager to identify deviations of a CI-based configuration change that could be the root cause of the problem.

## Request Fulfillment

### Objectives

- Provide a channel for users to request and receive standard services that have a predefined approval and qualification process.
- Provide information to users and customers about available services and procedures for obtaining them.
- Source and deliver the components of requested services.
- Assist with general information, complaints, or comments.

## How CA Technologies Solutions Help Meet the Objectives for Request Fulfillment

The following process describes how CA Service Catalog, CA Asset Portfolio Management, and CA SDM integrate to help improve the Request Fulfillment process:

1. CA Service Catalog provides a list, description, and workflow of services to enable request fulfillment.

CA Service Catalog provides the list of offerings that the user can access, the pricing, and the expected levels of service for the offering.

2. CA Service Catalog natively integrates with CA Asset Portfolio Management. CA Asset Portfolio Management maintains a list and status of available resources that can fulfill the request. When Service Asset Managers fulfill the order, they link the identified resource to the request and they create an RFC in CA SDM for deployment.
3. The CA SDM end-user self-service interface helps ensure that customers have access to the following information:
  - Knowledge documents
  - Hours of service
  - Requests for general information (single-click access)
  - Complaints or comments
  - View into CA Service Catalog offerings

## Continual Service Improvement

---

### Seven-Step Improvement Process

CA Technologies integrated solutions collaboratively enable the Seven-Step Improvement Process. Each solution provides metrics, measures, and process enablers that facilitate the following process:

1. Defining what measured: CA Clarity PPM is the central tool to collect these requirements, which are then validated through CA BSI.
2. Defining what you can measure: CA eHealth, CA Wily, and CA NSM help ensure that you can measure all technology attributes to improve your services. CA Clarity PPM, CA BSI, and CA SDM enable you to measure process level metrics.

3. Gathering the data: CA eHealth, CA Wily, and CA NSM enable the collection of the data that your organization identifies for technology and service level metrics. CA Clarity PPM and CA SDM collaboratively provide process metrics.
4. Processing the data: CA Technologies uses CA BSI and CA Business Intelligence reporting to provide a central view of the collected metrics.
5. Analyzing the data: CA Business Intelligence and CA BSI enable robust analysis of the gathered metrics.
6. Presenting and using the data: At this stage of the Seven-Step Improvement Process, you can take your CA Business Intelligence and CA BSI reports to your Service Manager, Continual Service Improvement Manager, and can Process owners, to review the collected data.
7. Implementing corrective actions: Finally, you can update the status of your portfolio in CA Clarity PPM. CA Clarity PPM creates an RFC in CA SDM and the cycle of improvement begins again. You have continuous visibility of business objectives that are tied to critical success factors and the underlying key performance indicators (KPIs) and metrics, all from the integrated suite of solutions CA Technologies provides.



# Chapter 3: CA Asset Portfolio Management

## CA Asset Portfolio Management Integration

---

This chapter discusses how CA SDM r12.6 and CA Asset Portfolio Management r12.6 can be configured to work together. The following key topics are covered:

- Integration points and functionality from CA SDM
- Integration points and value from CA Asset Portfolio Management to CA SDM
- How the integration works
- Integration instructions

## What is CA Asset Portfolio Management

---

CA Asset Portfolio Management r12.6 provides comprehensive IT ownership management to help you manage the financial and ownership information of your organizational IT-related Configuration Items (CIs). CA Asset Portfolio Management supports the entire life cycle of a CI from procurement through acquisition, allocation, use, and disposition, including legal and cost information.

**Note:** CA Asset Portfolio Management and CA Software Compliance Manager comprise the CA IT Asset Manager (CA ITAM) solution, which helps your organization optimize assets, mitigate risks, and reduce costs associated with managing IT assets.

## Integration Details

---

The integration between CA APM r12.6 and CA SDM enables sharing of business critical information to form a comprehensive view of assets and CIs.

## Integration Value

The CA APM integration provides the following values:

- Control, track, and improve life cycle management of CIs.
- Make owned CI data available to first-line support through the Common Asset Viewer.
- Provide easy access to service contract information and other legal information.
- Control, track, and improve procurement procedures.
- Provide better support to the users.
- Help lower the total cost of ownership (TCO).
- Let service desk analysts to determine whether an asset having problems is under maintenance, and can therefore be fixed at no cost.

## Integration Points Between CA APM and CA SDM

The following integration points are available from both products:

- CA APM and CA SDM share data when running on top of the same MDB for Configuration Items (CI), Contacts, Models, Locations, and Company information.
- Shared audit history – All changes to assets and CIs are recorded and can be viewed from each system, regardless of where the change was initiated from.
- Assets and CIs are clearly identified as such in both CA APM and CA SDM.
- Shared extended fields – Extended fields which are created for CIs can be configured to appear in CA APM.
- Launch in context a CA APM asset directly from a CI.
- Asset Families and classes are shared.

## Configuring the Integration Between CA APM and CA SDM

Most of the integration between CA APM and CA SDM is done through the installation of both products on a shared CA MDB. After the products are installed on a shared MDB, the following integration features are automatically enabled and functional:

- Sharing of common data, such as Contacts, Models, Locations, Companies, and CIs
- Sharing of audit history
- Assets which are marked as CIs in CA APM, and CIs marked as Assets in SDM, where appropriate.
- Common Asset Families and Classes

When viewing an asset in CA APM, you can see the asset details to know whether the asset is a CI or not.

The screenshot shows the 'Basic Information' form for an asset named APMSDMR126. The form includes the following fields:

- Asset Name:** APMSDMR126
- Asset Alias:** (empty)
- Serial Number:** APMSDMR126
- Alt Asset ID:** (empty)
- Host Name:** APMSDMR126
- DNS Name:** APMSDMR126
- MAC Address:** 00-0C-29-C6-7D-F1
- Audit Date:** (empty)
- Operating System:** (empty)
- Capacity:** (empty)
- Capacity Units:** (empty)
- Department:** (empty)
- Cost Center:** (empty)
- GL Code:** (empty)
- Requisition ID:** (empty)
- Purchase Order ID:** (empty)
- CI:**
- Asset:**

The 'CI' and 'Asset' checkboxes are highlighted with a red box.

To enable the sharing of extended fields fully, and to launch CA APM in the context of a CI, perform certain additional procedures.



## Share Extended Fields Between CA APM and CA SDM

Sharing extended fields lets you update and track the custom extended field from either product. To share extended fields, you first create the field in CA SDM through the Web Screen Painter, and then reference that field in a CA APM Global Configuration.

In this example we will be using a new field which holds the IT Business Code, an integer representing a business function for the asset.

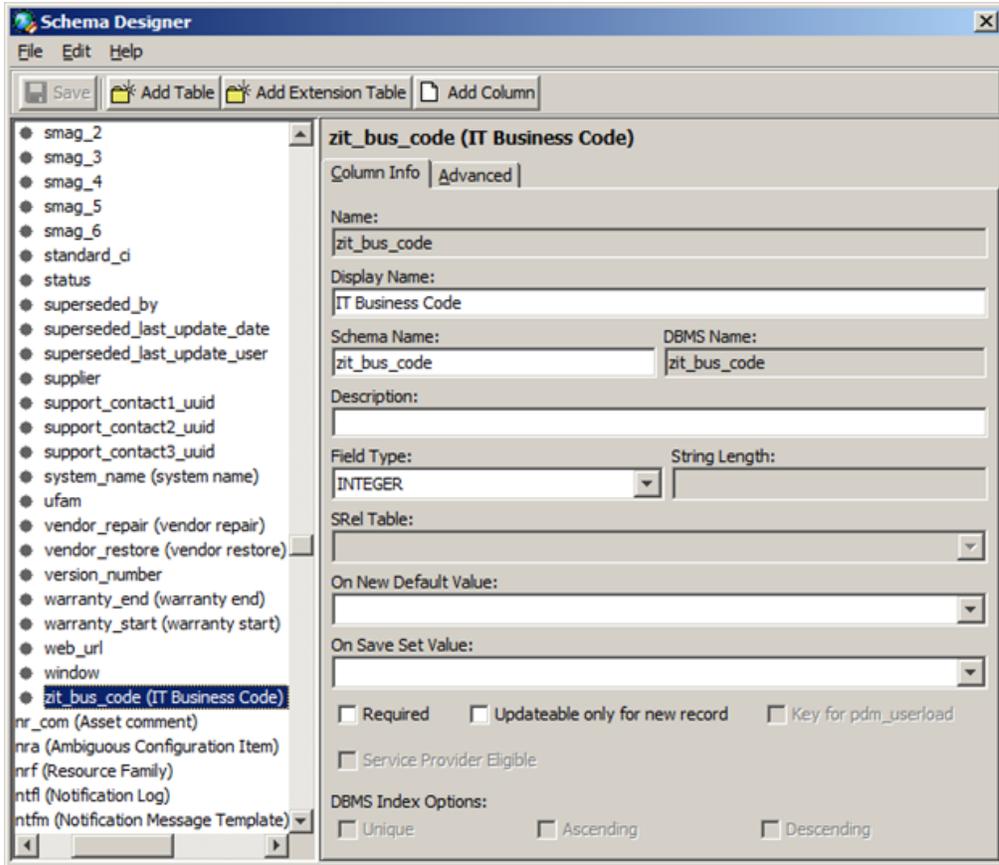
**Note:** For these steps to work, and the integration to work properly, you need to have applied CA APM 12.6 Cumulative Patch 2, CA APM Cumulative Patch 2 Bridge Fix, and CA APM Patch T5XU014.

### Follow these steps:

1. Launch CA SDM Web Screen painter and modify the Schema for the nr object.

This updates the `usp_owned_resource` table in the MDB. Pay particular attention to the Schema Name, Field Type, and Size (String Length), which are needed to properly reference this field from a CA APM Global Configuration.

**Note:** If the field type is a String in Web Screen painter, it cannot be larger than 255 in length. Anything larger than that gets created as an `ntext` data type, which is incompatible with CA APM. Strings of less than or equal to a length of 255 are created as `nvarchar` type, which is compatible with CA APM.

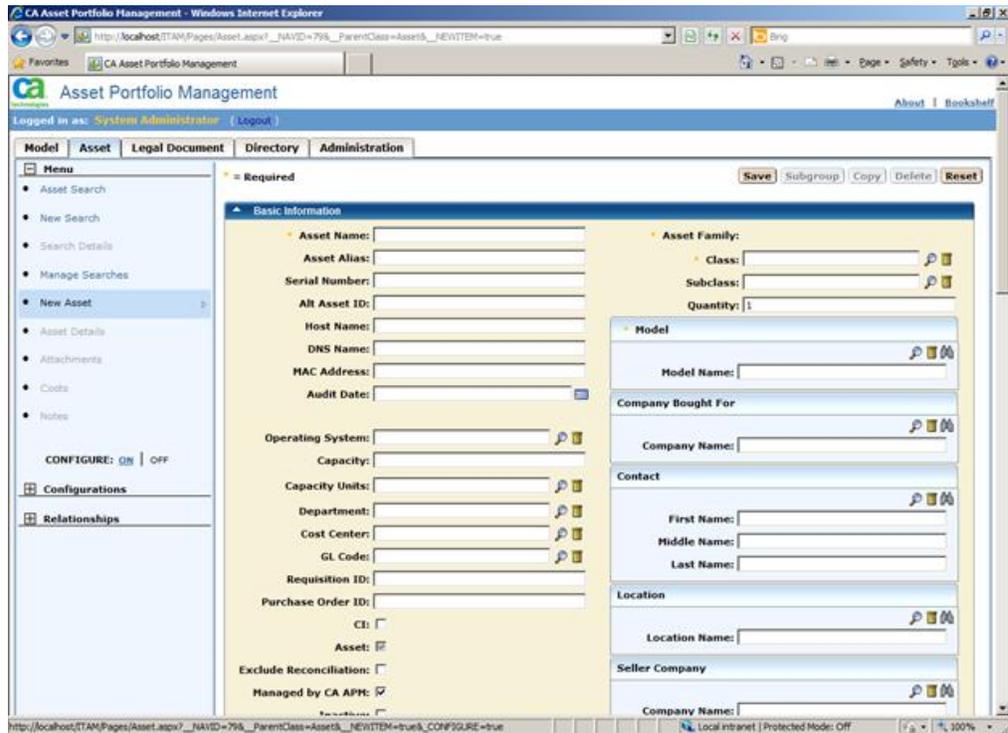


2. Publish the Schema changes using the pdm\_publish command.
3. Run the CreateAuditTableAndTriggersMsSql.sql script.

This creates the corresponding audit table for the new field. This script can be found on the APM Server in the InstallConfig/RemCom directory.

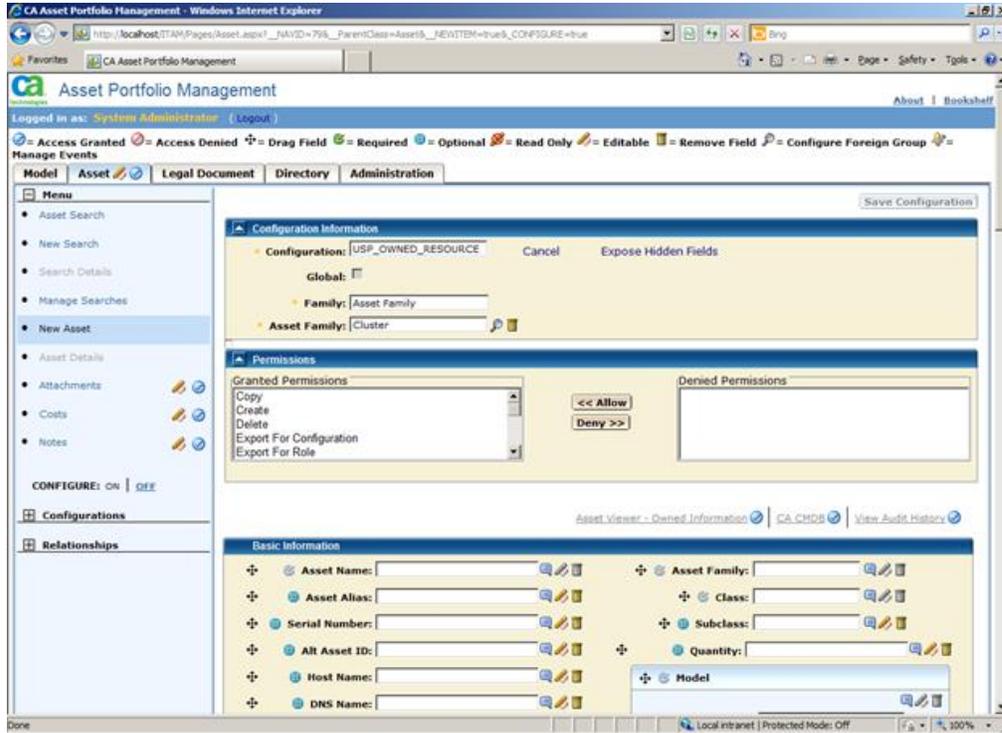
**Note:** This script must be run after any new field is created in Web Screen Painter that is going to be shared in CA APM. The default directory for the script is typically C:\Program Files (x86)\CA\ITAM\InstallConfig\RemCom. This can be changed by the user who installs CA APM.

4. Add a new field which references the new extended field to the cmdb\_detail.html form and publish the updated form. This allows you to see and modify the field from CA SDM.
5. Launch CA APM and click Configure: On, on the left hand menu.



The CA APM Configuration screen displays.

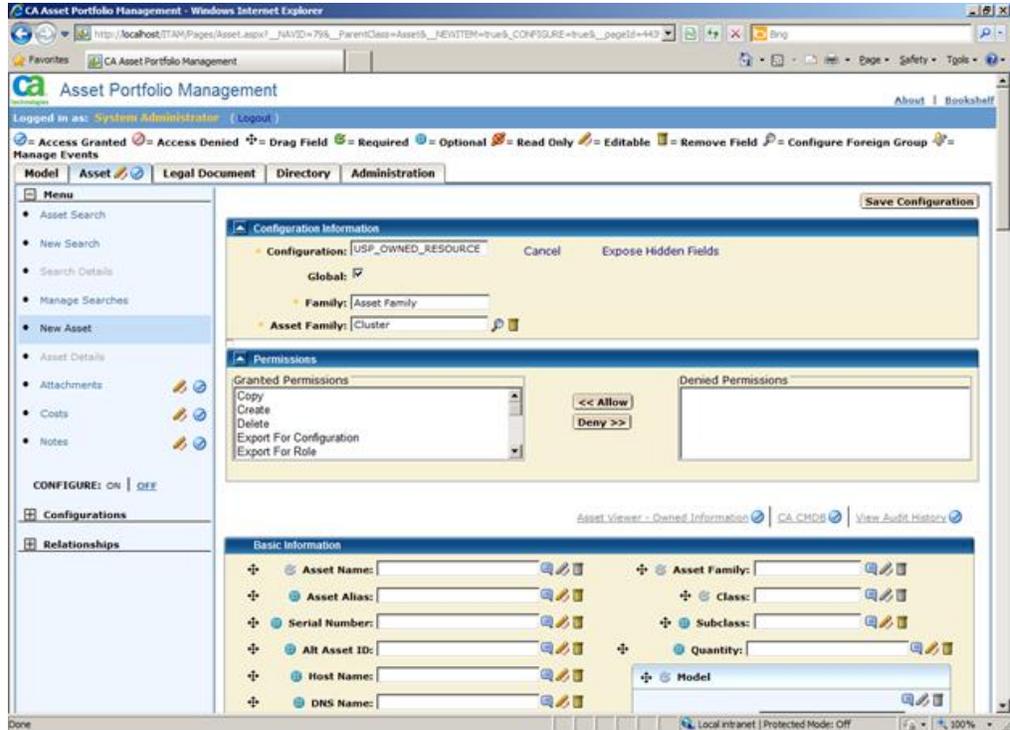
6. On the CA APM Configuration screen, create a new Configuration with a new name, or search for an existing Global Configuration. In this example we are creating a new one named USP\_OWNED\_RESOURCE



- After entering the new name, click anywhere on the screen.

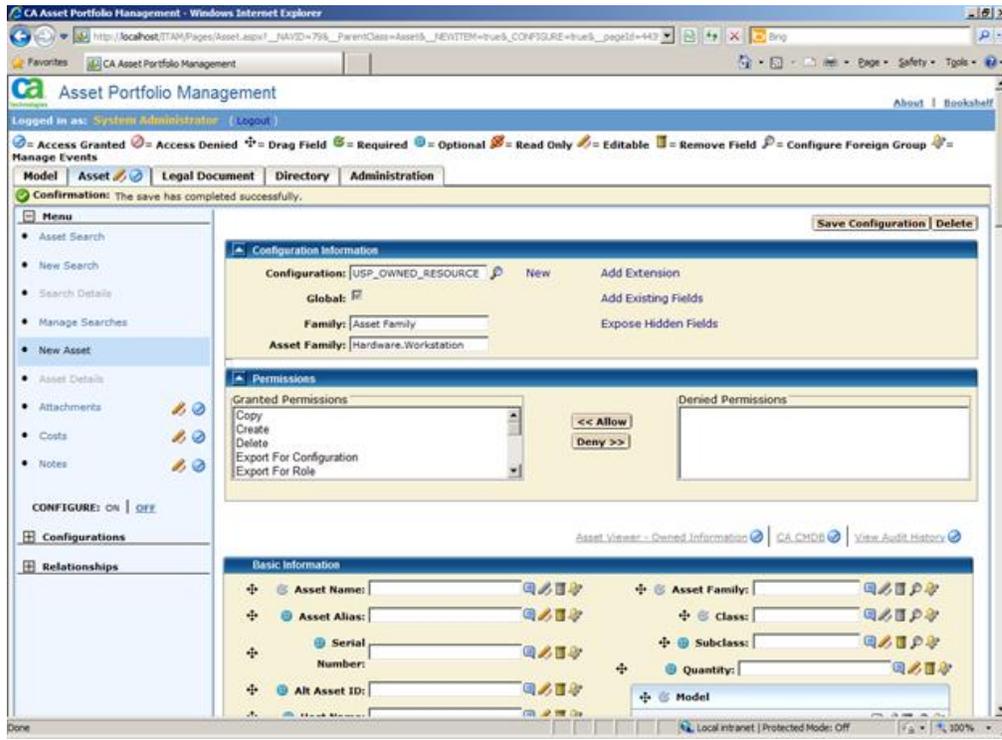
The other parts of the screen become active, in particular, the Global checkbox.

- Click the Global checkbox to mark this configuration as a Global Configuration.



9. Click the Save Configuration button.

The configuration is saved and new options are now available for this configuration.



**Note:** This step is not required if you are using an existing Global Configuration.

10. Click Add Extension to launch the Extension Wizard.

Configuration Wizard -- Webpage Dialog

1 2

Type Fields

Choose the type of field you would like to create:

Simple Field

Reference Field

Hierarchy

• Choose the page section to add this field to: Basic Information

Across all extended types

Back Next Finish Cancel

http://localhost/ITAM/Pages/ExtensionWizardPageHc Local intranet | Protected Mode: Off

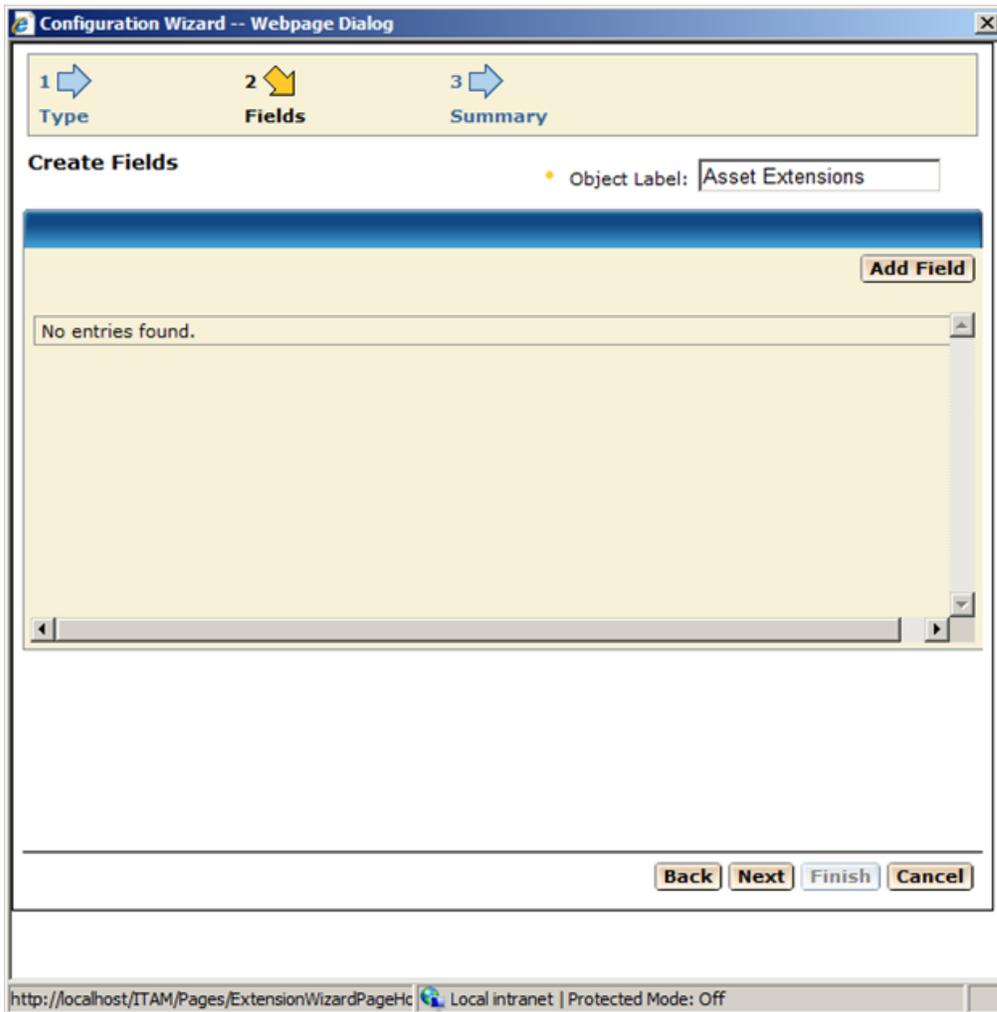
**Note:** This is launched as a pop up window, so you need to disable any pop up blocker, or enable pop up's from your APM site.

11. Select Simple Field, choose the area on the screen where you want the field to appear and make sure to select Across all extended types checkbox.

This field is now applicable to all Asset Families.

12. Click Next to continue the wizard.

The Field definition screen appears.



13. Click the Add Field button.

A new form for field information appears.

The screenshot shows a web-based configuration wizard titled "Configuration Wizard -- Webpage Dialog". At the top, there are three steps: 1 Type, 2 Fields (highlighted), and 3 Summary. The "Create Fields" section is active, showing "Object Label: Asset Extensions". Below this is a table with the message "No entries found." and a green checkmark icon. An "Add Field" button is located in the top right of the table area. Below the table is a form for creating a new field with the following fields:

- Label: IT Business Code
- Format: Integer (dropdown menu)
- Field Name: zit\_bus\_code
- Attribute Name: zit\_bus\_code
- Field Size: 4
- Description: (empty)
- Required:
- Inactive: Required

At the bottom of the wizard, there are buttons for "Back", "Next", "Finish", and "Cancel". The browser address bar shows "http://localhost/ITAM/Pages/ExtensionWizardPageHc" and the status bar indicates "Local intranet | Protected Mode: Off".

14. Fill in the form with the exact information that you have from the Web Screen Painter definition.

**Note:** Integer field size is 4, even though it is not specified in SDM Web Screen Painter.

15. After filling in the information, click the green check mark to save the field changes.

The field now displays in the list.

Configuration Wizard -- Webpage Dialog

1 Type      2 Fields      3 Summary

Create Fields      Object Label: Asset Extensions

Add Field

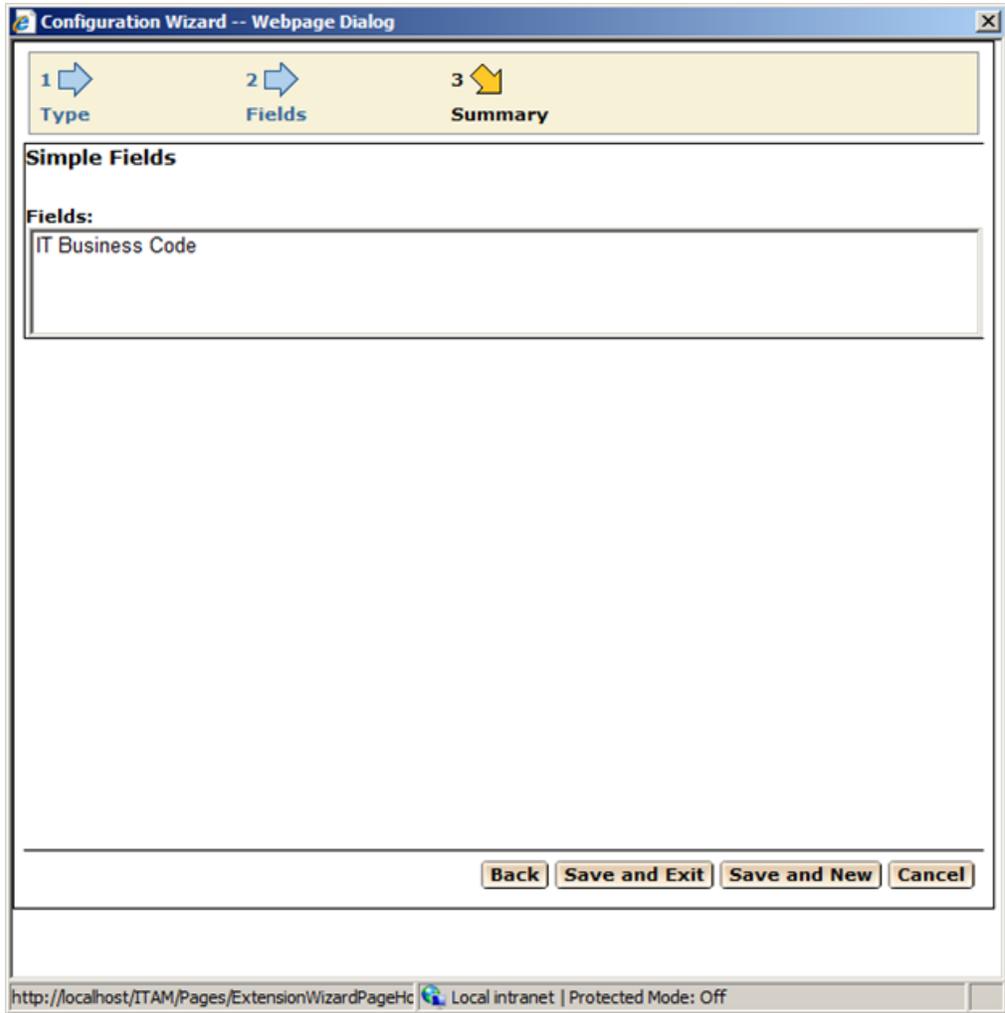
	Label	Format	Field Name	Attribute Name	Field Size	Description	Required	Inacti
	IT Business Code	Integer	zit_bus_code	zit_bus_code	4		<input checked="" type="checkbox"/>	<input type="checkbox"/>

Back   Next   Finish   Cancel

http://localhost/ITAM/Pages/ExtensionWizardPageHc   Local intranet | Protected Mode: Off

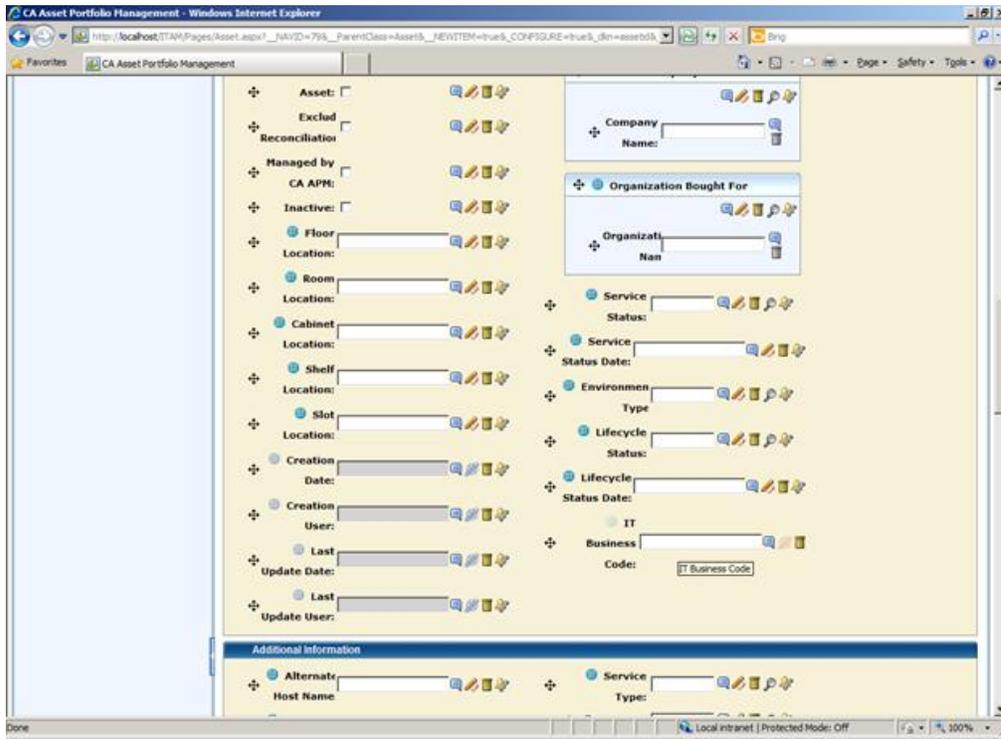
16. Click Next to continue.

The final screen of the wizard appears.



17. Click Save and Exit to add the field and exit the wizard.

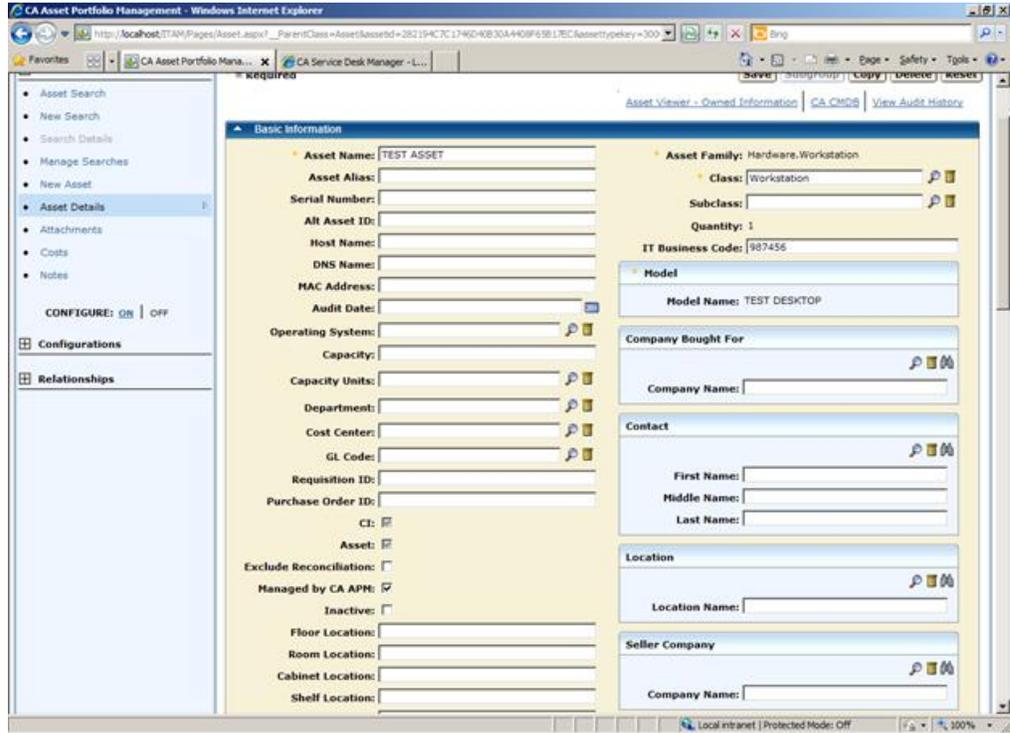
You are brought back to the APM Configuration screen. Look for your new field on the page.



- Click Save Configuration

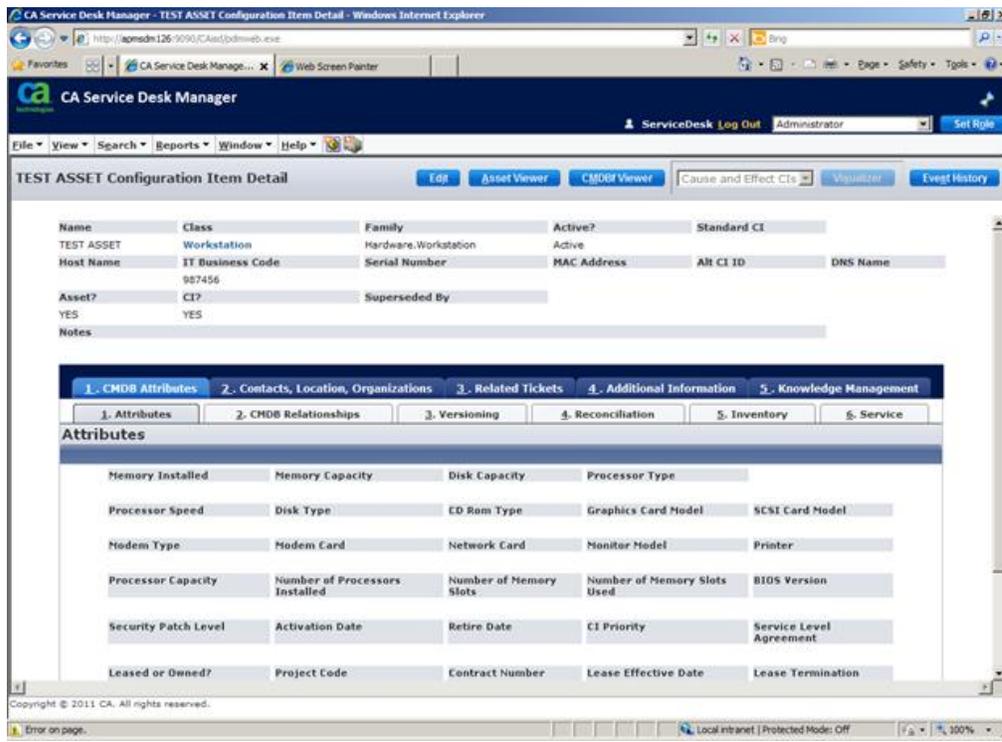
The changes are saved the changes to the APM Global Configuration.

- Open an asset in CA APM which is also a CI in CA SDM. Populate the new field with a value, and save the Asset.



20. Open the Asset in CA SDM.

The value for the field is the same.

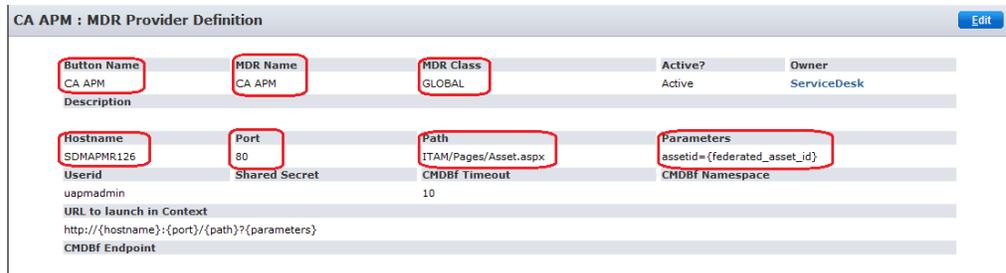


### Launch CA APM in Context From CA SDM

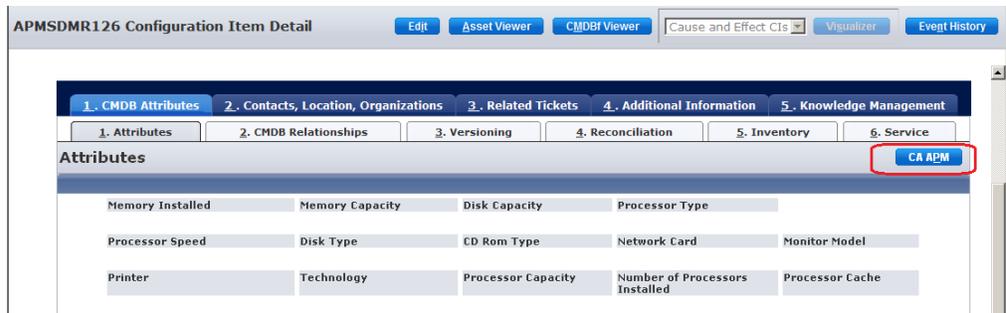
To launch CA APM in context from CA SDM, you add a Management Data Repository (MDR) in CA SDM to point to the proper CA APM URL.

**Follow these steps:**

1. Create an MDR in CA SDM with the following properties:
  - a. Button Name: CA APM
  - b. MDR Name: CA APM
  - c. MDR Class: GLOBAL
  - d. Hostname: CA APM Server Name
  - e. Path: ITAM/Pages/Asset.aspx
  - f. Parameters: assetid={federated\_asset\_id}



The MDR then appears as a button on the CI details page.



2. Click the CA APM button.

The corresponding asset record opens in CA APM.

Including CA Service Catalog in the Solution

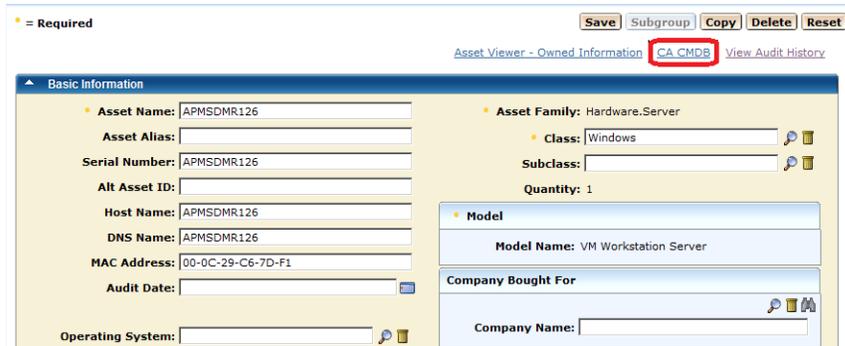
## Launch CA SDM in Context from CA APM

You can also launch CA SDM in context from CA APM.

### Follow these steps:

1. Click the CA CMDB link from a CI page in CA APM.

The CA SDM interface opens the detail page for the CI.



The screenshot shows the CA APM interface for an Asset Viewer. At the top, there are buttons for 'Save', 'Subgroup', 'Copy', 'Delete', and 'Reset'. Below these are navigation links: 'Asset Viewer - Owned Information', 'CA CMDB' (highlighted with a red box), and 'View Audit History'. The main content area is titled 'Basic Information' and contains several fields for asset details. On the left, fields include 'Asset Name' (APMSDMR126), 'Asset Alias', 'Serial Number' (APMSDMR126), 'Alt Asset ID', 'Host Name' (APMSDMR126), 'DNS Name' (APMSDMR126), 'MAC Address' (00-0C-29-C6-7D-F1), 'Audit Date', and 'Operating System'. On the right, fields include 'Asset Family' (Hardware.Server), 'Class' (Windows), 'Subclass', and 'Quantity' (1). Below these are sections for 'Model' (Model Name: VM Workstation Server) and 'Company Bought For' (Company Name).

## Including CA Service Catalog in the Solution

You can easily add CA Service Catalog to the solution for an even broader solution. By adding CA Catalog, you can include an asset request or fulfillment process to your solution. Those assets can either be new or existing assets, including assets that can also be CIs.

For more information on how to integrate CA Catalog with CA APM, see the *CA APM Implementation Guide* and *User Guide*, and the *CA Catalog Integration Guide*.

# Chapter 4: CA Client Automation Manager

## What is CA Client Automation Manager

---

CA Client Automation is designed to provide comprehensive visibility into the IT asset base and automate the daily operational processes needed to support the client device environment—whether physical or virtual. No matter how complex your IT environment, CA Client Automation can help streamline the time-consuming and labor-intensive tasks that bog down your IT organization, helping you run more efficiently and cost-effectively than ever before.

Key features include the following:

- Asset discovery and inventory
- Cross-platform reporting
- Intelligent analytics
- Operating system (OS) installation management
- Software delivery
- Remote desktop control
- Patch research and management
- Desktop migration

## Asset Management Functionality

The asset management functionality available in CA Client Automation provides a powerful solution for proactive management of IT assets in a business environment. It provides full-featured asset tracking capabilities including hardware, software, and network inventory, configuration management, and software usage monitoring.

Some key asset management features are as follows:

- **Hardware Inventory**
  - Provides detailed inventory information such as serial numbers, CPU model and speed, amount of system RAM, and available disk space.
  - Increase visibility with an extended inventory of virtualized platform environments, including VMWare ESX, Solaris Zones, etc.
- **Software Inventory**
  - Detects software applications which are installed on host systems. CA provides over 15,000 predefined software definitions or software signatures, and periodic online signature updates.
  - Produce a detailed software inventory, including virtualized applications, with a higher degree of granularity than that of traditional inventory-scanning solutions.
- **Software Usage Monitoring**
  - Monitors software usage. CA Client Automation lets you have complete control of the software running in the enterprise and align the software licenses to your needs.
- **Built-in Script Language**
  - Enables you to create and run jobs on the agent systems.
- **Policies**
  - Lets you set alarms when the threshold value is exceeded or an event occurs. It automates repetitive or time-consuming maintenance and security tasks to manage your IT environment efficiently.
- **Collect inventory data, without installing a dedicated management agent, by enabling users to provide information through such methods as visiting a corporate website, clicking a link in an email message, or using a USB memory stick.**
- **Scan client systems against the latest Federal Desktop Core Configuration (FDCC) / Security Content Automation Protocol (SCAP) standards set forth by the US Federal government, to more easily identify and report on systems that are out of compliance.**

## Reports

- Predefined and customized reports deliver all the information that you need about your enterprise.

## Intelligent analytics

CA Client Automation helps drive the strategic planning efforts of your IT executives by converting raw asset data into actionable intelligence they can leverage to make well-informed business decisions, reduce organizational risk, provide for greater policy compliance, and identify opportunities for additional efficiencies and cost savings.

- High-level analytics help you quickly identify risks in the environment and promote further investigation into asset deployment, performance metrics, service levels, and financials.
- Standardized displays help you find dominant system configurations, based on performance, hardware components, and software, and compare them against other assets in the environment.
- Green IT Assessment per defined policies includes the areas of power management, availability, usage, and identification of “rogue” systems.

## Software Delivery Functionality

The software delivery functionality available in CA Client Automation provides a flexible and comprehensive mechanism for building, distributing, installing, and managing software across your enterprise. Policy-based automation makes it simple to maintain the state of software on all the computers within the enterprise.

Key software delivery features include the following:

- An agent plug-in resides on all target computers and is responsible for installing, updating, and removing software packages in response to orders from the manager.
- The ability to install, update, and remove software packages remotely on-demand or scheduled, without having to grant system administrative privileges to users.
- A powerful data transport infrastructure optimizes network use.
- The ability to deploy existing software packages in many packaging formats.
- A powerful scripting language to perform tasks on target computers.
- A software packaging tool or Packager can be used to create software packages for deployment. The Packager captures all files and configuration changes that occur after a product has been installed. This information is collected and automatically transformed into a software package that is ready to be included in the software package library.
- The ability to track software installation, identify who installed the software, when and where it was installed, and how it was installed.
- Manage the deployment of virtualized applications, including VMWare ThinApp and Microsoft App-V technologies.

## OS Installation Management

- Deploy and redeploy systems with a comprehensive approach to operating system installation management that spans everything from bare metal buildups to rebuilds after crashes.
- Install and configure the Windows Vista or Windows 7 operating system by leveraging WinPE boot images, and download a predefined application set.
- Utilize the ImageX imaging tool within the Windows Automated Installation Kit (WAIK), and run it from WinPE to capture images from FAT, FAT32, and NTFS installations.
- Read, manage, and deploy standard images made with Symantec Ghost or PowerQuest DeployCenter.
- Detect, rebuild, and restore the most recently known configuration automatically, in the event of a crash.

## Remote Control Functionality

CA Client Automation enables your IT administrators to reliably and securely access, control, view, manage, and modify remote desktop and mobile systems. This allows end users to simultaneously exchange files, conduct interactive chat sessions, execute remote applications, and monitor and record activities with greater efficiency and effectiveness—no matter how far they may be from the main office. Remote desktop control functionality allows you to do the following :

- Configure and maintain systems from a centralized management console.
- Enforce policies through template-based remote control configurations that can be applied to groups of computers to prevent unauthorized changes.
- Manage remote systems using features for exclusive control, shared control, stealth view, Web viewer, and classroom and stealth modes.
- Transfer files, chat with the host user, record remote sessions for later playback, or reboot the host system.
- Enforce authenticity by aligning different security methods, encryptions, and access permissions to specific user and connection types.
- Cross-platform remote management support allowing connections from Windows to Linux, or Windows to Mac OS X.

## Windows New Desktop Migration

By providing automation that leads to greater control and improved execution of change initiatives, CA Client Automation enables you to preserve and transfer unique end-user settings, data, and preferences during a system migration, hardware refresh, operating system upgrade, new installation, or recovery process, and allows you to:

- Save unique data and settings to a local machine or server for later migration, or transfer them in real time via a connection between the old and new PCs.
- Leverage powerful features for account creation, redirection, and security, as well as tools for migrating user profiles and transferring data from NT domains to Active Directory (AD).
- Utilize advanced data collection capabilities to migrate comprehensive system and application settings.
- Initiate migration processes from a centralized location that uses shared configuration resources, such as option files and templates, and issues return codes to trigger the next steps in the process.
- Schedule the recurring storage of specific PC data and settings that collects only the changes that have taken place since the last time the file was saved.
- Leverage automated deployment setup, director, template editor, explorer, option editor, studio, and merger and acquisition tools to cut migration times.

## Path Research Management

The Patch Manager component is used for managing software patches in heterogeneous environments. It automates the identification, gathering, packaging, deployment, and on-going validation of patches and related software configuration changes throughout your enterprise.

The following are the two primary components in CA Patch Management:

- **CA Patch Manager** - Resides on your computer and provides a wizard-driven user interface to simplify the patch management process, which includes package creation, testing, enterprise deployment, patch-level assurance.
- **CA Online Content Service** - An online service available through SupportConnect to manage the collection of metadata for available or applicable patches. This service is provided as part of your CA Patch Manager subscription.

To help you deliver consistent, reliable software patch management, CA Client Automation addresses each step in the process—from monitoring and discovery through research, packaging, testing, and deployment. And with around-the-clock support from the CA Technologies Content Research Team, you gain the support needed to help keep your enterprise systems up-to-date with the most current and effective software patches. The solution's patch management features help you do the following :

- Leverage monitoring, validating, researching, and publishing features that work together to identify new patches and make them automatically available.
- Employ a simple, task-oriented user interface that combines with a Web-based reporting portal to provide the controls and information needed to administer each step in the patch process.
- Implement a formal patch testing phase that assesses patch packages—and metadata—against the required system configurations.
- Initiate package deployments automatically, using defined policies, and apply pre- and post-requisites, dependencies, and roll-up structures during installations.
- Monitor all patches and packages to ensure they remain valid and in effect, and that new or crashed systems are automatically restored to the most up-to-date patch level.
- Utilize monthly delta roll-ups of new patches to enable administrators to deploy a single patch package each month.

Use the CA Patch Manager to do the following:

- Know which software and patches are installed on your computer.
- Establish patch level policies and ensure automatic compliance with the defined policies.

- Perform impact and compliance analysis. For example, if patch ABC is required for product XYZ, you can verify the application of the patch, and also identify the computers which use the software, the departments where the computers are located, and the users who are affected if the patch is not installed. This information helps you determine the appropriate plan for distributing the patch without disrupting day-to-day business.
- Enforce the best practices for patch testing and distribution.

You can recognize the following benefits using CA Patch Management:

- A dedicated online patch research service that monitors for available patches, gathers the available patch data, and validates and identifies dependencies before the patch information is published and pushed to the CA Patch Management server.
- A formal patch management test phase. Packages can be deployed to test resources, allowing you to assess the impact of a patch before it is deployed enterprise wide.
- Newly deployed, found, or rebuilt computers are automatically brought up to patch level compliance.
- Patch distribution is tracked in real time.
- State compliance can be determined and patch level assurance enforced.
- A flexible, complete web-based portal reporting system with automatic report scheduling.
- Integration with CA SDM R12.6 and CA Client Automation R12.5.

## Integration Details

---

The integration of CA Client Automation with CA SDM makes CA Client Automation a service-aware solution. This means that CA Client Automation, based on certain events of its managed assets, can trigger an event to create tickets in CA SDM using the DSM web services. Tickets can be incidents, requests, problems, change orders, and issues. For this integration, ticket creation in CA SDM is controlled by the Service Aware policy, which enumerates a list of problem types. CA Client Automation uses problem types to categorize the problem and address the kind of ticket to be created.

The CA Client Automation integration provides a graphical user interface that allows context-sensitive launches of each solution in terms of the integration. The interface is named the Common Asset Viewer, which displays an integrated view of an asset. It also enables navigation between CA Client Automation and CA SDM.

The following table provides an overview of the supported in-context starts between the DSM Explorer or the Web Console and the CA SDM Web Interface:

From	To	In Context	Context
Explorer/Web Console	CA SDM Web Interface	Software job	Ticket being created on job failure
Explorer/Web Console	CA SDM Web Interface	Asset policy	Ticket being created on policy violation
CA SDM Web Interface	Explorer/Web Console	Ticket detail	Software job
CA SDM Web Interface	Explorer/Web Console	Ticket detail	Asset policy

**Note:** The configuration considerations in this section apply to both DSM domain and enterprise managers.

### Integration Points from CA Client Automation to CA SDM

The CA Client Automation integration points help CA Client Automation Administrators to do the following:

- Configure CA Client Automation to Open CA SDM tickets automatically when an asset management policy is violated, or when a software delivery job fails.
- Open the CA SDM Ticket Detail window manually in the context of a particular Configuration Item (CI).
- Start the CA SDM web interface from the Quick Launch window in the DSM Explorer.

**Note:** The asset management discovered assets information is stored in a common asset data model within the MDB. CA SDM uses multiple CA products, which employ this asset data model.

### Integration Points from CA SDM to CA Client Automation

The CA SDM Integration points help CA SDM Analysts to do the following:

- Interactively view both the Managed and Discovered asset spaces, using the Asset Viewer or Common Asset View option available in the CA SDM Configuration Item Detail window.
- Selectively choose discovered assets from the CI Search List window, for inclusion into the CA SDM managed space.

### Integration Points from CA Client Automation to CA SDM

The following are CA SDM integration points from CA Client Automation:

- Automatic ticket creation from CA Client Automation. Asset Management for query or event policies violation.
- Automatic ticket creation from CA Client Automation. Software Delivery for job failure.
- Interactive start, in context, menu option for ticket creation associated with a discovered Configuration Item (CI) from CA Client Automation.
- Launch In-context of CA SDM UI from the CA Client Automation. Explorer interface.
- The MDB's support of common asset properties strengthens the identification of assets between CA Asset Management and CA SDM.
- Common Asset Viewer, provided with CA SDM and CA Asset Management, displays an integrated view of an asset. It also enables navigation between asset handling applications.

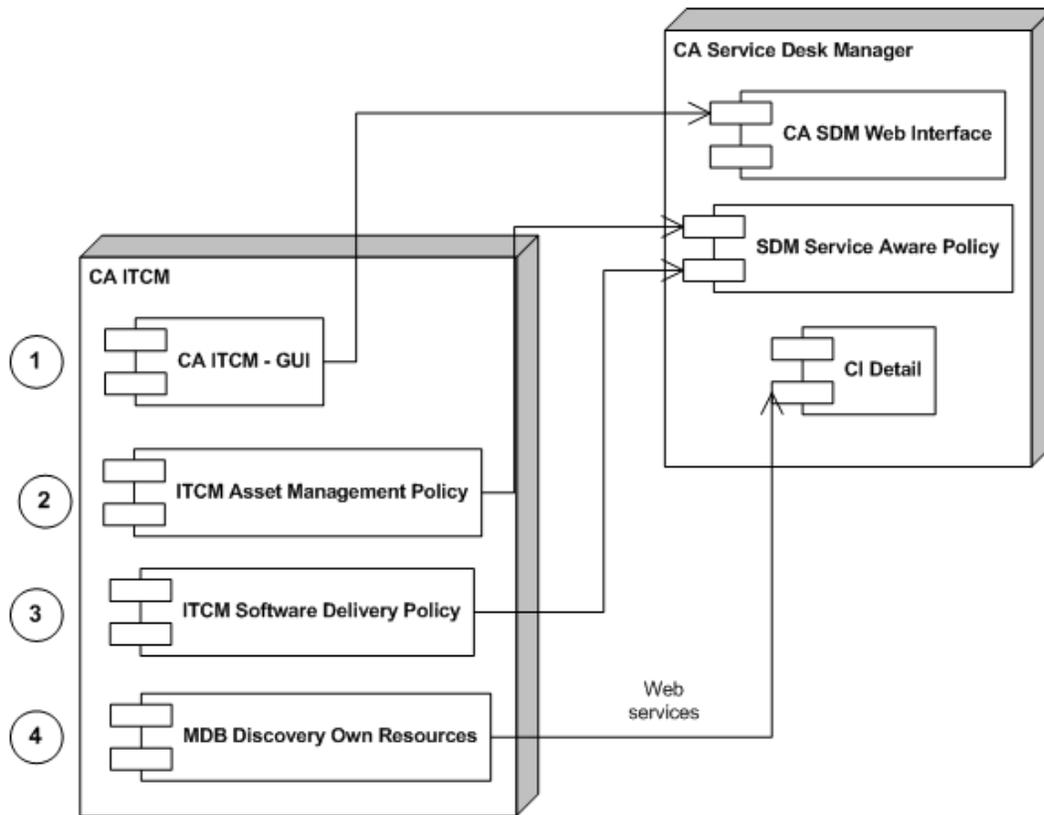
## Integration Value

The CA Client Automation integration provides the following values:

- Instant Configuration Item control, for hardware and software, at all levels in the infrastructure.
- Control of automatic incident creation through flexible event policies, problem category, and priority setting definitions.
- Simplified impact assessment when policy violation occurs.
- No extra maintenance required.
- Improved user support.
- Improved infrastructure management and increased efficiency.
- Flexible role and process management.
- Enhanced incident and problem solving at the organization level.
- Visual interaction with the user to monitor user activity and help improve how users perform certain tasks.
- Proactively anticipate incident creation and advise the CA SDM by knowing what policy or application changes are being made using Software Delivery reporting.

## How the Integration Works

The following diagram illustrates how the CA Client Automation integration works:



The following information applies to the previous diagram:

The integration allows a user to start the CA SDM Ticket Detail window in context to create an incident manually associated to a particular Configuration Item (CI). In addition, the CA SDM Web interface can be started from the CA Client Automation Explorer, Quick Launch window.

1. The integration allows CA Client Automation to automatically open CA SDM Tickets when a CA Client Automation Asset Management policy is being violated.
2. The integration allows CA Client Automation to automatically open CA SDM Tickets when a Software Delivery job fails.
3. CA Client Automation discovered asset information is stored in a common asset data model in the MDB for use by multiple CA solutions, including CA SDM, by certifying the Asset and Configuration Item (CI) from CA Client Automation into CA SDM from Asset Search List, Discovered Asset functionality.

## Integration Scenario

---

### Business Challenge

Anita Hirsch, VP of IT services at Forward, Inc., has requested that Don Hailey, the IT manager, coordinate all activities necessary to upgrade all computers in the enterprise that currently have less than 1 GB of RAM. Anita makes this request after analyzing some of the information reported by the CA SDM dashboard with Paul Kim, the IT Director. Both have seen a long list of incidents which are related to slow response time from the recently deployed accounting software. Paul has said that most users run Microsoft Word and Excel simultaneously with the accounting software. The recommended solution from the help desk has been to close some of the open applications. However, the recommendation is having a negative impact on productivity in some of the busiest branches of Forward, Inc. In fact, some customers have already complained about the poor services when requiring quotes or paying bills.

### How the Integration with CA Client Automation Helps Overcome the Challenge

The IT department of Forward, Inc. is responsible for managing complex desktop and server environments during this time of rapid change. The change created an enormous management burden on the IT department. The result is an inconsistent desktop environment that is difficult to maintain and does not align with the business goals. CA advises Forward, Inc. to implement CA Client Automation to have a comprehensive and accurate hardware inventory. The inventory helps them make informed decisions which are based on accurate information about the resources available for the day-to-day operation. Knowing that Forward, Inc. is currently running CA SDM R12.6 in production, CA also advises them to implement the CA Client Automation integration as part of the CA Client Automation R12.5 implementation.

### Configuring a Solution

Susan Jobin, the IT Asset Manager, has done a good job working as a team with other departments to implement CA Client Automation successfully in Forward, Inc. After the implementation, the IT Asset Management department can accurately provide other IT departments with information about available hardware resources. Susan plans to start the second phase of the project, which is to implement the integration between CA SDM and CA Client Automation. The goal of the integration is to create incidents in CA SDM automatically, when one of the software resources does not fit into the standards IT management establishes at Forward, Inc.

## Configuring the Integration from CA SDM r12.6

To configure the integration, perform certain configurations in CA SDM.

### Follow these steps:

1. Log in to CA SDM as an Administrator.
2. On the Service Desk Manager tab, select Search, Contacts.

The Contact Search window opens.

3. In the Last Name field, type *System\_MA\_User* and click search.

The user record with the last name *System\_MA\_User* appears.

4. Verify that *Analyst* appears in the Contact Type column, and *Administrator* appears in the Access Type column.

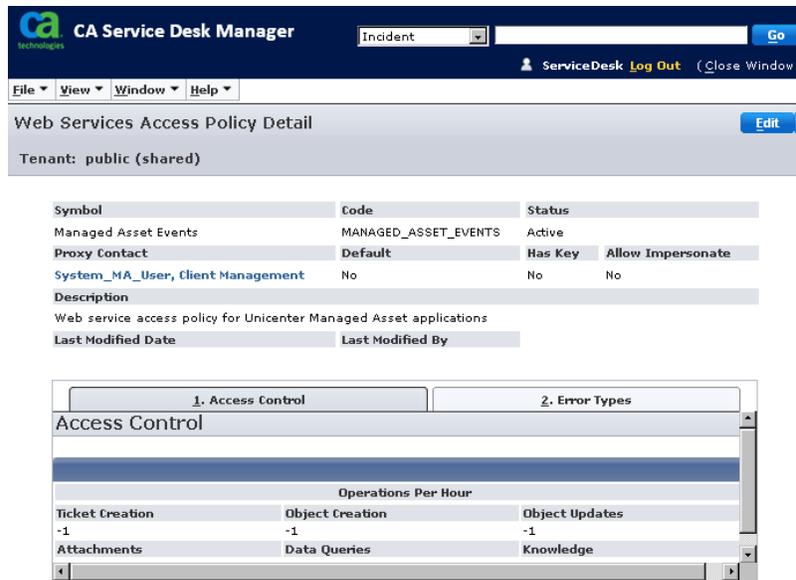
The screenshot shows the CA Service Desk Manager interface. The main content area displays a 'Contact List' table with the following data:

Name	Tenant	Contact Type	Access Type	Contact ID	User ID	Analyst
System_MA_User, Client Management	CA	Analyst	Administration		System_MA_User	

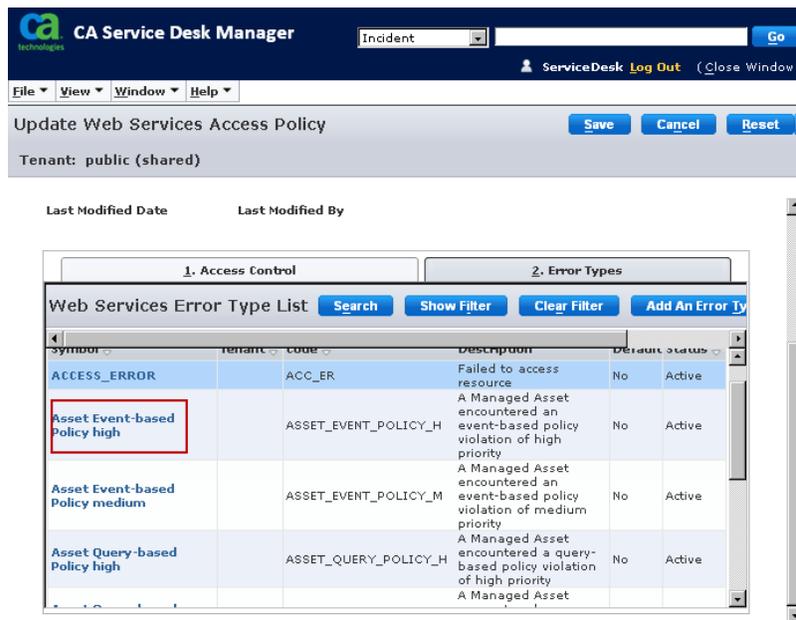
The 'Contact Type' and 'Access Type' columns for the first row are highlighted with a red box.

5. Browse to the CA SDM main window and click the Administrator tab.
6. Review the information on the left and expand the option named Web Serviced Policy.
7. Select the policies of the Web Services Policy node.
8. On the right, click the Managed Asset Events symbol.

The Managed Asset Events window opens.



9. Click Edit.
10. On the edited window, click the Error Types tab.



**Note:** 11 different Error types that can be associated with the Managed Asset Events policy.

11. Click Asset Event-based Policy high.  
The Asset event-based policy window opens.
12. Click Edit. Perform the following steps to modify the policy:

- a. Select the Default check box.
- b. Select Incident in the Ticket template type drop-down list.
- c. Select Asset Event ITIL Policy High in the Ticket template name search field.

**Note:** Information in the templates can be added and modified, and additional templates can be created.

- d. Click the Duplicate handling tab and select Add Activity Log. Make sure not to create a ticket.

The screenshot shows the CA Service Desk Manager interface for configuring a ticket template. The main configuration area is titled "Update Web Services Error Type" and includes fields for "Asset Event-based F", "ASSET\_EVENT\_POLICY\_H", and "Active". The "Default" checkbox is checked. The "Ticket Template Type" is set to "Incident" and the "Ticket Template Name" is "Asset Event ITIL Policy High". The description is "A Managed Asset encountered an event-based policy violation of high priority".

The "Duplicate Handling" section is expanded, showing the following options:

- Create Ticket (do not detect duplicates)
- Add Activity Log (do not create ticket)
- Create Standard Log (do not create ticket)
- Attach As Child (create a child ticket)

The "Maximum time interval for searching duplicates" is set to 24:00:00.

- e. Click Save.

CA SDM is now configured to integrate with CA ITCM.

## Configure the Integration from CA Client Automation R12.5

To complete the integration, configure CA Client Automation.

### Follow these steps:

1. Open the DSM Explorer of the domain manager.
2. Navigate to Control Panel, Configuration, Configuration Policy.
3. Right-click Default Computer Policy and click Un-Seal.
4. Expand the Default Computer Policy and navigate to DSM, Service Desk Integration , and click Default.
5. Decide whether you want to set the logon type to service desk to managed or not managed.

Based on the decision, perform the steps in the following topics:

- a. Configure the System for Managed Logon
- b. Configure the System for Notmanaged Logon

## Configure the System for Notmanaged Logon

1. Verify that the following default values are set; else, double-click the setting to modify the value:

Name	Value
Enabled	True
Identifier Field	summary
Logon Password	<encrypted>
Logon Service Aware Policy	MANAGED_ASSE...
Logon User Name	System_MA_User
Service Desk Endpoint	http://mamsr01-...
Throttling	False
Timeout	120
Type of Logon to Service Desk	notmanaged

- **Enabled:** True
- **Identifier Field:** Summary
- **Logon Password:** Servicedesk
- **Logon Service Aware Policy:** MANAGED\_ASSET\_EVENTS
- **Logon User Name:** System\_MA\_User
- **Service Desk Endpoint:** http://forwardinc:8092/axis/services/USD\_r11\_WebService
- **Throttling:** False
- **Timeout:** 120
- **Type of Logon to ServiceDesk:** notmanaged

Save the settings and seal the policy.

2. Create a Windows user named System\_MA\_User with the following definitions on the CA SDM Server:

- **User Name:** System\_MA\_User
- **Password:** servicedesk

- **User cannot change the password:** Select this check box.
- **Password never expires:** Select this check box.

The notmanaged logon type is configured.

## Configure the System for Managed Logon

### Follow these steps:

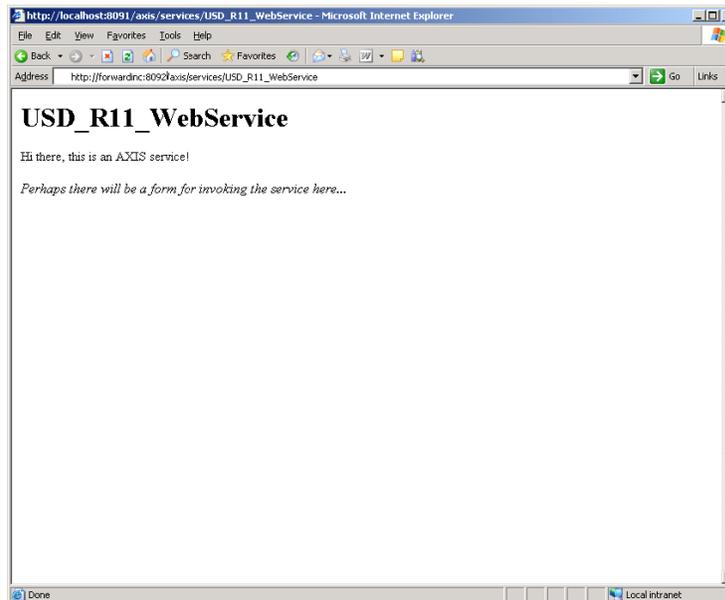
1. Start CA SDM services.
2. Using a command prompt window, run `pdm_pki -pMANAGED_ASSET_EVENTS`.
3. The command creates the `MANAGED_ASSET_EVENTS.p12` file in the current directory. The file contains the password that is equal to the policy name (in this case, `MANAGED_ASSET_EVENTS`). The command also adds the public key of the certificate to the `pub_key` field (`public_key` attribute) in the `sapolicy` table/object.
4. Start the CA SDM web interface and click Administration, Web Services Policies, Policies, and Managed Asset Events.
5. In the policy `MANAGED_ASSET_EVENTS`, insert the Proxy Contact as ServiceDesk and confirm that the `MANAGED_ASSET_EVENTS` policy record has Key as YES.
6. Open DSM Explorer and , verify that the values of the following configuration policies are set as given:
  - **Enable:** True
  - **Identifier Field:** summary
  - **Logon Password:** password for the logon CA SDM webservices
  - **Logon Service Aware Policy:** `MANAGED_ASSET_EVENTS`
  - **Logon User Name:** ServiceDesk
  - **Service Desk Manager endpoint:** `http://<Service Desk Server:Port Number>/axis/services/USD_r11_WebService`
  - **Throttling:** False
  - **Timeout:** 120
  - **Type of Logon to Service Desk Manager:** Managed
7. Copy the `MANAGED_ASSET_EVENTS.p12` file to the `<CA SDM install path>\bopcfg\www\CATALINA_BASE\webapps\axis` directory.
8. On the CA Client Automation computer, use a command prompt window to execute the following command:

```
cacertutil import -i:MANAGED_ASSET_EVENTS.p12 -ip:MANAGED_ASSET_EVENTS  
-t:MANAGED_ASSET_EVENTS
```

9. Return to the Configuration Policy in DSM Explorer and click Seal.
10. Close and open the DSM Explorer.
11. Verify that the CA SDM - Web services functionality is running by entering the following URL in the Internet Explorer browser:

`http://<Service Desk Server:Port Number>/axis/services/USD_R11_WebService`

**Note:** In this URL, change the port number, based on your server information. If the configuration is successful, a window similar to the following sample window opens:



### Testing the Integration

Test the integration to help ensure that the integration is successful. You can test the integration in the following ways:

- Using interactive mode
- Using non-interactive mode

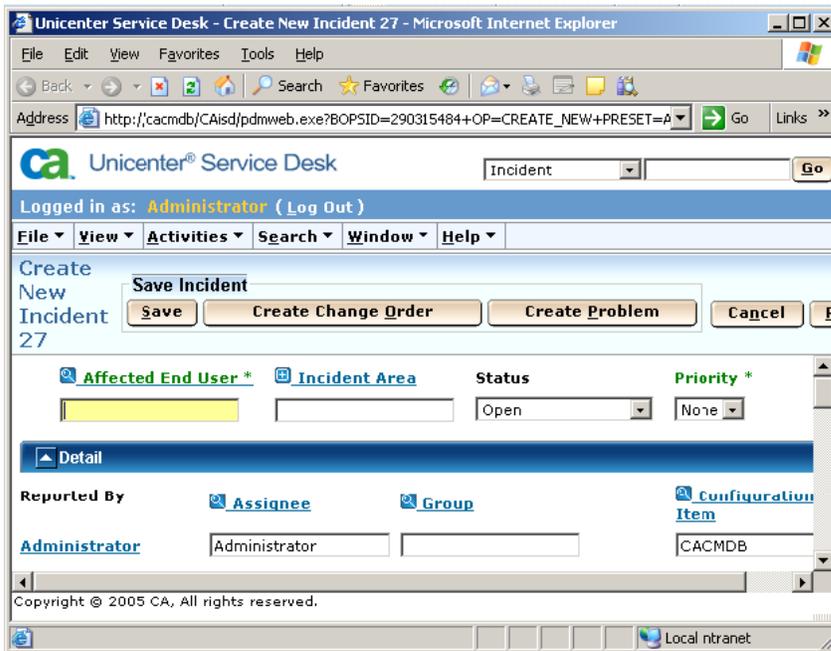
### Test the Integration Using Interactive Mode

You can test the integration in interactive mode from the DSM Explorer.

#### Follow these steps:

1. Open DSM Explorer.
2. Right-click a computer from the list of computers in the domain manager. Select the Create Service Desk Manager ticket option.

If the integration is successful, a new CA SDM Incident window opens. The Asset Management analyst can use the window to create a new incident manually. There is some information already populated (that is, Configuration Item) on the incident detail window. This information is part of the template used. You can add and modify the information, if necessary, as shown in the following screenshot:.



The integration testing is complete.

## Test the Integration using Non-Interactive Mode

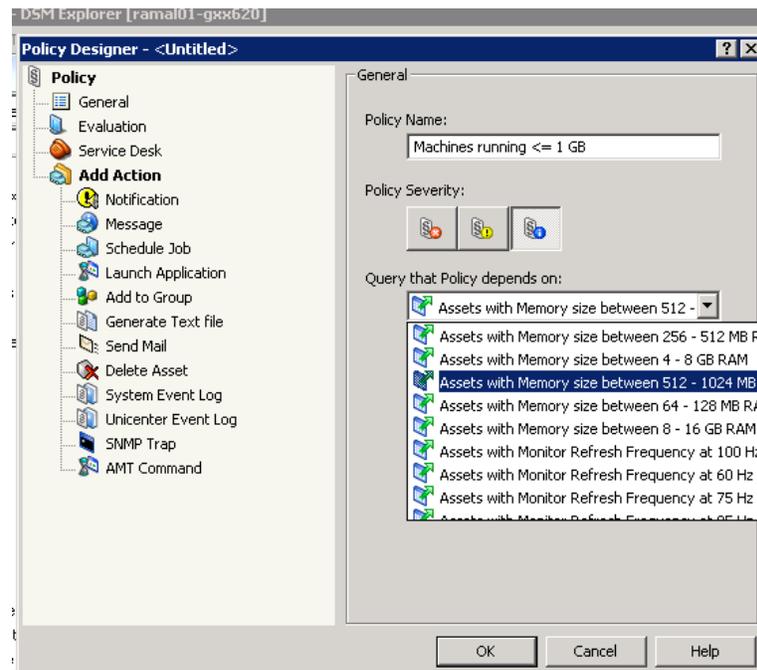
You can configure CA Client Automation event policies, to open and update tickets (Incident, Change Order, Problem, and Request) in CA SDM. When an event policy is violated, a new ticket is created, or an activity log can be added to an existing ticket.

### Follow these steps:

1. From the DSM explorer, navigate to Policies, Query Based.
2. Right-click Query Based folder and select New.

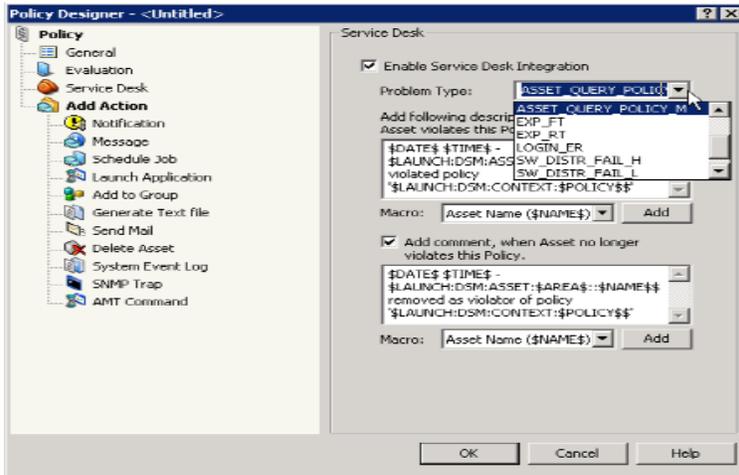
The Policy Designer dialog opens.

3. Complete the following fields:
  - a. In the Policy Name field, enter *Machines running <= 1 GB*.
  - b. In the Query that policy depends on field, select the query named *Assets with Memory Size between 512 and 1024 MB RAM*.
  - c. Click alert in the Policy Severity field (first icon from left to right).



4. From the left side of the Policy designer, click Service Desk Manager. Complete the following fields:
  - a. Select the Enable Service Desk Manager Integration check box.

- b. In the problem type drop-down list, select ASSET\_EVENT\_POLICY\_HIGH and click OK.



5. Expand Policies, Query Based, select the policy named Machines running <= 1 GB, right-click the policy, and choose Evaluate Now.

The right pane displays the computers that have the RAM size which is equal to or less than 1 GB.

6. In the Information pane, click Related CA SDM Ticket.

The Service Desk Manager Request List window opens, listing the incidents created for the computers that violated the policy. As a result, CA SDM users can now request memory for the computers that are part of the incident and are being recognized as those computers not following Forward, Inc. standards. The non-interactive integration testing is complete.

## Integration Summary

---

The integration of CA Client Automation with CA SDM makes CA Client Automation a service-aware solution. This means that CA Client Automation can trigger the creation of CA SDM tickets based on certain events occurring with its managed assets.

Ticket creation in CA SDM is controlled by the Service Aware policy named ManagedAssetEvents. The Service Aware policy is automatically installed when CA SDM is installed. CA Client Automation uses a set of problem types available with the Service Aware policy to categorize the problem and to address the type of ticket to be created.

CA Client Automation and CA SDM provide an interface that allows each product to be started in-context from the other product.

- CA Client Automation can automatically create tickets in CA SDM from a query or event policy, when those policies are violated.
- CA Client Automation Software Delivery integrates with CA SDM only through policies. A ticket can automatically be raised for a failed Software Delivery job.
- CA Client Automation creates tickets in the context of discovered assets, for example, computers or users. When a ticket is created, a discovered asset is mapped to an owned asset, which is known in CA SDM. This allows CA SDM Administrators to browse and report on relationships between tickets and owned assets.

Assets that have been discovered by CA Client Automation, that CA SDM is not aware of, can be certified as a CA SDM owned resource from the search Asset List window, Discovered Asset functionality.



# Chapter 5: CA Patch Manager

## CA Patch Manager Integration

### Integration Details

---

CA Patch Manager lets you configure the creation of CA SDM Change Orders for managing patch life cycles. The CA SDM installation provides a web services interface that enables CA Patch Manager to integrate with CA SDM. On enabling integration, all patch processes falling into the CA Patch Manager workflow attempt to create a change order with the configured CA SDM server based on the specified template. The change order which is created contains the summary and description of the patch.

**Note:** CA Patch Manager workflow is a component specific to CA Patch Manager, and is not related to the CA SDM Workflow IDE.

#### Integration Points from CA SDM to CA Patch Manager

The following is the integration point from CA SDM to CA Patch Manager:

- Change the status of the patch in CA Patch Management once a work flow task activity has been accepted or approved in CA SDM.

#### Integration Points from CA Patch Manager to CA SDM

The following is the integration point from CA Patch Manager to CA SDM:

- Configure the automatic creation CA SDM change orders when a patch enters one of the following states in CA Patch Manager:
  - Acceptance
  - Deferral
  - Approval
  - Deployment

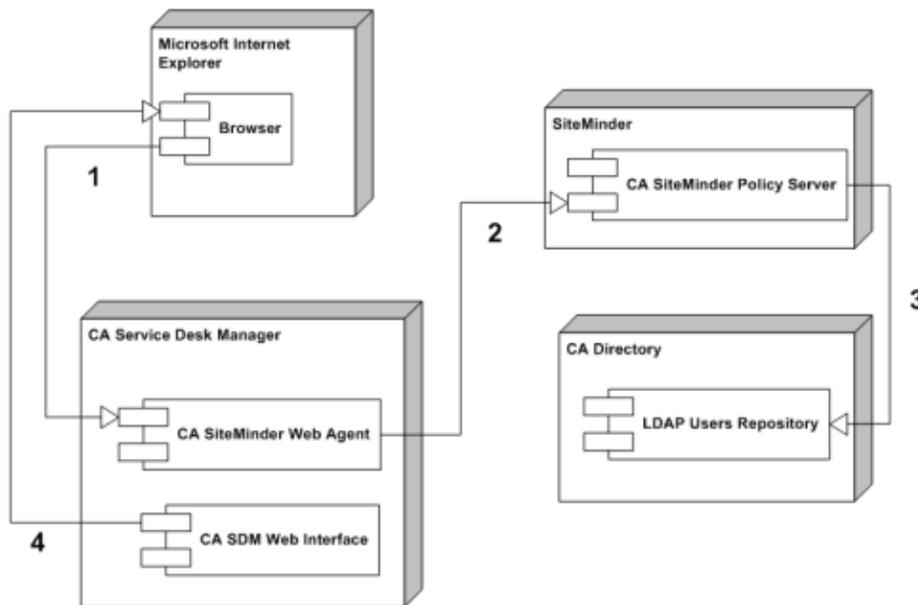
## Integration Value

The CA Patch Manager integration provides the following values:

- Automatic change order creation for patches as they become available.
- Consistent approval process for the changes.
- Complete management of the patch process from approval through testing, and finally deployment.
- Automatic notification to the CA SDM administrators that a patch has already been deployed, or will be deployed. This helps in anticipating the workload of CA SDM analysts.
- The automatically updating Configuration Items from the point of view of the patches.

## How the Integration Works

The following diagram illustrates how the integration between CA Patch Manager and CA SDM works:



The integration between CA Patch Manager and CA SDM works as follows:

1. CA Patch Manager provides a built-in functionality that provides the ability to create a change order in CA SDM automatically, when a patch enters an enabled workflow state. This integration requires a valid CA SDM server name, username/password to connect to the CA SDM server, and issue templates.
2. The CA SDM Change Order in turn has workflow capabilities that, for example, can enable CA SDM to interact with CA Patch Manager workflow using remote references functionality. This functionality helps manage the status of the patch in the promotion life cycle in CA Patch Manager.

## Integration Example

---

### Business Challenge

The Forward, Inc. HR representative, June Arnold, is attempting to submit her expense report in the new Expenses product developed in-house. June has encountered an error in the software, and an incident has automatically been opened in CA SDM using the integration between the Expenses product and CA SDM. Forward Inc. implemented the integration with the objective of making CA SDM aware of the potential errors that users encounter in the most commonly used products in the organization.

Donald Bell, first-level support at the Forward, Inc help desk, researched the incident in the CA SDM Knowledge Tools documents. He concluded that a required patch is needed on the Expenses product running on June's computer. Donald knows that, to apply fixes, the Change Management department must provide an authorization. However, Donald is not familiar with the official policy and procedure, and he also does not know who else may be running the Expenses product. Donald only knows that the product was installed on more than 300 computers across the organization three weeks ago.

### CA Approach

Keeping all software in an organization controlled and updated can be difficult and expensive. The software delivery and CA Patch Manager components that are part of CA ITCM, can automate the identification, gathering, packaging, deployment, and ongoing validation of patches. These components also help manage related software configuration changes throughout your enterprise.

## Configuring a Solution

Susan Jobin, the IT Asset Manager, is responsible for coordinating all the necessary resources and activities to automate the software update procedure in Forward, Inc's Configuration Items (CI). Part of the solution is that an incident must trigger the software update and change procedure. To implement the solution, set up the integration between CA SDM and CA Patch Manager.

## Configure the Integration from CA SDM

To configure the integration, complete the following steps in CA SDM.

**Note:** As previously mentioned, create Change Order Templates for each status selected in the UPM Administration tab. Verify that the templates have already been created.

### Follow these steps:

1. Log in to CA SDM as an Administrator.
2. Create a capminteg.bat file in any directory. In this example, the file is created directly in the c:\ directory.
3. Copy the following command to the capminteg.bat file:

```
java -Djava.class.path="C:\Program Files\CA\CA Patch Management\bin\event.jar"  
com.ca.CA.upm.eventmanager.UPMEMSack  
"http://bsodsmv1:8090/upm/services/UPMEMS" %1 true
```

4. Create a remote reference using the following steps:

From the main CA SDM window, click the Administration tab and select Servicedesk, Application Data, Remote References.

Click Create New in the left side of the window.

Complete the fields in the Create New Remote Reference window as shown in the following screenshot:

## Integration Example

The screenshot shows the CA Service Desk Administration console. At the top, there is a header with the CA Technologies logo, the text 'CA Service Desk', a search bar containing 'Incident', and a 'Go' button. Below the header is a navigation menu with 'File', 'View', 'Window', and 'Help' options. The main content area is titled 'Create New Remote Reference' and contains several input fields and buttons. The 'Symbol \*' field contains 'CAPM', the 'Code \*' field contains 'CAPMINTEG', and the 'Record Status \*' dropdown is set to 'Active'. There is a 'Spelling' button next to the 'Description' field, which contains 'CAPMINTEG'. The 'Function Access' field is empty, and the 'Architecture Type \*' dropdown is set to 'all'. The 'NT Server, Unix Server, or Unix Client Exec Command' field contains 'C:\\CAPMINTEG.Bat'. At the bottom, the 'Last Modified Date' and 'Last Modified By' fields are empty, with 'ServiceDesk' listed as the user.

5. From the main CA SDM window, click the Administration tab, Events and Macros, Macros.
6. Create a new macro to call the remote reference that you previously created.
  - **Object Type:** workflow task
  - **Macro Type:** execute remote reference

The screenshot shows the 'Create New Macro' form in CA Service Desk Manager. The form is titled 'Create New Macro CAPM' and includes buttons for 'Save', 'Cancel', and 'Reset'. The 'Tenant (T)' dropdown is set to '<empty>'. The 'Symbol \*' field contains 'CAPM' and the 'Record Status \*' dropdown is set to 'Active'. The 'Macro Description' field is empty, with a 'Spelling' button next to it. The 'Object Type' is 'Workflow Task' and the 'Macro Type' is 'Execute Remote Reference'. The 'Last Modified Date' and 'Last Modified By' fields are empty, with 'ServiceDesk' listed as the user. A preview window at the bottom shows a 'Remote Reference' step with the symbol 'CAPM'.

7. Create a new change order category.

**Example:** *Change.IT.Workstation.Config.*

8. Add a work flow task named *approval*, and in the task behavior for the approve status, add the macro previously created in step 5 as the action on true.

## Create Change Order Template in CA SDM

A CA SDM Change Order template is a Change Order model that is used when creating new Change Orders. Create a Change Order Templates for each status selected in the UPM Administration tab.

### Follow these steps:

1. Log in to CA SDM as an Administrator or Analyst.
2. Click the Service Desk Manager tab and choose File, New Change Order.
3. Enter the information for the new change order.

The screenshot shows the 'Save Change Order' dialog in CA Service Desk Manager. The title bar reads 'CA Service Desk Manager' and 'Change Order'. Below the title bar is a menu bar with 'File', 'View', 'Activities', 'Search', 'Window', and 'Help'. The main area contains the text 'Create New Change Order 28' and a 'Save Change Order' button. Below this are several input fields: 'Requester \* (T)' with the value 'System\_MA\_User, C', 'Affected End User \* (T)' with the value 'System\_MA\_User, C', 'Category (TO)', 'Status \* (TO)' with the value 'RFC', 'Priority \*' with the value '3', and 'Type' with the value 'Normal'. There is also a 'Detail' section with fields for 'Root Cause (TO)', 'Organization (TO)', 'Project (TO)', and 'Closure Code (TO)'. The 'External System Ticket' field is also visible.

4. Click the Template tab in the Change Order Detail window.
5. In the Template Name field, enter a name for the template.

The screenshot shows the 'Template' dialog in CA Service Desk Manager. The title bar reads '06/30/2011 03:11 pm'. Below the title bar is a menu bar with '1. Related Tickets', '2. Additional Information', and '3. Logs'. The main area contains the text 'Specify a template name to convert this change into a template'. Below this are several input fields: 'Template Name' with the value 'UPM\_Patch\_Acceptor', 'Template Class', and 'Template Active \*' with the value 'Active'. There is also a 'Description' field with a 'Spelling(\$)' button.

6. Click Save.

The change order template is created.

## Configure the Integration from CA Patch Manager

### Follow these steps:

1. From the Start menu, select Programs, CA, CA Patch Manager, Deploy Workflow Integration.

A command prompt opens. The CA Patch Manager Workflow gets activated, and the process runs in the background. When the process is complete, the command prompt closes.

```

Deploy Workflow Integration
ketFactory.java:120)
  at org.apache.axis.transport.http.HTTPSender.getSocket(HTTPSender.java:1
91)
  at org.apache.axis.transport.http.HTTPSender.writeToSocket(HTTPSender.ja
va:404)
  at org.apache.axis.transport.http.HTTPSender.invoke(HTTPSender.java:138)
  at org.apache.axis.strategies.InvocationStrategy.visit(InvocationStrateg
y.java:32)
  at org.apache.axis.SimpleChain.doVisiting(SimpleChain.java:118)
  at org.apache.axis.SimpleChain.invoke(SimpleChain.java:83)
  at org.apache.axis.client.AxisClient.invoke(AxisClient.java:165)
  at org.apache.axis.client.Call.invokeEngine(Call.java:2784)
  at org.apache.axis.client.Call.invoke(Call.java:2767)
  at org.apache.axis.client.Call.invoke(Call.java:1792)
  at org.apache.axis.client.AdminClient.process(AdminClient.java:439)
  at org.apache.axis.client.AdminClient.process(AdminClient.java:404)
  at org.apache.axis.client.AdminClient.process(AdminClient.java:410)
  at org.apache.axis.client.AdminClient.process(AdminClient.java:320)
  at org.apache.axis.client.AdminClient.main(AdminClient.java:463)

<http://xml.apache.org/axis/>hostname:ramal01-gxx620
Workflow Management WebServices deployment completed
Press any key to continue . . .

```

**Note:** CA Patch Manager workflow is a component unique to CA Patch Manager. It is not a component of the CA SDM Workflow IDE.

2. Log in to CA Patch Manager as an Administrator.
3. Click the Administration tab.
4. On the left side of the window, click Events.

On the right side of the window, the configuration window opens.

5. Enter the following information for the configuration fields in the window named Service Desk Manager:

- a. Web Services URL:

`http://SDM_Server_Name:8080/axis/services/USD_WebServiceSoap`

CA Patch Manager is compatible with USPSD 6.0 R11, and R12.x web services. However, the versions offer different web service URL strings. CA SDM 6.0 implements a .NET web service, with the following default URL:

`http://<USPSDServerAddress>:80/USD_WS/usd_ws.asmx`

CA SDM R11 offers two web services. CA Patch Manager only integrates with the R12 web service that is backward-compatible with USPSD 6.0 web service clients. The following is the default, backward-compatible web service URL for R12:

http://<Service Desk Server Address>:8080/axis/services/USD\_WebServiceSoap

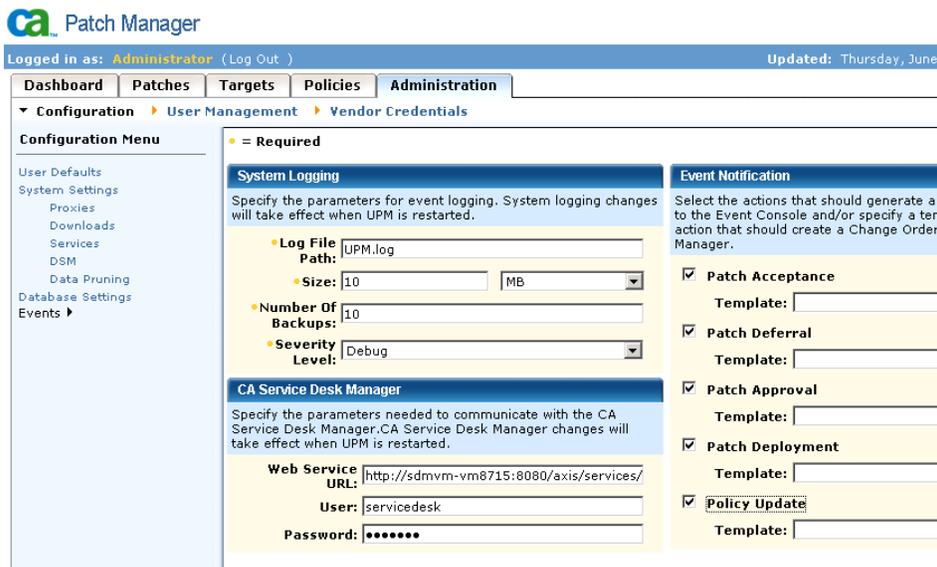
b. User: ServiceDesk

c. Password: Enter the password of the ServiceDesk user.

**Note:** As a best practice, replace the CA SDM user with a different user (that is, System\_UPM\_generated). This name is used when configuring CA Patch Manager. This user must exist in CA SDM and the Access type must be Analyst.

- On the External Event Confirmation window, select the Patch Acceptance, Patch Deferral, Patch Approval, Patch Deployment, and Policy Update check boxes. Select the change order templates for each event. For more information about creating change order templates, see [Create Change Order Template in CA SDM](#) (see page 94).

**Note:** For each option you select in this step, you must have already created a Change Order Template in CA SDM.



The configuration of the integration is complete.

## Testing the Integration

To verify that the integration is working correctly, follow these steps:

1. Log in to CA Patch Management.
2. From the Dashboard tab, click one of the patches in the left side window named Patches Pending Acceptance.

If the integration is successful, a new change order is created in CA SDM, as illustrated in the following sample window. The description contains all the information defined in CA Patch Manager for the patch, as well as the Status based on the Workflow functionality active in CA Patch Manager.

The screenshot displays the '679 Change Detail' window in the Unicenter Service Desk. The interface includes a navigation menu with options like 'File', 'View', 'Activities', 'Actions', 'Search', 'Reports', 'Window', and 'Help'. The main content area shows the following details:

Requester	Affected End User	Category	Status	Priority
ServiceDesk	ServiceDesk	Change.IT.Workstation.Config	RFC	2-Med-High

Below this table, there are sections for 'Detail', 'Summary Information', and 'Order Description'. The 'Order Description' section contains the following text:

Workflow 8e6581d5-cc23-03db-e432-96c7ca6e99fb - Patch CA - Windows 2003 Post Gold EN 32Bit x86 - FULL Security Rollup v0702.00 has entered Unicenter Patch Management Workflow

Workflow {dcb1a7e8-bf63-4491-9a46-edbf1f98b88d} status changed from STATUS\_PENDING\_USER\_ACCEPTANCE to STATUS\_PENDING\_WORKFLOW\_ACCEPTANCE. Approval will set the Patch to STATUS\_ACCEPTED. Rejection will set the Patch to STATUS\_PENDING\_USER\_ACCEPTANCE. null

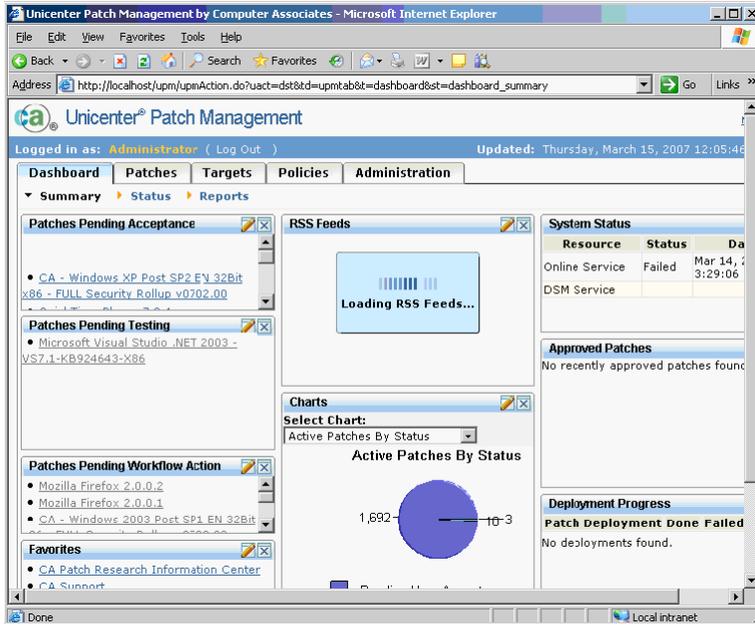
Open Date	Actual Start Date	Resolve Date	Close Date	Change Start Date...	Change End Date...
03/06/2007 03:45 pm	03/06/2007 03:45 pm				

At the bottom, there are checkboxes for 'Mainframe Changes?', 'Distributed Changes?', 'Enterprise Changes?', and 'Project Management?'.

After the Change order approval task has been approved, the status of the patch will change from Pending Acceptance to Patches Pending Testing in the CA Patch Manager Dashboard.

**Note:** The CA SDM administrator can complete the steps described in Configuring the Integration from CA SDM for other statuses in the CA Patch Management work flow. You can add more CA SDM workflow tasks to start remote references with the proper line to update CA Patch Manager work flow status.

# Integration Example



## Integration Summary

---

The integration of CA Client Automation with CA SDM makes CA Client Automation a service-aware solution. This means that CA Client Automation can trigger the creation of CA SDM tickets based on certain events occurring with its managed assets.

Ticket creation in CA SDM is controlled by the Service Aware policy named ManagedAssetEvents. The Service Aware policy is automatically installed when CA SDM is installed. CA Client Automation uses a set of problem types available with the Service Aware policy to categorize the problem and to address the type of ticket to be created.

CA Client Automation and CA SDM provide an interface that allows each product to be started in-context from the other product.

- CA Client Automation can automatically create tickets in CA SDM from a query or event policy, when those policies are violated.
- CA Client Automation- Software Delivery integrates with CA SDM only through policies. A ticket can automatically be raised for a failed Software Delivery job.
- CA Client Automation creates tickets in the context of discovered assets, for example, computers or users. When a ticket is created, a discovered asset is mapped to an owned asset, which is known in CA SDM. This allows CA SDM Administrators to browse and report on relationships between tickets and owned assets.
- CA SDM provides the ability to enable a web services interface for remote administration. CA Patch Management takes advantage of these web services, giving CA Patch Management Administrators the ability to create CA SDM Change orders for patch work flow management. CA SDM can also execute a set of remote references to complete the patch life cycle in both CA SDM and CA Patch Management. This capability allows Change Management departments to control and track all software updates inside the organization.
- Assets that have been discovered by CA Client Automation, that CA SDM is not aware of, can be certified as a CA SDM owned resource from the search Asset List window, Discovered Asset functionality.



# Chapter 6: CA Configuration Automation

## CA Configuration Automation Integration

---

This chapter discusses how CA SDM r12.6 and CA Configuration Automation r5.0 SP1 can be configured to work together. The following key topics are covered:

- Integration points and functionality from CA SDM
- Integration points and value from CA Configuration Automation to CA SDM
- How the integration works
- Integration instructions

The chapter includes procedures for reconciling CIs and relationships to avoid having duplicates, and also touches upon configuring SSL to communicate with a secure CA SDM server.

## What is CA Configuration Automation

---

CA Configuration Automation is a suite of products that lets you manage the distributed hardware and software services in your environment from a centralized browser-based UI.

CA Configuration Automation provides application-level best practices for managing change, configuration and compliance. You can discover and manage components of your enterprise at the network, server, service and software level.

Cohesion ACM is used to populate CA SDM automatically and maintain CA SDM with accurate CI attributes and relationship information.

CA Configuration Automation performs the following core operations:

- **Discovery:** CA Configuration Automation Discovers the Server and Devices in the enterprise. Discovers Software Applications extensively by discovering application components across servers and networks. The Discovery includes Directory, Files, Registry Entries, Database Tables and Configuration Parameters.
- **Monitor:** CA Configuration Automation can detect change in a Software Component and Server configuration by monitoring your enterprise through snapshots.
- **Change Detection:** The comprehensive Change Detection features provide the ability to compare the state of an application across time or to a similar application on another server. The comparison and monitoring capabilities of CA Configuration Automation, let you have an overall view of your enterprise across time and examine changes at any point in any network, server, or application.
- **Audit:** CA Configuration Automation helps control applications and establishes best practices with flexible, in-depth policy definition and automated enforcement of the rules you define. Auditing the performance configurations, security settings, and dependent variables of your enterprise hardens the application infrastructure, freeing organizations from manual, error prone reviews.
- **Report:** CA Configuration Automation schedules formal application infrastructure reports and sends out on demand notifications by email and SNMP to keep you informed of changes and policy violations. You can customize the provided base report templates to select columns, filters, and targets of the reports to ensure that the right parties get the information required for critical decisions.

The CA Configuration Automation solution is comprised of three components:

- **CA Configuration Automation Server:** CA Configuration Automation Server provides a browser-based user interface acting as a central register. Through this interface you can manage persistent storage and communication with the CA Configuration Automation Agents, and also control data access.
- **CA Configuration Automation Database:** CA Configuration Automation Database stores all the collected CA Configuration Automation data and configuration information.
- **CA Configuration Automation Agent:** CA Configuration Automation Agent is a light-weight executable that inspects and implements server-directed operations on software components running on CA Configuration Automation-managed servers in the Enterprise. Each time CA Configuration Automation Agent interrogates the managed servers, the newly collected data overwrites the previous service data stored in the CA Configuration Automation Database.

## Integration Details

---

### Integration Points and Functionality from CA SDM

One of the integration features between CA SDM r12.6 and CA Configuration Automation 5.0 SP1 is the ability to launch the CA Configuration Automation interface from a CI in CA SDM to view additional details on that CI.

**Note:** As CA Configuration Automation does not support a unique federated asset ID for NIC or File System CIs, it also does not support MDR Launcher for NIC or File System CIs. Therefore, a CA Configuration Automation-based NIC or a File System CI does not display an MDR launch button even if it was imported successfully.

### Integration Points and Functionality from CA Configuration Automation

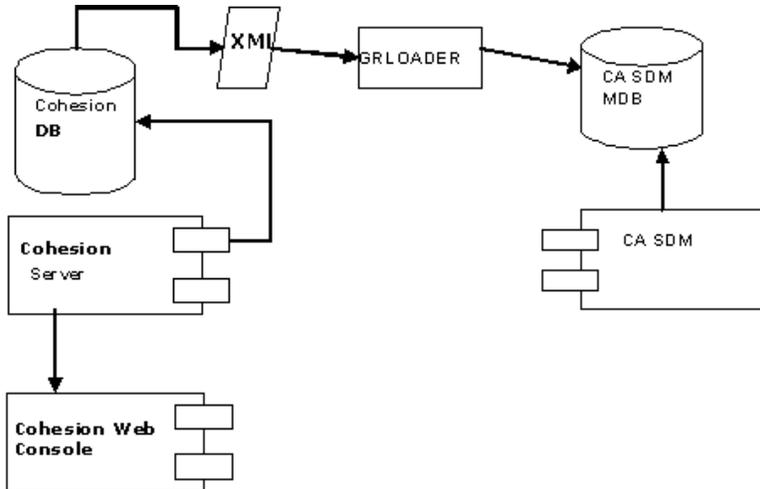
Integrating CA Configuration Automation with CA SDM makes the following functionalities available:

- Import the CI details and relationships into CA SDM.
- Ability to launch CA Configuration Automation details to view details of discovered CI attributes through the MDR launcher.
- Refreshing CI details which is useful in confirming a change to the infrastructure.

CA Configuration Automation detects changes from a baseline or Gold standard configuration, across applications and servers, which supports change and configuration managements efforts.

## How the Integration Works

The following diagram illustrates how the integration between CA Configuration Automation and CA SDM works:



The integration between CA Configuration Automation and CA SDM works as follows:

- Integration between these solutions is provided out of the box. CA Configuration Automation performs discovery and provides data which is used to define CIs and their attributes in CA SDM.
- CA Configuration Automation uses both the agent and agent-less discovery techniques to discover servers, software components and the relationships automatically. CI data and relationship details are exported to the CA SDM repository On Demand or at scheduled intervals through an XML formatted flat file. This file is then fed into the GRLoader program to populate CA SDM.
- A federation link is maintained between the CI that is created in CA SDM and the source discovery application, which is CA Configuration Automation in this case. Maintaining this link enables you to launch back into the CA Configuration Automation UI from the CA SDM UI in the context of a particular CI. From there, you can view additional CI details that are only stored in CA Configuration Automation.

The Mapping of CI attributes between CA Configuration Automation and CA SDM is controlled by a mapping xml file called "*cldb\_mapping.xml*" file, whose default location is in the "C:\Program Files\CA\Cohesion\Server\server\webapps\cohesion\WEB-INF\classes" directory.

*Cldb\_mapping.xml* enables CA SDM users to customize the mapping of Cohesion CIs and their attributes so they match the structure of SDM CIs when exported to CA SDM.

The Cohesion CA CMDB Export report uses the contents of the `cmdb_mapping.xml` file. The Cohesion CA CMDB Export report is the mechanism by which CA Configuration Automation exports CI data to CA CMDB to determine the Cohesion CIs, attributes, and relationships to be exported and how to map them to CA CMDB families, classes, attributes, and relationships. A CMDB Export report the mechanism by which CA Configuration Automation exports CI data to CA CMDB.

### Prerequisites for Integration

The following are the prerequisites for the integration:

- CA SDM r12.6 and CA Configuration Automation 5.0 SP1 must have been installed and working in the environment. For more information on installing and configuring these applications, see the respective product documentation.
- CA Configuration Automation discovery must be available in the environment. CA Configuration Automation is required for modifying the `cmdb_mapping.xml` file and importing CI data into CA SDM.

Review Appendix C in the *CA Configuration Automation Implementation Guide* and make a backup copy of the default `cmdb_mapping.xml` file. By default, the file is located in the following locations:

- `\Program Files\CA\Cohesion\Server\server\webapps\cohesion\WEB-INF\classes` (Windows)
- `/opt/CA/Cohesion/Server/server/webapps/cohesion/WEB-INF/classes` (UNIX or Linux)

Review Chapter 7 in the *CA Configuration Automation Implementation Guide*. Follow the instruction to configure CA Configuration Automation user authentication in the section titled Integrating CA Configuration Automation with Other Applications.

- For CA Configuration Automation 5.0 SP1 Windows servers, we recommend that you apply the following patches available on <http://support.ca.com> in the following order:
  - RO13251 (Windows): WIN-CMDB TWA COMPATIBILITY AND FIXES Integration Example
  - RO13250 (Windows): WIN-SERVER RELATIONSHIPS IN CMDB EXPORT REPORT

### Configure the Integration from CA SDM

The integration of CA Configuration Automation and CA SDM provides the ability to launch the CA Configuration Automation interface from a CI in CA SDM to view additional details of the CI.

**Note:** As CA Configuration Automation does not support a unique federated asset ID for NIC or File System CIs, CA Configuration Automation does not support launching the MDR for NIC or File System CIs. Therefore, a Cohesion-based NIC or a File System CI does not display the MDR launch button even if it was imported successfully.

## Define CA Configuration Automation as a MDR Provider

### Follow these steps:

1. Log in to the CA SDM UI and click the Administration tab.
2. Navigate to CA CMDB, MDR Management, MDR List.
3. Click Create New.
4. Enter the following details:
  - a. **Button Name:** The button label that appears on the CI Detail page For example, Cohesion
  - b. **MDR Name:** The MDR name that must match the `com.cendura.installation.name` parameter in the `cendura.properties` file. The default location of the properties file is "`C:\Program Files\CA\Cohesion\Server\lib`"
  - c. **MDR Class:** COHESION
  - d. **Owner:** Administrator. This is the CA SDM contact that is responsible for this MDR
  - e. **Hostname:** The hostname of the Cohesion server
  - f. **Port:** The Cohesion port number. Example: 8091
  - g. **Path:** Retain the default value
  - h. **Parameters:** Retain the default value
  - i. **Userid:** The CA Configuration Automation user ID with at least the Specialist role. Example: Sdmin
  - j. **Shared Secret:** The secret password which you defined for the `com.cendura.security.oneclickauth.secret` parameter in the `cendura.properties` file. The following is a snippet from the `cendura.properties` file:

```
# -- Configure One-Click Authentication --
com.cendura.security.oneclickauth.secret=sdmin
com.cendura.security.oneclickauth.scheme=
com.cendura.security.oneclickauth.user=SDMAdmin
```

- a. **CMDBf Timeout:** Retain the default value
- b. **CMDBf Namespace:** Retain the default value
- c. **URL to Launch in Context:** Retain the default value
- d. **CMDBf Endpoint:** Retain the default value

The following screenshot shows the new MDR definition with all the CA Configuration Automation properties set:

**CA Service Desk Manager**

Incident

ServiceDesk  (Close Window)

File View Window Help

Create New MDR Definition

Button Name *	MDR Name *	MDR Class	Active? *	Owner
Cohesion	cohvm-vm2011	Cohesion	Active	ServiceDesk

Description

Hostname	Port	Path	Parameters
cohvm-vm2011	8080	CAisd/html/cmdb_coh	hostname={hostname}+port={port}+family={family}+name={
Userid	Shared Secret	CMDBf Timeout	CMDBf Namespace
sdmadmin	sdmadmin	10	

URL to launch in Context

http://sdmvm-vm2011:8080/{path}?{parameters}

CMDBf Endpoint

5. Verify that the Userid you specified is available in CA SCM.
  - a. Log in to the CA Cohesion ACM Administration UI
  - b. Click the Users tab and verify that the user name exists.

The following screen shot shows the existence of the SDMAdmin user, which is used as the userID in this example.

**CA Cohesion® Application Configuration Manager**

User: admin

Help ?

**User Management**

Users Directory Groups Roles Server Access Control

Other Actions

0 Rows selected (3 total) View Option: Default View By: All Name: All

Full Name	User ID	Status	Role	Email	Current User	Creation Date
Admin External User	admin	Active	Administrator		<input checked="" type="checkbox"/>	
Sync Master	SyncMaster	Active	Administrator		<input type="checkbox"/>	
SDMAdmin	SDMAdmin	Active	Specialist		<input type="checkbox"/>	06/01/2011 16:13:07 EDT

User

Full Name: Admin External User Role: Administrator

User ID: admin

Status: Active

Email:

Creation Date:

CA SDM is now configured to integrate with CA Configuration Automation.

## Configure the Integration from CA Configuration Automation

CA Configuration Automation provides predefined report templates. The CA CMDB Export report template is used to import CA Configuration Automation data into CA SDM. The report includes the CIs that CA Configuration Automation has discovered and their respective relationships. The report generates an HTML or XML format, which is then exported as Configuration Items (CIs) into an XML file. The GRloader then reads the XML file, and imports the CIs to an instance of CA SDM.

### Consideration for Exporting the CIs

Consider the following points before performing the export operation:

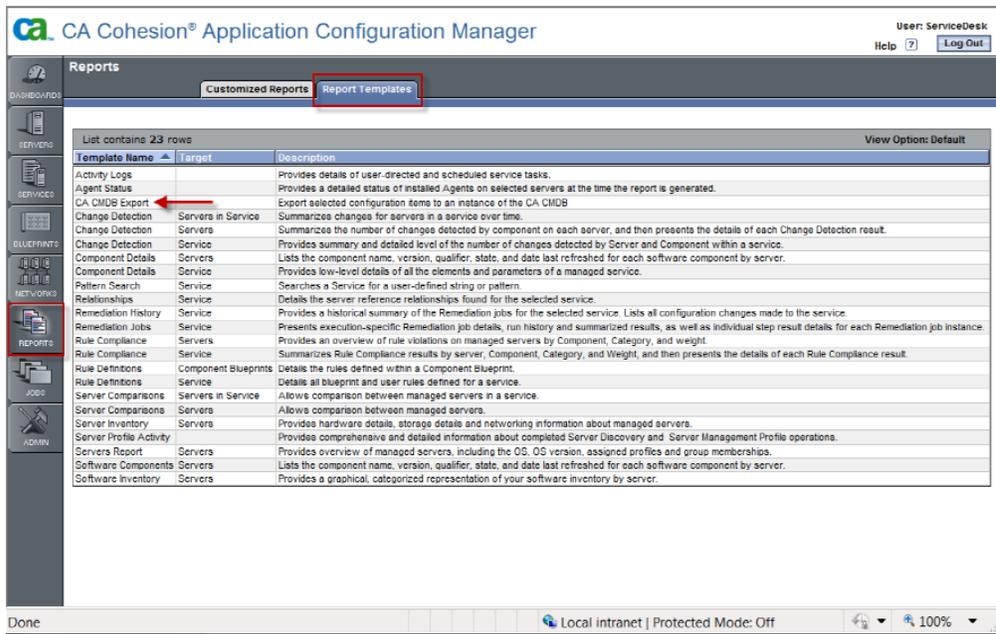
- Servers which are discovered by a Network Discovery operation are stored in the server table using the fully qualified domain name. For example, factotum.abc.com.
- The CMDB Export Report uses the short name derived from the HostName parameter. The HostName parameter is obtained only after a server state is set to Managed and a Server Discovery Profile is run. For example, if the Network Discovery operation discovered a server called factotum.abc.com, the CMDB Export Report will use factotum as the managed server name that is mapped to the CMDB CI name after a Server Discovery Profile is run.
- If you run the CMDB Export Report against unmanaged servers which have never had a Discovery Profile run against them, it will not export these servers because they do not have a short name or a HostName value.
- If you run the CMDB Export Report against managed servers that have not had a Discovery Profile run at least once, it will not export these servers.
- The mapping of Cohesion CIs and their attributes are available in the cmdb\_mapping.xml. We recommend that you customize this file to help ensure that you have more accurate mapping and thus avoiding duplicate CIs. For more information about customizing the file, see [Tips for Modifying the CMDB Attribute Mapping Section](#) (see page 130) in this chapter.

Also review Appendix C in the *CA Configuration Automation Implementation Guide* and make a backup copy of the default cmdb\_mapping.xml file. Review Chapter 7 in the *CA Configuration Automation Implementation Guide*. Follow the instruction to configure CA Configuration Automation user authentication in the section titled Integrating CA Configuration Automation with Other Applications.

## Save a CA CMDB Export Report

### Follow these steps:

1. Log in to the CA Configuration Automation web interface using a user ID that has permission to modify/execute reports. A user ID with Super User, Operator, and Specialist role has full rights to Reports.
2. Click Reports in the navigation menu and then click the Report Templates tab as shown in the following screenshot:



3. Click CA CMDB Export template.

The Run or Save Report dialog is displayed.

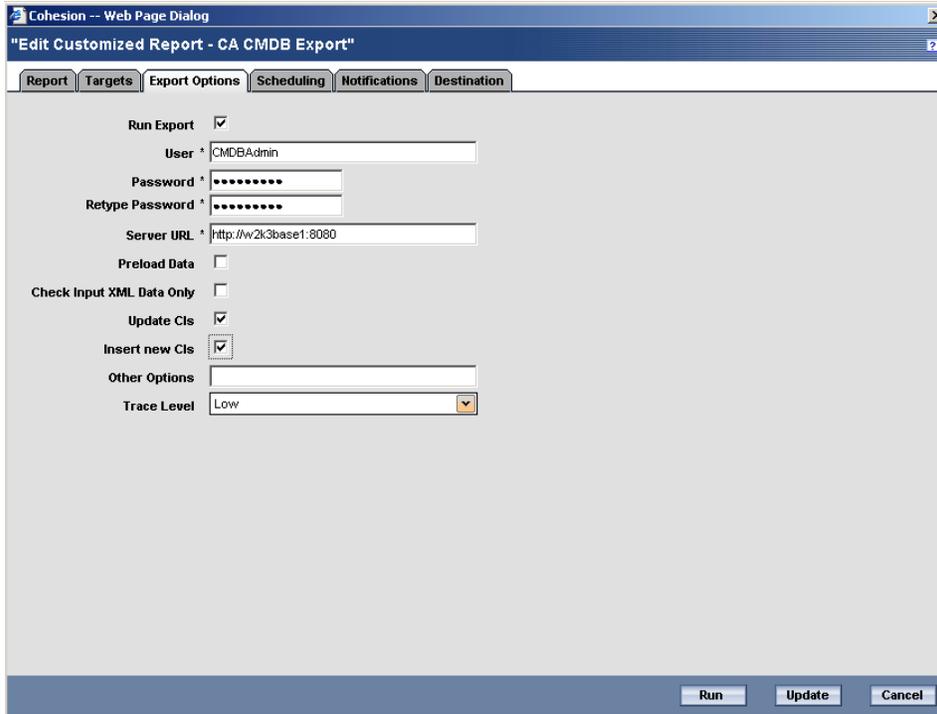
4. Edit any of the default values for the Report Name, Report Description, or Format fields. You can either select the HTML or XML format for the report.
5. Click the Targets tab and perform the following tasks:
  - a. Select the check boxes against the types of CIs you want to export.
  - b. Select the Include servers which are unlisted in Server Table check box to export the CIs from servers that are not listed in the Server table. CA Configuration Automation has information about servers that are not listed in the Server table. For example, after discovering CA Configuration Automation software, it will know the server on which CA Configuration Automation and the CA Configuration Automation database are hosted.

- c. Select the data that you want to export as the Host status, Services, Services Groups, Servers, and Component Blueprints in the export:
6. Click the Export Options tab and complete the following fields:
    - a. **Run Export:** Selected

**Note:** If the check box is not selected, the configuration items are not exported to CA SDM. The exported XML is displayed within the report output. You can preview the report to debug the data transferred between CA Configuration Automation and CA SDM.

    - b. **User:** CA SDM user name. The user must have access to creating CIs in CA SDM.
    - c. **Password:** The password of the user.
    - d. **Server URL:** The CA SDM Server URL and port. For example:  
[http://CMDB\\_server\\_name:8080](http://CMDB_server_name:8080)
    - e. **Preload Data:** (Optional) Selected. When selected, the report preloads several tables into memory. This Option is used to improve the performance of large export jobs with more than 50 entries. Selecting this option also increases memory usage, so it may impact other processes.
    - f. **Check Input XML Data Only:** (Optional) Selected. When selected, the updates to the database are prevented. This allows you to validate the input before actually loading the data into the database. The data can be found in the cohesionServer.log file, which is located in the c:\Program File\CA\Cohesion\Server (default location) directory.
    - g. **Update CIs:** Selected
    - h. **Insert new CIs:** Selected
    - i. **Other Options:** Specify any other options. See step 7 for more details.
    - j. **Trace Level:** Low

The following screenshot shows the Export Options with the completed fields:



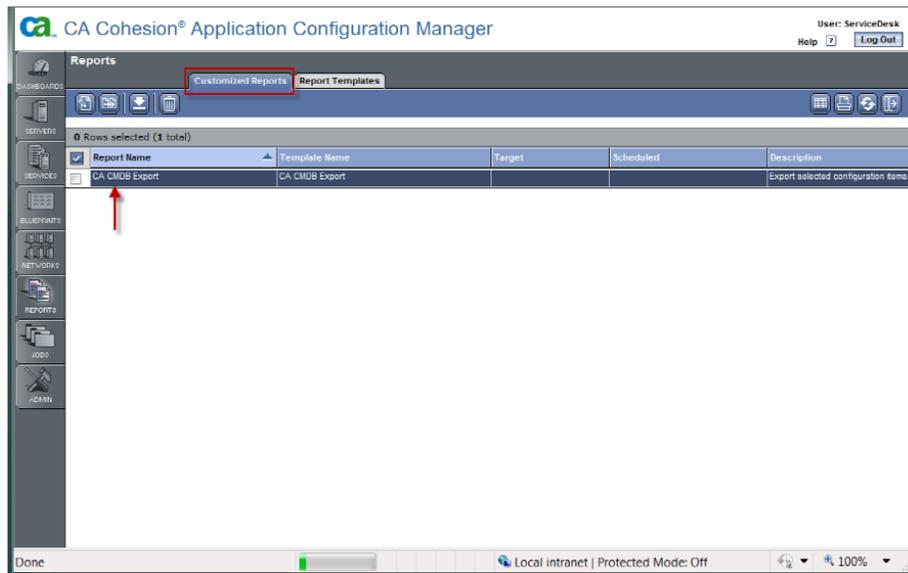
- (Optional) Use the Other Options field in the Export Options tab to define the export using a command line-like interface to enter the following required and optional GRLoader information:

**Note:** Some of these options are also available as UI fields. For example, the Server URL field in the Export Options tab is equivalent to the `-s` option listed in the following table.

Entry	Description
-u	CA CMDB user name (required)
-p	CA CMDB password (required)
-s	CA CMDB server URL and port (required); Example: <code>http://CMDB_server_name:8080</code>
-i	Input XML file (required)
-D	Name prefix for relations (optional); default is GRLoader
-e	Error XML file (optional); default is <code>inputname_err.xml</code>
-E	Allow overwriting Error XML if it exists (optional)
-P	Preload data to improve processing speed for large exports (optional)
-T	Trace level (optional)
-C	Check input XML only (optional)
-a	Allow updates to configuration items; default is do <i>not</i> allow updates (optional)

Entry	Description
-n	Allow new configuration items to be created (optional)
-N	Path to nx.env (only used when running JVM) (optional)
-v	Show GRLoader version (optional)
-h	Display the help (optional)

- Click Save to save the report.
- Click the Customized Reports tab and verify that the CA CMDB Report is displayed in the list of customized reports.



The report is saved.

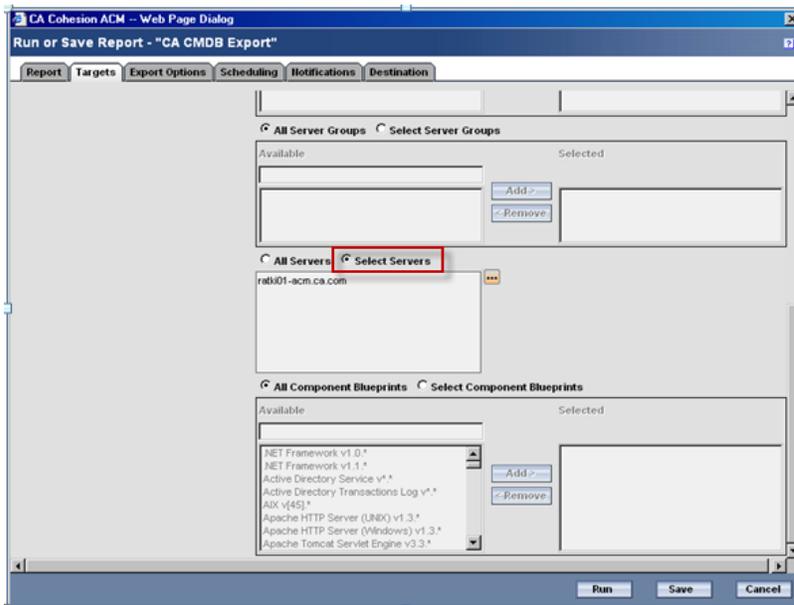
## Testing the Integration

### Testing the Integration from CA Configuration Automation

To test the integration, use the CA CMDB Export customized report that you created to export the discovered CIs from CA Configuration Automation into the CA CMDB.

#### Follow these steps:

1. Log in to CA Configuration Automation.
2. Click Reports in the navigation Menu tab.
3. Click the Customized Reports tab to view your list of customized reports.
4. Right-click the saved customized CA CMDB Export report and select Edit/View This Report....
5. Click the Targets tab and specify the objects that nt to export from CA Configuration Automation. Click the ellipsis button next to the Server selection area to select the servers you want to export to CA SDM. The following screenshot shows the selection of one server from CA Configuration Automation that will be exported to CA SDM:



6. Click the Export Options tab and specify the connection details to the CA SDM server:

The screenshot shows a web-based dialog box titled "CA Cohesion ACM - Web Page Dialog" with a subtitle "Run or Save Report - 'CA CMDB Export'". The dialog has several tabs: "Report", "Targets", "Export Options", "Scheduling", "Notifications", and "Destination". The "Export Options" tab is active. The form contains the following fields and controls:

- Run Export:** A checked checkbox.
- User:** A text input field containing "cmdbadmin".
- Password:** A text input field with masked characters (dots).
- Retype Password:** A text input field with masked characters (dots).
- Server URL:** A text input field containing "http://userid-cmdb:8080".
- Preload Data:** An unchecked checkbox.
- Check Input XML Data Only:** An unchecked checkbox.
- Update CIs:** A checked checkbox.
- Insert new CIs:** A checked checkbox.
- Other Options:** An empty text input field.
- Trace Level:** A dropdown menu currently set to "Low".

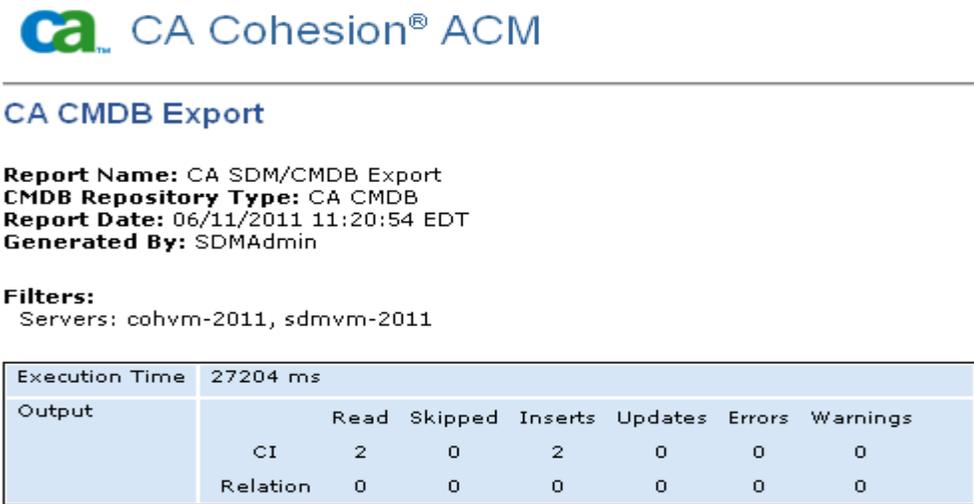
At the bottom right of the dialog, there are three buttons: "Run", "Save", and "Cancel".

The User ID provided in the User field must identify a user in CA SDM who has the rights to create CIs.

7. In the Server URL field, specify the CA SDM host URL.
8. Verify the User, Password, and Server URL values.
9. Select the Run Export option.
10. Click Run.

After the report is complete, an export report similar to the following screenshot displays showing how the export was performed:

---



The screenshot shows a report header with the CA Cohesion ACM logo. Below the logo is the title 'CA CMDB Export'. The report details include: Report Name: CA SDM/CMDB Export, CMDB Repository Type: CA CMDB, Report Date: 06/11/2011 11:20:54 EDT, and Generated By: SDMAdmin. A 'Filters' section lists 'Servers: cohvm-2011, sdmvm-2011'. A table displays execution statistics: Execution Time is 27204 ms. The table has columns for Output, Read, Skipped, Inserts, Updates, Errors, and Warnings. The 'CI' row shows 2 Read, 0 Skipped, 2 Inserts, 0 Updates, 0 Errors, and 0 Warnings. The 'Relation' row shows 0 Read, 0 Skipped, 0 Inserts, 0 Updates, 0 Errors, and 0 Warnings.

Execution Time	27204 ms						
Output	Read	Skipped	Inserts	Updates	Errors	Warnings	
CI	2	0	2	0	0	0	
Relation	0	0	0	0	0	0	

Copyright 2009 CA. All rights reserved.

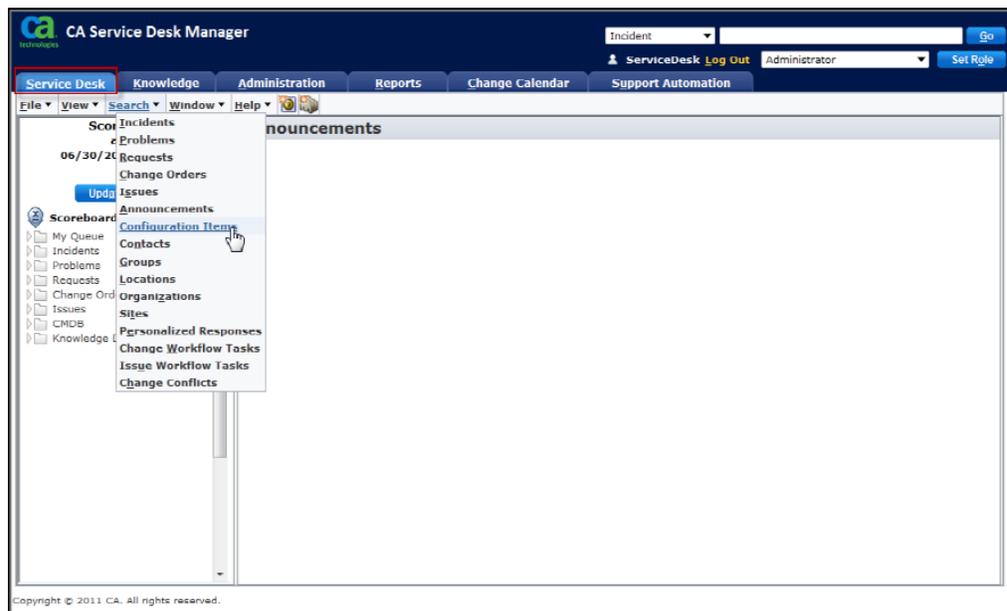
The testing of the integration is complete.

## Test the Integration from CA SDM

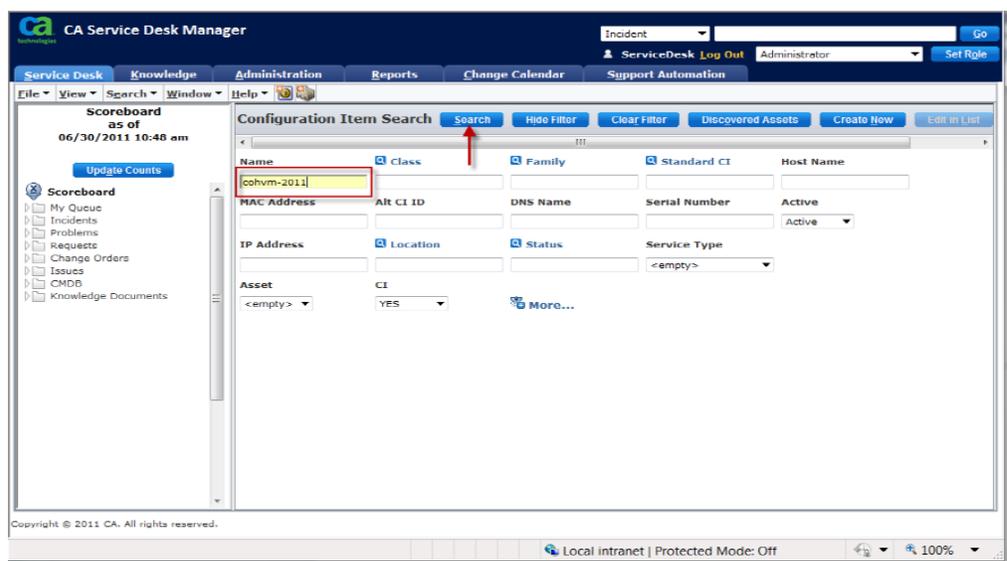
To test the integration, verify whether you are able to launch the CA Configuration Automation UI in context from a CI definition in CA SDM.

Follow these steps:

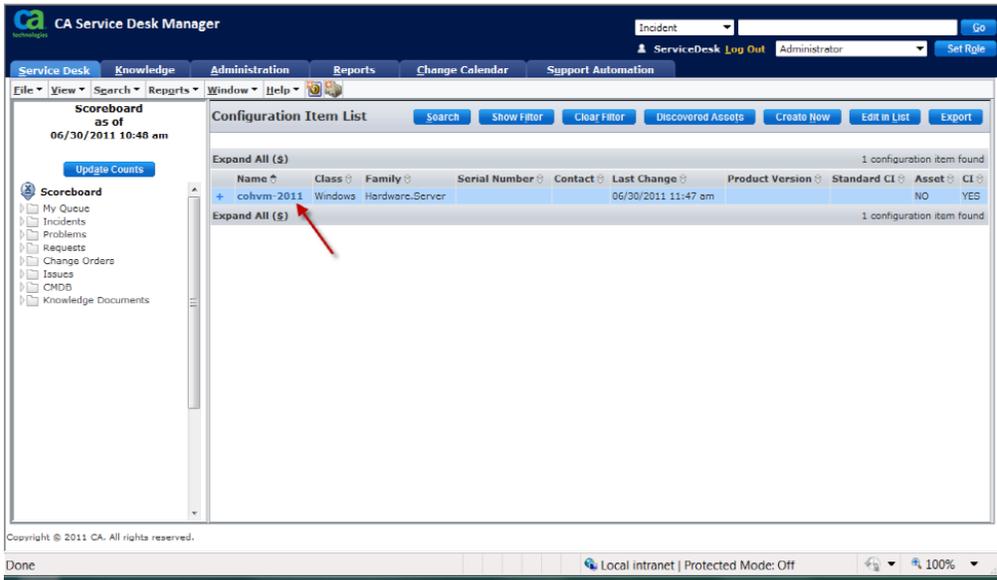
1. Log in to the CA SDM UI.
2. Click the Service Desk tab and click Search, Configuration Item.



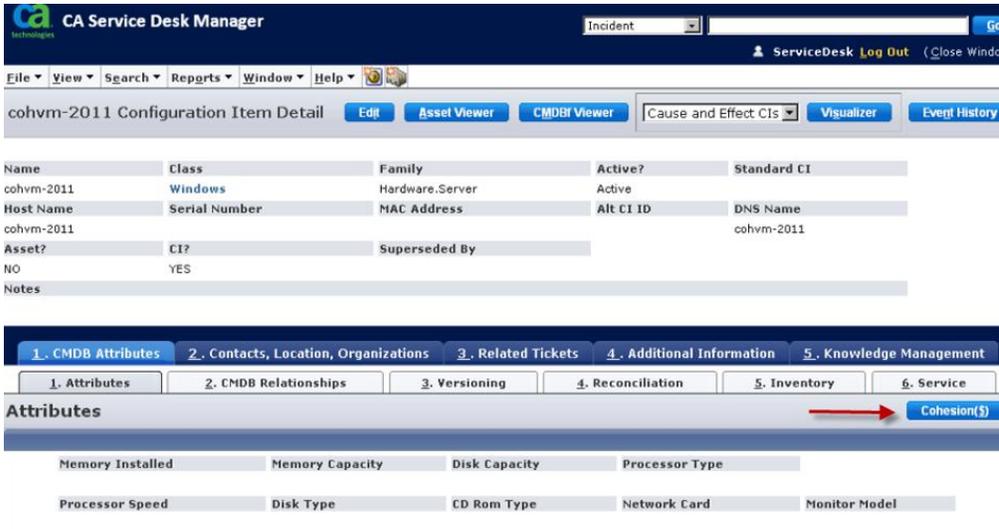
3. Type the CI name in the Name field and click Search.



- Click the CI to open the Configuration Item Detail form.



- Click the Cohesion button in the Attributes Tab.



- Click on the Detail Tree for ... link in the Cohesion MDR Launch window to get the detail information for the CI as shown in the following screenshot.



- Click CI Change Detection to compare differences between two snapshots and also launch the Rule Compliance feature.

The CA Configuration Automation CI Detail Tree opens as shown in the following screenshot:



The testing of the integration is complete.

## Reconciling CIs to Avoid Duplicates

---

Reconciliation helps ensure that updates from multiple data sources that refer to the same business object only update a single CI, even if they possess different identifying information. *Ambiguity* represents the possibility that a CI is not unique. CIs are *ambiguous* when they represent the same real business object. CI transactions are ambiguous when they have more than one possible target CI. Ambiguous CIs can lead to incorrect data in the CA SDM CMDB database, which negates the value of the CA SDM CMDB database and can lead to incorrect business actions.

Automatic CI reconciliation is a key CA SDM advantage that saves significant time in comparison to manual data maintenance. The process of reconciling CIs uses several specific identifying attributes. However, automatic reconciliation can in the following results:

- False positive matches:

Existing CIs are updated instead of creating a CI.

- False negative matches:

New CIs are created instead of updating an existing CI. The set of CIs with similar identifying attributes are ambiguous because they resemble the same real business object with similar identifying attributes.

## Reconciliation Approaches

CA SDM supports the following reconciliation approaches:

- **MDR-Based Reconciliation (Passive)**  
Allow CA SDM to reconcile any ambiguous data based on the MDR-Based Reconciliation process.
- **Identify and Resolve ambiguous CIs (Reactive)**  
Identify and resolve ambiguous CIs through identification and management of existing CIs in CA SDM.
- **Review and modify inbound data using a Transaction Work Area TWA (Proactive)**  
Review and modify inbound data before loading into CA SDM using a transaction work area (TWA).

### Using Transaction Work Area for Reconciliation

CA SDM provides a facility where you can store CI data before you load it into CA SDM. This *staged* data is stored as transactions in the Transaction Work Area (TWA). A staged transaction is a unit of work that creates or updates a CI or relationship. The TWA can contain many transactions for a given CI or relationship.

You can capture data being loaded into CA SDM before that data is committed so that you can do the following:

- Modify nonstandard data by cleansing and standardizing the data before it is loaded.
- Supplement incomplete data. For example, CI names starting with "NY" can have their locations set to "New York".
- Modify data that does not match existing lookup tables (SRELs).
- Schedule transactions for implementation at a future time.
- Reconcile transactions to existing CIs in the CA CMDB before you load the data.
- Validate the CI and relationship transactions to prevent the creation of invalid data or new CIs when a single or existing CIs have to be updated. You can view each transaction and the potential CIs that it can update so that you can reconcile the transaction manually to the correct target CI.

You can use the TWA to help you proactively manage the reconciliation process. You can configure GRLoader to load the data into the TWA, where CA SDM lets you modify the transaction data to handle transactions that can create, potentially update, or reference the wrong CI.

### Populating TWA

Input data for TWA can come from a number of sources, including the following:

- CA products like CA Configuration Automation, CA CEM, CA Introscope, and CA Spectrum that import data by using GRLoader
- Any other MDR that imports data using GRLoader
- Another CMDB
- Microsoft Excel spreadsheets
- Database tables
- An ETL tool chosen by a vendor

### Configure TWA with CA Configuration Automation

You can pass the TWA parameter (Ittwa) in the CA CMDB Export report options. This parameter causes the GRLoader to load the data into the TWA.

The -Ittwa (Load To Transaction Work Area) parameter loads XML data to the TWA in the initial state.

#### Follow these steps:

1. Open the CA CMDB Export report in the CA Configuration Automation web interface.
2. Click the Targets tab and select the servers or services that need to be loaded into TWA.
3. Click the Export Options tab.
4. Clear the Update CI and Insert new CIs options.
5. Enter **-Ittwa** in the Other Options field and click Run. The following screenshot shows the appropriate values to be set in the Export Options tab:

**"Edit Customized Report - CA SDM/CMDB Export"**

Report Targets **Export Options** Scheduling Notifications Destination

Run Export

User

Password

Retype Password

Server URL

Preload Data

Check Input XML Data Only

Update CIs

Insert new CIs

Other Options

Trace Level

Run Update Cancel

- When the Report runs without errors, the result window is displayed as shown in the following screenshot:

**CA Cohesion® ACM**  
**CA CMDB Export**

**Report Name:** CA SDM/CMDB Export  
**CMDB Repository Type:** CA CMDB  
**Report Date:** 06/14/2011 14:51:07 EDT  
**Generated By:** CA SDM,

**Filters:**  
 Servers: tenant-vm001

Execution Time	35883 ms						
Output		Read	Skipped	Inserts	Updates	Errors	Warnings
	TWA_CI	1	0	1	0	0	0
	TWA_Rel	0	0	0	0	0	0

Copyright 2009 CA. All rights reserved.

- Open the CA SDM UI, go to the Administration tab, and Select CA CMDB, Reconciliation Management, Transaction Work Area, CI Transactions. The CI Transactions in the TWA that were imported from CA Configuration Automation are displayed as shown in the following screenshot:

**CA Service Desk Manager**

Incident [ ] [Go] | ServiceDesk Log Out Administrator [Set Role]

Service Desk | Knowledge | **Administration** | Reports | Change Calendar | Support Automation

File | View | Window | Help

CA CMDB  
 CI Classes  
 CI Families  
 CI List  
 CI Models  
 CI Relationship List  
 CI Relationship Types  
 CI Service Status  
 MDR Management  
 Reconciliation Management  
 Ambiguous CI Transacti  
 Ambiguous CIs  
 Superseded CIs  
 Transaction Work Area  
**CI Transactions**  
 Relationship Transaction

CI Transaction List [Search] [Show Filter] [Clear Filter] [Create New] [E]

Expand All (\$) 1 CI Transaction found

Last Modified	Tenant	Name	Serial Number	MAC Address	DNS Nam
+ 06/14/2011 02:51 pm		tenant-vm001			tenant-vm001

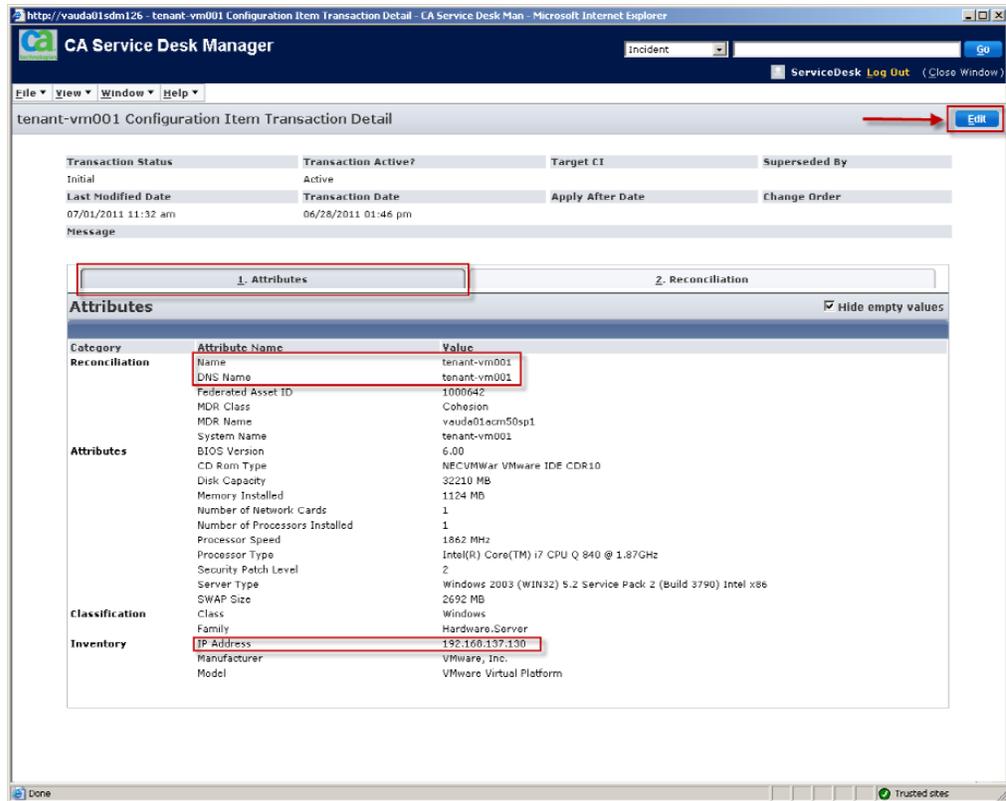
Expand All (\$) 1 CI Transaction found

Copyright © 2011 CA. All rights reserved.

- Click the date in the Last Modified column to open the CI Transaction for editing purposes.

**Note:** The Relationship Transactions are listed under CA CMDB, Reconciliation Management, Transaction Work Area, Relationship Transactions.

- Verify that the CI Transaction details are correct by reviewing the attributes on the Attributes tab.
- (Optional) Click Edit to update the details of the transaction, if necessary.



11. Click the Reconciliation tab and verify whether the CI Transaction reconciles to the correct CI, if a CI already exists that matches the CI in the CI Transaction. Typically the attributes to verify are the Name, DSN Name, IP Address, System Name, MAC Address, and Serial Number.
12. The Reconciliation tab lists any preexisting CIs in CA SDM that match this CI transaction.

**Note:** To determine if a CI in the list is truly a match, click the CI name to view the CI Detail form of the CI. Review the attributes in the CI Details window to confirm that the proposed CI is a match. Review the attributes on the Attributes and Inventory sub tabs of the CMD Attributes tab too.

## Reconciling CIs to Avoid Duplicates

The screenshot displays the CA Service Desk Manager interface. The main window title is "tenant-vm001 Configuration Item Detail". The interface includes a menu bar (File, View, Search, Reports, Window, Help) and a toolbar with buttons for Edit, Asset Viewer, CMDB Viewer, Cause and Effect CIs, Visualizer, and Event History. The main content area shows a table of attributes for the CI "tenant-vm001".

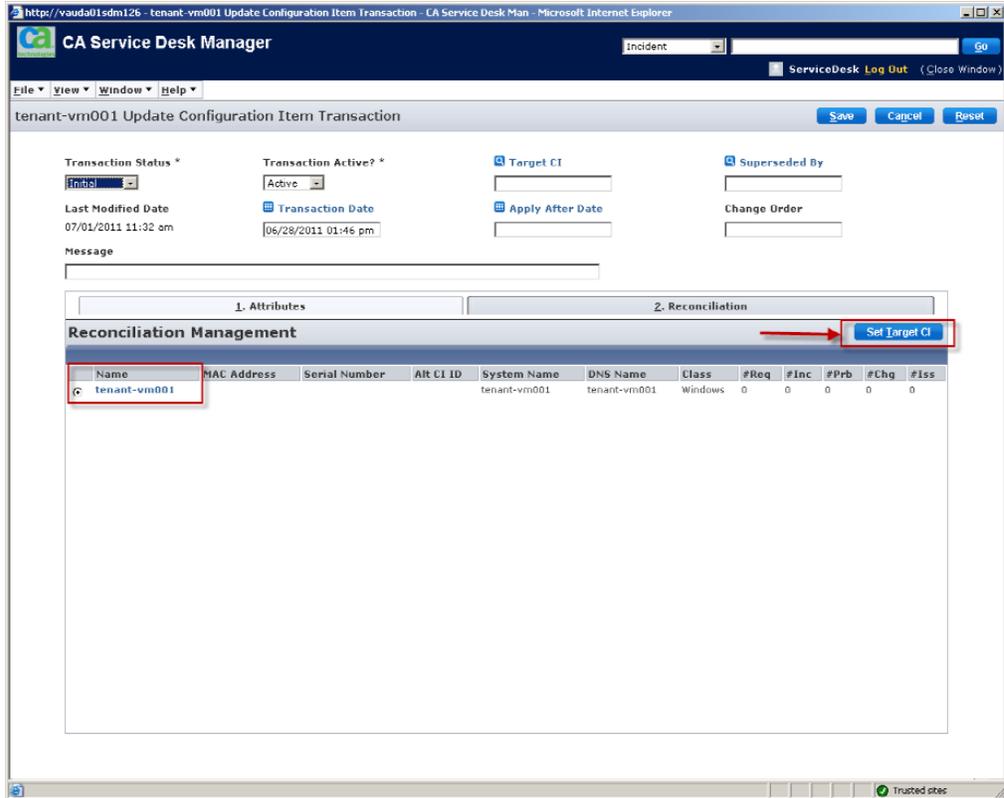
Name	Class	Family	Active?	Standard CI
tenant-vm001	Windows	Hardware Server	Active	
Host Name	Serial Number	MAC Address	Alt CI ID	DNS Name
tenant-vm001				tenant-vm001
Asset?	CI?	Superseded By		
NO	YES			

Below the attribute table, there are several tabs for navigation: 1. CMDB Attributes, 2. Contacts, Location, Organizations, 3. Related Tickets, 4. Additional Information, 5. Knowledge Management. Under the "Inventory" section, there is another table of attributes:

IP Address	Model	Manufacturer	License Number	Service Status
192.168.137.130				
Acquire Date	Installation Date	Expiration Date	Warranty Start Date	Warranty End Date
Product Version	Financial Reference	Quantity	Asset Lifecycle Status	
		1		

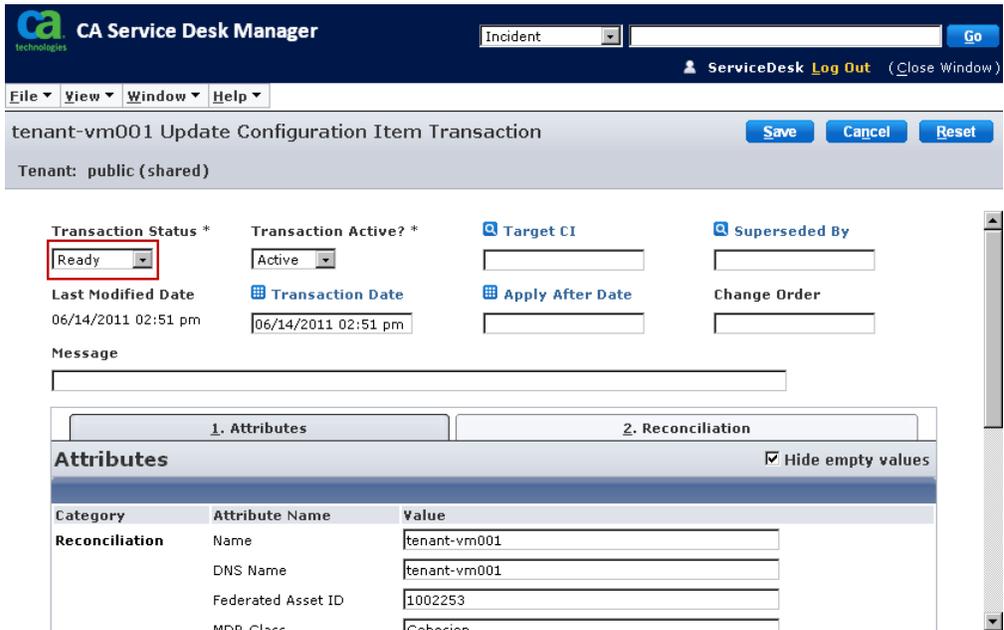
After you are sure that there is a match, do the following:

- a. Click on the radio button next to the CI name and click Set Target CI.



13. Load the CI transaction in CA SDM using the following steps:

- a. Change the Transaction Status from *Initial* to *Ready* and then click Save as shown in the following screenshot:



- b. From a Command prompt on the CA SDM server, issue the following GRLoader command to load the CI and relationships into CMDB:

```
GRLoader -n -u <CA SDM username> -p <password> -s <CA SDM Server Url  
http:<servername:port> -lftwa
```

After Successfully loading the CI, the Transaction Status changes to Successful.

Now the CI has been exported into CA SDM and can be found when searching for Configuration Items.

## Configure SSL Communication for CA Configuration Automation

---

When CA SDM is configured to use the Secure Sockets Layer (SSL), you need to configure CA Configuration Automation for it to successfully communicate with the secured instance of CA SDM. Otherwise, when you attempt to run a report from CA Configuration Automation to export CIs, GRLoader will be unable to log on to the SSL enabled CA SDM Server.

To enable GRLoader to work correctly, Java has to be able to authenticate the server certificate for the Web Services. This process includes following tasks:

- Create a certificate.
- Add the certificate to the Java cacerts store, also known as the trusted key store.
- Pass the URL of the https server to GRLoader.

### Create Certificate

To create the certificate, first open a command prompt and change directories to the JRE install location on the CA SDM Server directory. The following is the default location for this directory:

```
C:\Program Files\CA\SC\JRE\1.6.0_23
```

Execute the following command:

```
bin\keytool -export -alias <insert alias here> -keystore <storename> -rfc -file  
<insert .cer filename> -storepass <password>
```

For example:

```
bin\keytool -export -alias tomcat -keystore .keystore -rfc -file tomcat.cer  
-storepass changeit
```

The certificate is created.

## Add Certificate to Java Trusted Key Store

To enable GRLoader to communicate with the CA SDM https server, configure Java to use the certificate you created in the previous step. GRLoader uses the following copy of Java on the CA Configuration Automation Server:

```
C:\Program Files\CA\Cohesion\Server\j sdk\jre
```

However, you need to run the following command on the cacerts file in the following directory:

```
C:\Program Files\CA\Cohesion\Server\j sdk\jre\lib\security
```

Therefore, you will need to import the .cer file or certificate file you just created on the CA SDM Server to the cacerts directory on each of the CA Configuration Automation Servers that run reports against it. To import the certificate follow these steps:

1. Open a command prompt and change directories to the JRE install location. By default, the following is the default JRE location:

```
C:\Program Files\CA\Cohesion\Server\j sdk\jre
```

2. Enter the following command:

```
bin\keytool -import -alias <insert alias> -file <insert .cer filename> -keystore
<storename> -storepass <password>
```

For example:

```
bin\keytool -import -alias tomcat -file tomcat.cer -keystore lib\security\cacerts
-storepass changeit
```

The certificate is now added to the Java trusted key store.

## Pass the URL to GRLoader

Finally, to run reports from the CA Configuration Automation Server against the https CA SDM server, modify the Server URL attribute in the Export Option tab to the following:

```
<https server url:port>
```

For example:

```
https://localhost:8443
```

For more details on configuring GRLoader to work in an SSL environment, consult the technical document TEC428625, which is available on support.ca.com.

## Tips for Modifying the CMDB Attribute Mapping

---

CA Configuration Automation installs a file called *cmdb\_mapping.xml* that enables CA SDM users to customize the mapping of Cohesion CIs and their attributes so they match the structure of CMDB CIs when exported to CA SDM.

The CA CMDB Export report uses the *cmdb\_mapping.xml* file to determine which Cohesion CIs, attributes, and relationships are exported and how to map them to CA SDM families, classes, attributes, and relationships.

When the *cmdb\_mapping.xml* file is used as provided without any modifications, the results are likely to include duplicate CIs. This chapter provides some tips and tricks for modifying the xml file to produce more accurate results.

The *cmdb\_mapping.xml* file contains three mapping types: Attribute Mapping, Class Mapping, and Relationship Mapping. For information on attribute mapping, refer to Appendix C in the *CA Configuration Automation Implementation Guide*.

By default, the *cmdb\_mapping.xml* file is located in the following locations:

- `\Program Files\CA\Cohesion\Server\server\webapps\cohesion\WEB-INF\classes` (Windows)
- `/opt/CA/Cohesion/Server/server/webapps/cohesion/WEB-INF/classes` (UNIX or Linux)

**Note:** Editing the *cmdb\_mapping.xml* file with the Windows text editor will corrupt the file. Always use an XML editor to modify the file.

## Remove Model Attributes

The CA Configuration Automation CI Server has several attributes that can be exported into CA SDM. Most of the attributes exported are of a STRING type in CA SDM. Others, like the model attribute, reference other CA SDM objects and will require you to lookup the record before the CI can be created in CA SDM. When the CA CMDB Export report is run, CA Configuration Automation attempts to associate the model name discovered in Cohesion with the server CI and send that information to CA SDM. The Model record must exist in the ca\_model\_def table of the MDB for CA SDM to access. If it does not exist, errors will be generated in the CA CMDB Export report, in the following manner:

```
<!--ERROR: Error setting attr 'model' on object 'nr:10B22E3C4236664D825BF7A72BE416DB' to value '1330D45A5897D040B52391F821071FE4' NOT FOUND 1330D45A5897D040B52391F821071FE4-->
```

If the model data does not exist in CA SDM, the server CI passed from CA Configuration Automation will not be created in CA SDM. If the servers are not created, then the relationships around the CIs will also fail, resulting in more errors in the export results. To avoid generating any errors before the model information has been created in CA SDM, you can comment on the model attribute mapping line in the server CI mapping section. Comments are denoted by <!--text here -->.

### Follow these steps:

1. Open the cmdb\_mapping.xml file on the CA Configuration Automation server in an XML editor.
2. Search for the server CI attribute mapping section:

```
<!--attribute mapping for server CI -- >
```

3. Comment out the model attribute mapping line:

```
<!--<attributeMapping CohesionCI="server" CohesionAttr="model" CMDBAttr="model" CMDBFamily="*" />-->
```

## Removing Redundant Software CIs

CA Configuration Automation associates each managed server with the software discovered on it. Note in the following screenshot that Microsoft Cluster Server is listed twice - once for each server it was discovered on:

The screenshot shows the CA Cohesion Application Configuration Manager interface. The main window displays a table of software components discovered on managed servers. The table has columns for Component Name, Version, Qualifier, Server Name, and Component State. Two entries for 'Microsoft Cluster Server' are highlighted with a red box, showing they were discovered on different servers.

Component Name	Version	Qualifier	Server Name	Component State
<input checked="" type="checkbox"/> Microsoft Cluster Server	5.2	C:\WINDOWS	lodvm123456n2	Managed
<input type="checkbox"/> Microsoft Cluster Server	5.2	C:\WINDOWS	lodvm123456n1.vndom1.local	Managed
<input type="checkbox"/> Microsoft SQL Server - Client	9.00.1399.06	C:\Program Files\Microsoft SQL Server\80\Tools	lodvm123456n2	Managed
<input type="checkbox"/> Microsoft SQL Server - Client	9.00.3042.00	C:\Program Files\Microsoft SQL Server\80\Tools	lodvm123456n1.vndom1.local	Managed
<input type="checkbox"/> Microsoft SQL Server - Datafiles	9.00.1399.06	F:\Microsoft SQL Server\MSSQL.1\MSSQL	lodvm123456n2	Managed
<input type="checkbox"/> Microsoft SQL Server - Datafiles	9.2.3042.00	F:\Microsoft SQL Server\MSSQL.1\MSSQL	lodvm123456n1.vndom1.local	Managed
<input type="checkbox"/> Microsoft SQL Server 2005	9.2.3042.00	C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL	lodvm123456n1.vndom1.local	Managed
<input type="checkbox"/> Microsoft SQL Server 2005	9.00.1399.06	C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL	lodvm123456n2	Managed
<input type="checkbox"/> MySQL (Windows)		C:\FastESP\rdoms	lodvm123456n2	Managed
<input type="checkbox"/> Windows	5.2	Microsoft Windows Server 2003 R2 SP2	lodvm123456n1.vndom1.local	Managed
<input type="checkbox"/> Windows	5.2	Microsoft Windows Server 2003 R2 SP2	lodvm123456n2	Managed

This information can be imported into the CA CMDB as software CIs and will be associated through a relationship to the server it was discovered on. Using the default `cmdb_mapping.xml` file, the software CI being imported into CA SDM will be created once each time it is discovered on a server. If you are looking for a 1:1 ratio of software per server, the results may match your requirement.

The following screenshot shows the result of software discovered on the two servers that were selected for import in the CA CMDB Export report. Since the Microsoft Cluster Server software CI was discovered on two servers, it was imported into the CA CMDB twice. The Configuration Item list in CA CMDB does not show that the server attribute is different for each CI record. Therefore, the software CI appears to be a duplicate record.

The screenshot shows the CA Service Desk / CA CMDB interface. The 'Configuration Item List' table contains the following entries:

Name	Class	Family	Serial Number
Microsoft Cluster Server v5.2 (C:\WINDOWS)	COTS	Software.COTS	
Microsoft Cluster Server v5.2 (C:\WINDOWS)	COTS	Software.COTS	
Microsoft SQL Server - Client v9.00.1399.06 (C:\Program Files\Microsoft SQL Server\80\Tools)	SQL	Software.Database	
Microsoft SQL Server - Client v9.00.3042.00 (C:\Program Files\Microsoft SQL Server\80\Tools)	SQL	Software.Database	
Microsoft SQL Server - Datafiles v9.00.1399.06 (F:\Microsoft SQL Server\MSSQL_1\MSSQL)	SQL	Software.Database	
Microsoft SQL Server - Datafiles v9.2.3042.00 (F:\Microsoft SQL Server\MSSQL_1\MSSQL)	SQL	Software.Database	
MySQL (Windows) (C:\FastESP\rdbms)	Other Software Database	Software.Database	
MySQL Datafiles (C:\FastESP\data\rdbms)	Other Software Database	Software.Database	
MySQL Datafiles (C:\FastESP\rdbms\data)	Other Software Database	Software.Database	

Importing duplicate software CIs may not be desirable and can add complications to reporting. One option to only import each software CI once and keep the necessary relationships intact, is to comment out the `system_name` attribute line.

**Follow these steps:**

1. Open the `cmdb_mapping.xml` file on the CA Configuration Automation server.
2. Search for the attribute mapping section for software components.

```
<!--attribute mapping for Software Component CI -- >
```

3. Comment out the `system_name` attribute mapping line.

```
<!-- <attributeMapping CohesionCI="component" CohesionAttr="system_name" CMDBAttr="systems_name" CMDBFamily="*" />-- >
```

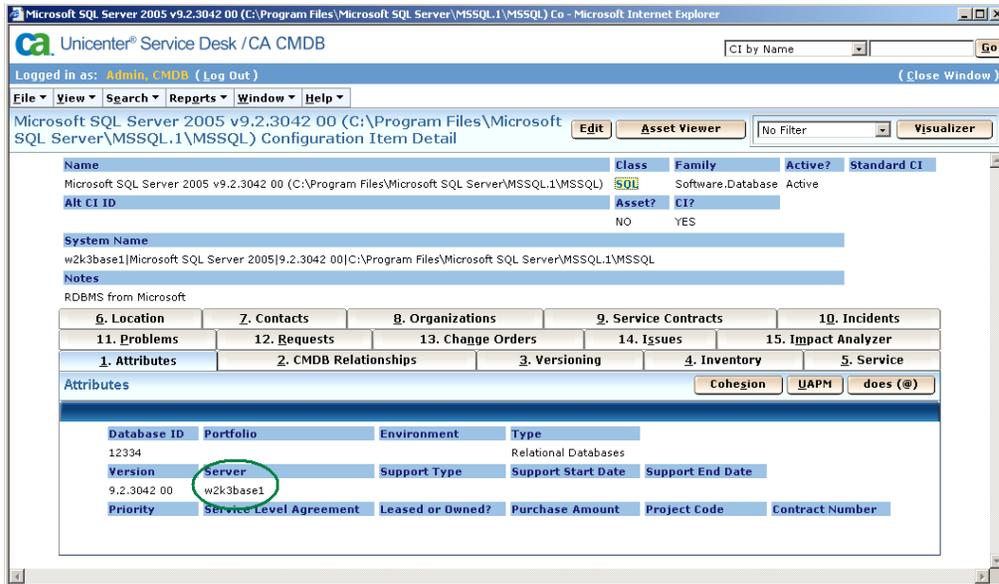
**Note:** This only works if the software installed on each server has the same install path.

Another option is to use the NameQualifier parameter in the Component Blueprint to remove the path indicated in the CI name. If defined, it is displayed after the name in the discovered service tree view. Refer to the *CA Configuration Automation Product Guide*, Chapter 5, section "Component Blueprint Building Reference Files", under the Category Descriptions sub section for instructions on modifying this parameter.

4. Comment out the server attribute mapping line:

```
<!-- <attributeMapping CohesionCI="component" CohesionAttr="host" CMDBAttr="server" CMDBFamily="*" />-- >
```

This prevents the Server attribute value, shown in the following screenshot, from getting updated each time the software CI is discovered on a new server.



### Tips for Modifying the CMDB Class Mapping

The class mapping section of the `cmdb_mapping.xml` file includes a list of default Cohesion components and their default mappings to CA CMDB Classes. Any component not listed in this section will be assigned a default class value. For example, if a discovered software component is not listed in the xml file it will be given a default value of `Software.COTS` as defined in the following line:

```
<!--mapping to define the CMDB Class to map to à  
...  
<classMapping CohesionCI="component" ComponentName="*" CMDBFamily="Software.COTS"  
CMDBClass="COTS" / >
```

**Note:** When you specify or change a CMDB class mapping in the xml file, that class and family must already exist in CA SDM or else the export fails.

## Modify the Class Mapping

You can modify the class mapping section, if there are software components that are not already listed in the xml file, or that need to be reclassified. For example, to avoid classifying a discovered instance of Microsoft Active Directory as Software.COTS by default, add the following to the xml file:

### Follow these steps:

1. Open the cmdb\_mapping.xml file on the CA Configuration Automation server.
2. Find the section that defines the CMDB Class mapping section:

```
<!--mapping to define the CMDB Class to map to -->
```

3. Add the following line:

```
<classMapping CohesionCI="component" ComponentName="Active Directory Service"
CMDBFamily="Security" CMDBClass="Application Security" />
```

4. Add the following lines to help ensure proper classification of discovered software UI, Microsoft Cluster, and Java Web Applications in the CMDB Class mapping section:

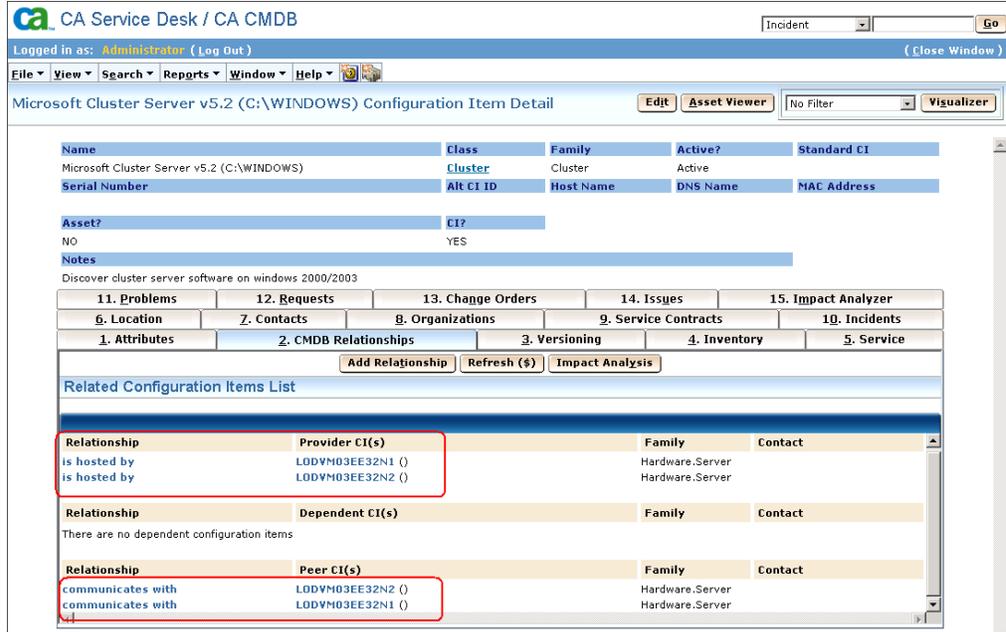
```
<classMapping CohesionCI="component" ComponentName="Microsoft Cluster Server"
CMDBFamily="Cluster" CMDBClass="Cluster" />
<classMapping CohesionCI="component" ComponentName="Java Web Application"
CMDBFamily="Software.Application Server" CMDBClass="Application Server" />
```

In the following screenshot, you can see that the Microsoft Cluster Server v5.2 is listed once and is classified correctly with a class of Cluster. Previously, the component had two records and was classified as Software.COTS.

Configuration Item Name	CMDB Family	CMDB Class
Log4j (C:\Program Files\CA\SC\Mdb\Windows)	COTS	Software.COTS
Microsoft Cluster Server v5.2 (C:\WINDOWS)	Cluster	Cluster
Microsoft SQL Server - Client v9.00.1399.06 (C:\Program Files\Microsoft SQL Server\80\Tools)	SQL	Software.Database
Microsoft SQL Server - Client v9.00.3042.00 (C:\Program Files\Microsoft SQL Server\80\Tools)	SQL	Software.Database
Microsoft SQL Server - Datafiles v9.00.1399.06 (F:\Microsoft SQL Server\MSSQL\1\MSSQL)	SQL	Software.Database
Microsoft SQL Server - Datafiles v9.2.3042.00 (F:\Microsoft SQL Server\MSSQL\1\MSSQL)	SQL	Software.Database

5. Click the Microsoft Cluster Server v5.2 link and click the CMDB Relationships tab.

The relationships with the two cluster nodes are identified correctly as shown in the following screenshot:



**Note:** For more information on the attributes in the class mapping section, see the Appendix C of the *CA Configuration Automation Implementation Guide*.

## Reconciling Managed Hardware across Multiple Domains

Reconciling managed hardware which is discovered through CA Configuration Automation can be a challenge when the discovery crosses multiple domains. This reconciliation becomes even more challenging when the hardware itself is discovered across multiple domains. When the default configurations are used, the discovery process performed with CA Configuration Automation creates one server CI and an additional CI for each Network Interface Card (NIC), Hard Drive, and File System component existing on the server. This happens because the actual server CI record is discovered through CA Configuration Automation with a Fully Qualified Domain Name (FQDN) in each domain. If no action is taken to reconcile the records, the data is added into CA SDM for each instance of the discovered name.

For example, the exchsvr01 server listed in the table that follows has four NIC cards, five hard drives and IPs in two domains. As a result, discovery identifies two servers, eight NIC cards, and ten hard drives as shown in the following table:

Discovered FQDN	Desired Name	Description
exchsvr01.dom1.abc.com	exchsvr01	Discovered by Cohesion in dom1.abc.comabc.com domain
exchsvr01.dom2.abc.comabc.com		Discovered by Cohesion in dom2.abc.comabc.com domain

Discovered FQDN	Desired Name	Description
exchsvr01.dom1.abc.coma bc.com   DISK-0	exchsvr01   DISK-0	Hard Drive
exchsvr01.dom2.abc.coma bc.com   DISK-0		Hard Drive
exchsvr01.dom1.abc.coma bc.com   DISK-1	exchsvr01   DISK-1	Hard Drive
exchsvr01.dom2.abc.coma bc.com   DISK-1		Hard Drive
exchsvr01.dom1.abc.coma bc.com   DISK-2	exchsvr01   DISK-2	Hard Drive
exchsvr01.dom2.abc.coma bc.com   DISK-2		Hard Drive
exchsvr01.dom1.abc.coma bc.com   DISK-3	exchsvr01   DISK-3	Hard Drive
exchsvr01.dom2.abc.coma bc.com   DISK-3		Hard Drive
exchsvr01.dom1.abc.coma bc.com   DISK-4	exchsvr01   DISK-4	Hard Drive
exchsvr01.dom2.abc.coma bc.com   DISK-4		Hard Drive
exchsvr01.dom1.abc.coma bc.com   DISK-5	exchsvr01   DISK-5	Hard Drive
exchsvr01.dom2.abc.coma bc.com   DISK-5		Hard Drive
exchsvr01.dom1.abc.coma bc.com   NetworkAdaptor-0	exchsvr01   NetworkAdapto r-0	Network Interface Card
exchsvr01.dom2.abc.coma bc.com   NetworkAdaptor-0		Network Interface Card
exchsvr01.dom1.abc.com   NetworkAdaptor-1	exchsvr01   NetworkAdapto r-1	Network Interface Card
exchsvr01.dom2.abc.com   NetworkAdaptor-1		Network Interface Card
exchsvr01.dom1.abc.com   NetworkAdaptor-2	exchsvr01   NetworkAdapto r-2	Network Interface Card
exchsvr01.dom2.abc.com   NetworkAdaptor-2		Network Interface Card
exchsvr01.dom1.abc.com   NetworkAdaptor-3		Network Interface Card

Discovered FQDN	Desired Name	Description
exchsvr01.dom2.abc.com   NetworkAdaptor-3	exchsvr01   NetworkAdaptor-3	Network Interface Card

Though this result may be acceptable for managing discovered data in the CA Configuration Automation application, it may not be desirable as data input into CA SDM where the server CI needs to exist as one record with relationships to the four NICs and five Hard Drives. We can correct the mapping of Cohesion to CA CMDB data by performing the following tasks:

1. Using the component blueprint parameter in Cohesion to look up a server's Host Name. This helps ensure that the Host Name in CA Configuration Automation can be mapped to the Name in CA SDM through the Cohesion XML mapping file.
2. Removing the fully qualified domain name from the hard drive.
3. Adding the MAC address to the NIC blueprint and passing it into CA SDM through the Cohesion XML mapping.

**Note:** This situation only occurs when the NICs are registered with IP addresses that exist in multiple domains. If the IP addresses are in the same domain, the relationship between the server and its NICs will be passed into the CA SDM.

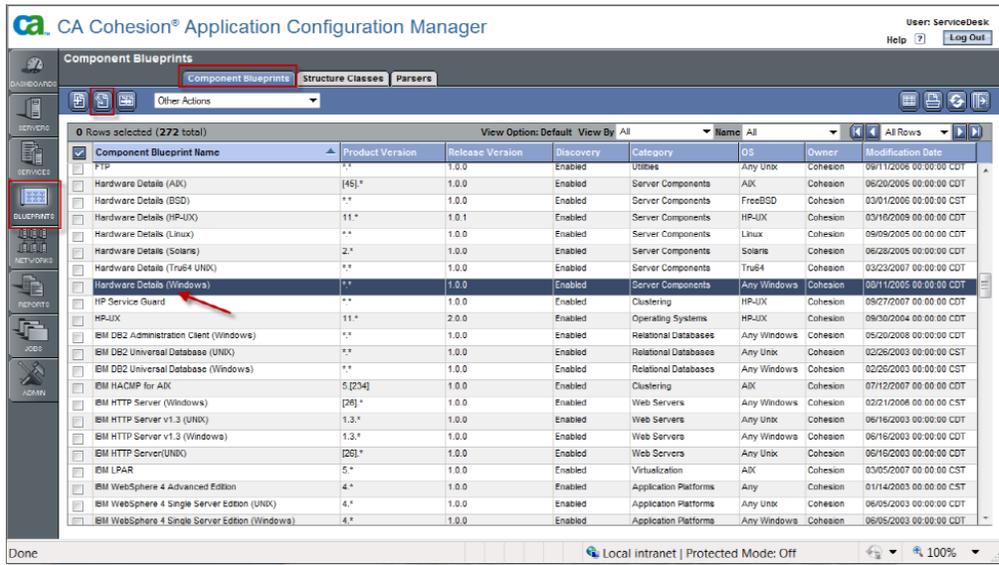
### Reconcile Discovered Servers

The first step is to reconcile the two server records using the Hostname. The two discovered servers are then passed from CA Configuration Automation into CA SDM by mapping the Discovered Host Name field to the CA SDM system\_name field. By default, the Cohesion Blueprint uses the unqualified hostname as a parameter in CA Configuration Automation, and this parameter will be used as a mapping value in the CA Configuration Automation XML mapping file.

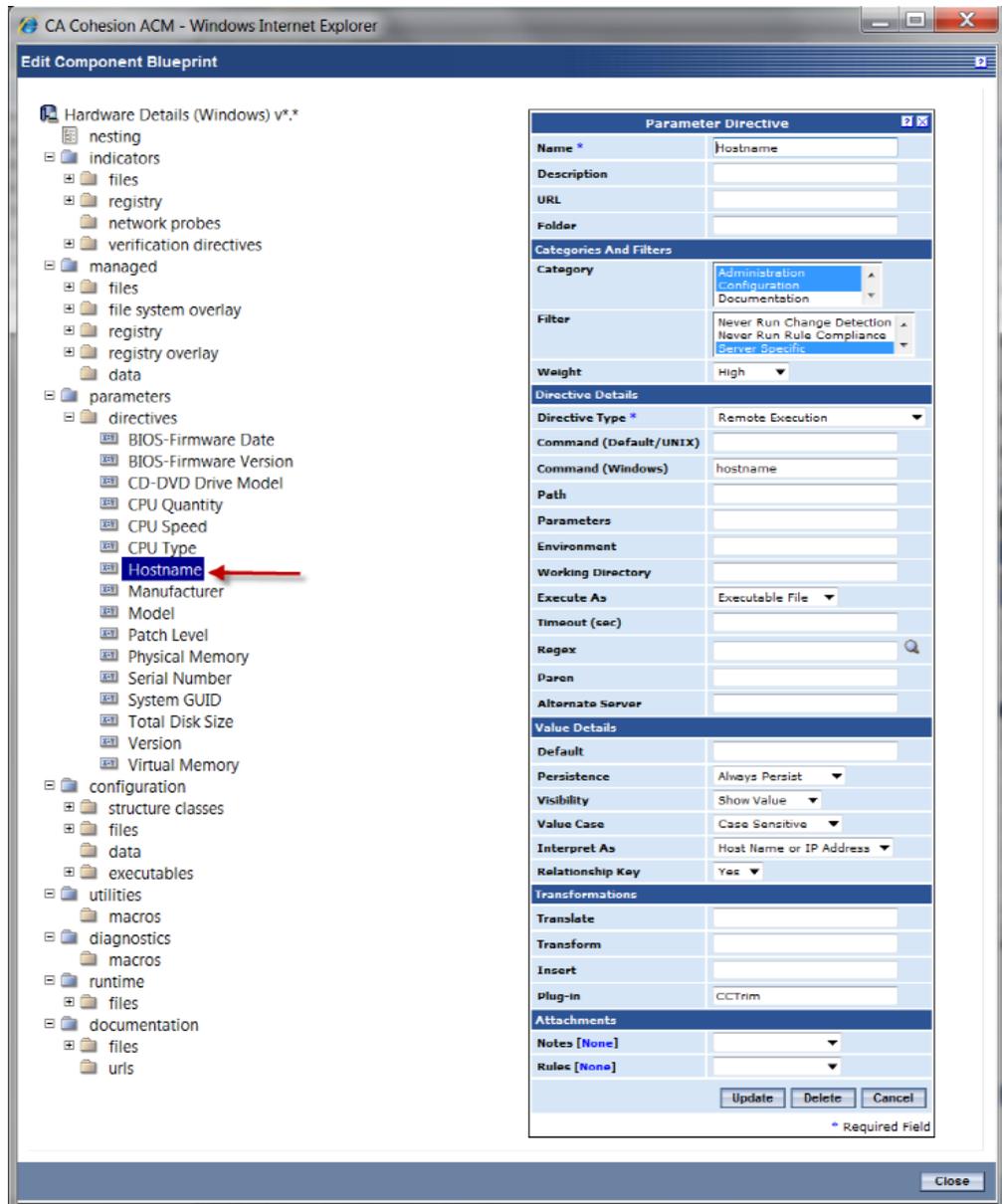
## Verify the Computer Name (Short Name)

Follow these steps:

1. Launch the CA Configuration Automation UI.
2. Click the Blueprints tab and select Hardware Details (Windows) as shown in the following screenshot:



3. Click Edit/View.
4. Expand the parameters, directives, Hostname as shown in the following screenshot:



5. Verify the settings and close the window if the default settings are adequate.

### [View the cmdb\\_mapping.xml File](#)

#### **Follow these steps:**

1. On the CA Configuration Automation Server, browse to the \Classes folder under the Cohesion install directory. The default path is

C:\Program Files\CA\Cohesion\Server\server\webapps\cohesion\WEB-INF\classes

2. Locate the cmdb\_mapping.xml file in this directory and open it using an XML editor.
3. In the first section, <!-- attribute mapping for server CI -->, locate the mapping for system\_name. For example:

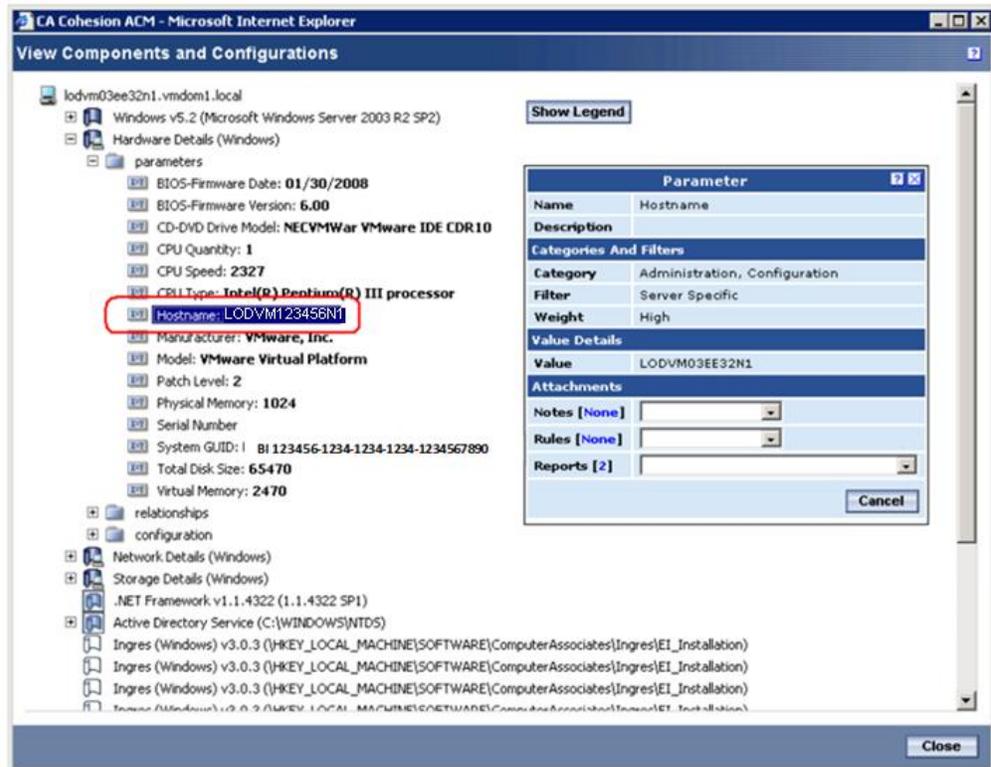
```
<attributeMapping CohesionCI="server" CohesionAttr="Hostname"  
CMDBAttr="system_name" CMDBFamily="*" />
```

Note that the attribute CMDBAttr="system\_name" is mapped to CohesionAttr="Hostname"

## Verify Collection of Hostname Parameter

Follow these steps:

1. Run a Discovery profile and/or Management Profile, if you have not already done so.
2. Review the Hardware Detail for one or more servers and verify that the Hostname parameter in the Hardware Detail component shows the short name of the computer.



## Reconcile Relationships

After you have reconciled the discovered servers, modify the XML mapping file for proper reconciliation. Add the MAC Address attribute in this file, to CIs classified with the Network.Network Interface Card family. This attribute enables the NIC cards to be properly reconciled through CORA using MAC Address when it is passed into CA SDM.

## Update the XML File to Add MAC Address

### Follow these steps:

1. Open the `cmdb_mapping.xml` file in an XML editor.

2. Search the file for the NIC class section:

```
<!--attribute mapping for NIC CI -->
```

3. Add the following line to the NIC CI attribute mapping section:

```
<attributeMapping CohesionCI="server" CohesionAttr="mac_address"
CMDBAttr="mac_address" CMDBFamily="*" />
```

4. Modify the following line to use Hostname for the CohesionAttr instead of uname:

```
<attributemapping CohesionCI="nic" CohesionAttr="Hostname" CMDBAttr="name"
CMDBFamily="*" />
```

## Reconcile NIC Relationships

Reconciling NIC relationships will add the physical address or `mac_address` for each NIC found on a server. CORA only supports a single NIC per server. If a server has multiple NICs, CORA creates a new CI for every NIC.

Add the following Physical Address mapping line to the NIC CI class mapping section to map the CA Configuration Automation NIC Physical Address to the SDM Network Interface Card `mac_address` attribute.

```
<!-- attribute mapping for NIC CI -->
<attributeMapping CohesionCI="nic" CohesionAttr="Physical Address" CMDBAttr="mac_address"
CMDBFamily="*" />
```

### Modify the Virtual CI Class Mapping Section

Comment out the mac\_address mapping line from the Virtual CI class mapping sections of the mapping file. This will prevent CA Configuration Automation from adding the MAC address entries to the Hardware.Server class CI and helps CORA reconcile each entry once instead of creating multiple entries for each MAC Address it reconciles against.

#### Follow these steps:

1. Search for the Virtual CI class mapping section in the xml file:

```
<!--Attribute mapping for virtual CI -- >
```

2. Comment out the following line:

```
<!-- <attributeMapping CohesionCI="virtual" CohesionAttr="mac_address"
CMDBAttr="mac_address" CMDBFamily="*" /> -- >
```

**Note:** You can ignore the mac\_address mapping for Cohesion 5.0 Sp1, it does not have this entry.

### Modify the Hard drive CI Class Mapping Section

Update the xml file to use Hostname for the CohesionAttr instead of uname. If you use uname, each hard drive will be discovered in each domain. Using Hostname helps ensure that the Hard Drive information is only discovered once.

#### Follow these steps:

1. Search for the hard drive CI attribute mapping section in the xml file:

```
<!--Attribute mapping for Hard drive CI -- >
```

2. Modify the following line to use "Hostname" instead of "name".

```
<!-- <attributeMapping CohesionCI="Hard Drive" CohesionAttr="Hostname" CMDBAttr="name"
CMDBFamily="*" /> -- >
```

## Modify the File System CI Class Mapping Section

Modify the following line to use Hostname for the CohesionAttr instead of unname. If you use unname, each file system will be discovered in each domain. Using Hostname helps ensure that the File System information is only discovered once, no matter how many domains the server exists in.

### Follow these steps:

1. Search for the File System CI attribute mapping section in the xml file:

```
<!--Attribute mapping for File System CI -- >
```

2. Modify the following line to use Hostname instead of name.

```
<!-- <attributeMapping CohesionCI="File System" CohesionAttr="Hostname" CMDBAttr="name"  
CMDBFamily="*" /> -- >
```

The reconciliation of relationships is complete.

## Integration Summary

---

Integrating CA SDM and CA Configuration Automation allows the import of CI Details and Relationships into CA SDM, the ability to launch CA Configuration Automation details to view details of discovered CI attributes through the MDR launcher, and the ability to refresh CI details to help confirm changes to the infrastructure.

Cohesion's ability to detect changes from baseline or Gold standard configuration across applications and servers supports Change and Configuration Managements efforts.

# Chapter 7: CA ecoMeter

## CA ecoMeter Integration

---

This chapter discusses how CA SDM r12.6 and CA ecoMeter can be configured to work together. The following key topics are covered:

- Integration points and functionality from CA SDM
- Integration points and value from CA ecoMeter to CA SDM
- How the integration works
- Integration instructions

## What is CA ecoMeter

---

CA ecoMeter helps you better visualize, monitor, and manage the use of energy in your data centers and facilities. CA ecoMeter provides the ability to visualize your energy usage in a user-friendly interface. It also intelligently responds to alarms related to the energy consumption in your environment helping you achieve better operational efficiency and lower energy costs.

You can configure how you want to capture real-time data from the monitored devices. You can then calculate and store the estimated value after every polling interval. After you have this information, you can view both real-time and historical usage from the CA ecoMeter web interface. The view provides a clear picture of the efficiency metrics, consumption, and demand in the data center.

CA ecoMeter lets you incorporate the monitoring of devices such as air conditioning units, and electrical systems such as Generators, Power Distribution Units (PDUs), Uninterruptible Power Systems (UPS), as well as Building Management Systems into your CA Service Desk or other monitoring solution.

## Integration Details

---

The integration of CA ecoMeter with CA SDM creates a ticket in CA SDM when an alarm is raised in CA ecoMeter. CA SDM can receive the alerts from CA ecoMeter through email, web services call, or text API. However, this document only covers the alerts delivered through email to CA SDM. Although, the integration is bidirectional, that is both the products can communicate and share information among each other, this document only covers the integration from CA ecoMeter to CA SDM. It is possible to send information from CA SDM to CA ecoMeter, but that is not covered in this document.

### Integration Points and Functionality from CA SDM

The integration uses the inbound email functionality which was previously known as "maileater" in CA SDM. The email functionality is configured from the Administration tab of the main user interface under the Email node. You can also use alternate approaches using the web services API or the `pdm_text_cmd.exe` utility, but these are not covered in this document.

### Integration Points and Functionality from CA ecoMeter

The integration from CA ecoMeter uses the Live Exceptions tool from CA eHealth. Specifically, the integration leverages the profile and rule message functionality. You define a threshold on elements that CA ecoMeter is monitoring. When the configured condition is met, the notifier rule associated with the profile and rule message is used to launch a simple script which creates a formatted email and sends it to CA SDM.

**Note:** CA eHealth is part of the CA ecoMeter solution offering.

### Integration Value

The CA ecoMeter integration provides the following values:

- CA ecoMeter sends alarms which are related to equipment like air conditioning units, generators, and building management systems in the data center, to CA SDM. The alarms help the service desk personnel to fix high severity issues, by providing complete insight into the potential causes for an outage or service disruption.
- Apart from helping to expedite the resolution of the incident, the integration can even help avert service outages related to these devices. The integration provides warning of an alarm condition in advance, by using the monitoring rules.

## Integration Example

### Configure the Integration from CA SDM

To configure the integration from CA SDM, activate the mailbox functionality introduced in CA SDM r12.5. If you are using a release preceding CA SDM r12.5, the email configuration is different. For more information on configuring the mailbox functionality on prior releases, see the *Implementation Guide and Administration Guide* of the respective releases.

#### Follow these steps for CA SDM r12.5:

1. Click the Administration tab in CA SDM and navigate to Email, Mailboxes as shown in the following screenshot:

The screenshot displays the CA Service Desk Manager Administration interface. The left sidebar shows a navigation tree with 'Mailboxes' selected under the 'Email' category. The main content area is divided into two panes. The top pane, titled 'Mailbox List', shows a table with one entry: 'Default' with an 'Email Type' of 'NONE'. A red arrow points from this entry to the 'Default Mailbox Detail' pane on the right. The 'Default Mailbox Detail' pane shows configuration options for the 'Default' mailbox, including 'Check Interval (in Sec)' set to 30, 'Email Type' set to NONE, and various attachment and security settings.

Name	Email Type	Check Interval (in Sec)	Active
Default	NONE	30	Active

User Name	Password	Security Level
NONE		Clear Text

Attachment Repository	Attach Entire Email	Force Attachment Splitout
No	No	No

Allow Anonymous	Save Unknown Emails
No	No

Details

Initial Mailbox

Last Modified Date

Last Modified By

1. Rules

2. Policy

Mailbox Rules

Create New Export

2. Complete the fields with the required information.

For more information on how to configure this functionality, see the section "Email Administration" in Chapter 4, "Implementing Policy", of the *CA SDM Administration Guide*.

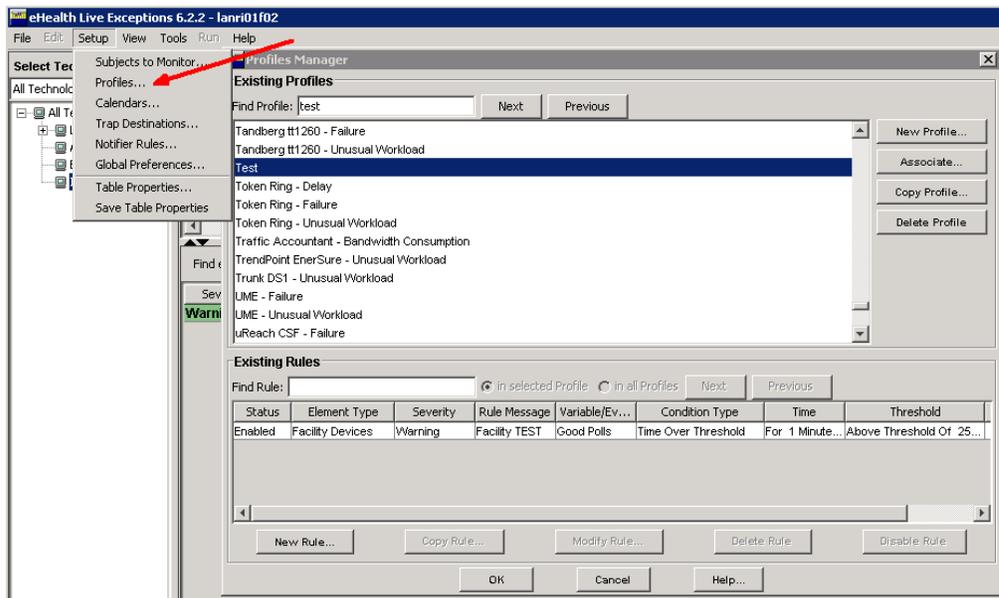
## Configure the Integration from CA ecoMeter

### Create a Profile

A profile includes the elements that you want to monitor in CA ecoMeter.

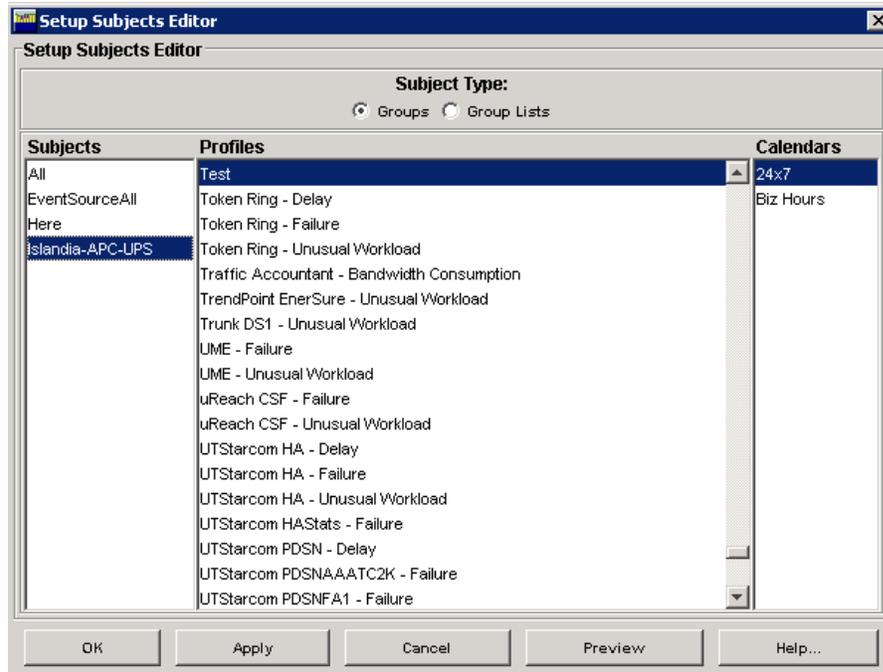
#### Follow these steps:

1. Open the eHealth Live Exceptions tool that is part of CA eHealth.
2. Click Setup, Profiles from eHealth Live Exceptions.
3. Click New Profile to define the profile and the rules of the profile as shown in the following screenshot. The screenshot shows a simple test profile and rule message that is used to generate a test email message:



4. Click Associate in the Profiles Manager dialog to associate the new profile with the required elements group that is being monitored.

The Setup Subjects Editor opens. The following screenshot shows the existing subjects, profiles, and calendars:



5. Select the group, profile, and the calendar and click OK.
6. Click OK to confirm your selection in the next dialog.

The profile is created.

## Create a Notifier Rule

A notifier rule specifies the actions to take when an alarm is raised, cleared, acknowledged, or unacknowledged.

### Follow these steps:

1. Click Setup, Notifier Rules....

The Notifier Manager dialog opens.

2. Click New and complete the following fields in the Notifier Rule Editor:

- a. **Name:** Test

- b. **Action:** Run Command

3. Complete the following fields:

- a. **Command:** email.sh ServiceDeskMailBox@abc.com

- b. **When an alarm is:** Select all the options

4. Complete the following fields under the Monitored Using category:

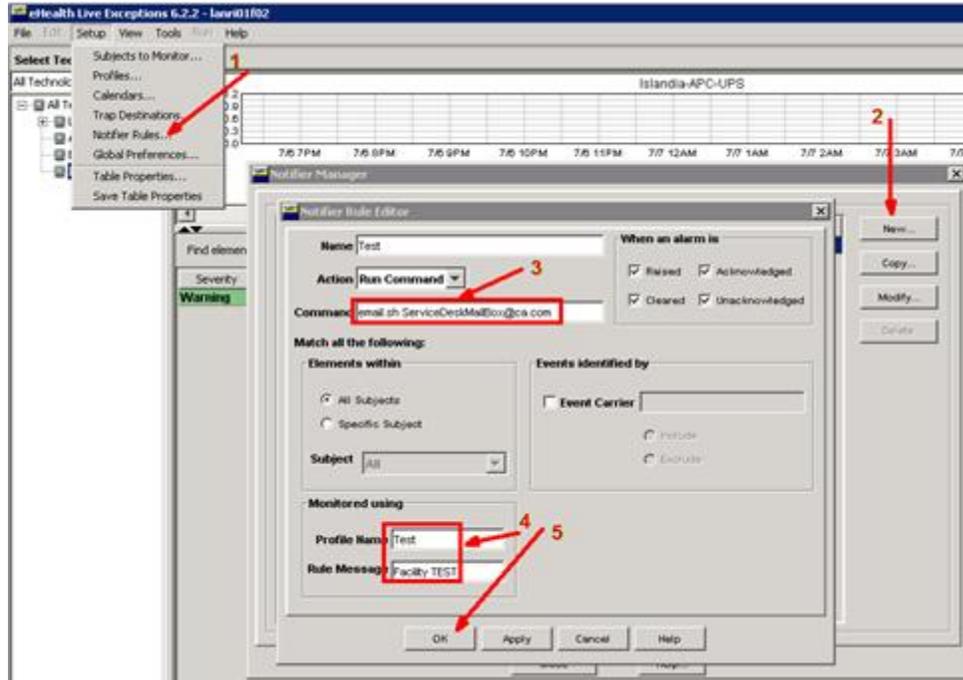
- a. **Profile Name:** Test

- b. **Rule Message:** Message sent to CA SDM

5. Click OK.

The rule is created.

The following screenshot shows a completed dialog:



## Create an Email Script

CA ecoMeter uses the email script to generate the alert emails that are sent to CA SDM.

### Follow these steps:

1. Open a text editor and copy the following content to a new file:

```
#!/bin/sh
RECIPIENT=$1
shift 1
SEVERITY=$1
RULE_MSG=$5
ELEMENT=$4
shift 9
REASON=$8
shift 9
ALARMID=$7
SUBJECT="ALARM FROM CA ecoMeter"
BODY=`echo "CA ecoMeter ALARM REPORTED THE FOLLOWING: $REASON $SEVERITY $RULE_MSG
$ELEMENT Alarm ID-$ALARMID"`
nhMail -e "$SUBJECT" "$BODY" $RECIPIENT
```

**Note:** The first parameter in the previous code snippet, is for the RECIPIENT's email address. The email address is not part of the eHealth event data, it is passed to the script from the notifier rule in CA ecoMeter.

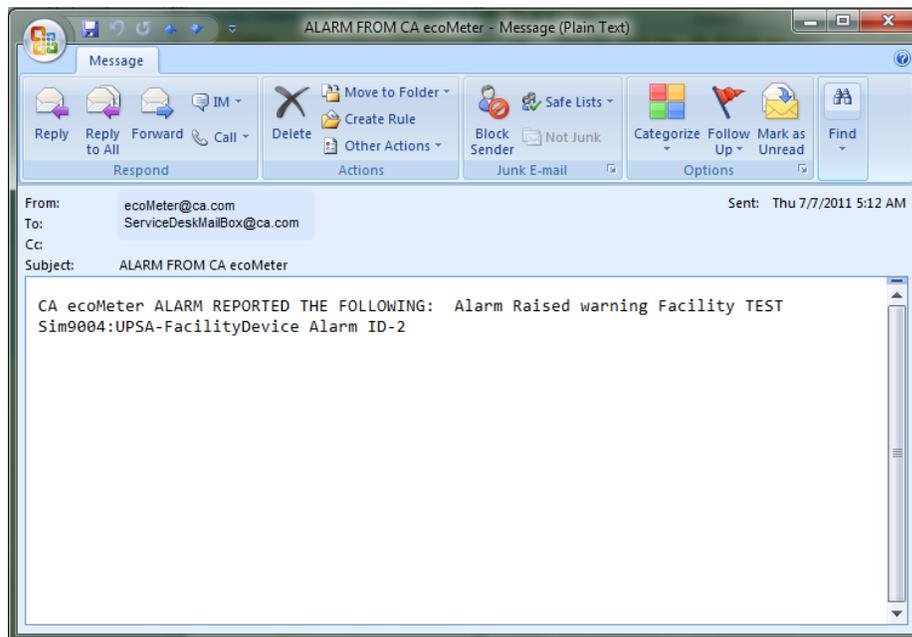
This script takes the required variables from the eHealth Live Exception event data and places them into a formatted email that is sent to the CA SDM mailbox. The variables in the previous code are just a small sample of the available variables. The following additional variables are available from the eHealth event data, which you can use:

```
[Severity]
[Start Time]
[Start Time(UTC)]
[Element Name]
[Rule Message]
[Tech Type]
[Variable]
[Problem Start Time]
[Problem Start Time(UTC)]
[Problem Duration (seconds)]
[Condition Type]
[Profile Name]
[Group Name]
[Group List Name]
[Event Carrier]
[IP Address]
[Reason]
[Server Port]
```

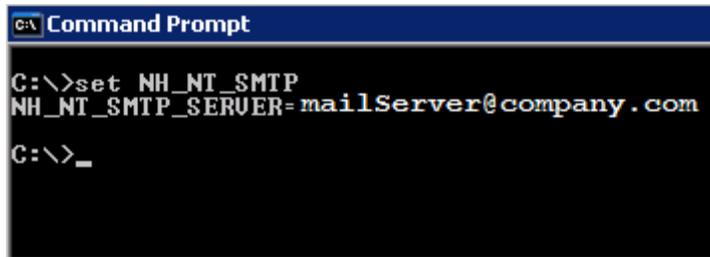
[Server IP Address]  
 [eHealth Server Name]  
 [Element ID]  
 [Element Alias]  
 [Component]  
 [Description]  
 [Alarm ID]  
 [Ack]  
 [Ack User]  
 [Ack Time]  
 [Ack Time (UTC)]  
 [Ticket #]  
 [Status]  
 [Assigned]  
 [Notes]

2. Save the file as email.sh in the \$NH\_HOME\bin directory. \$NH\_HOME represents the eHealth Performance Manager installation directory.

This configuration results in the following email being generated and sent in response to an alarm condition:



3. Verify that the NH\_NT\_SMTP\_SERVER environment variable is set to the SMTP email server of your company as shown in the following screenshot:



```
CA\ Command Prompt
C:\>set NH_NT_SMTP
NH_NT_SMTP_SERVER=mailServer@company.com
C:\>_
```

The configuration of the integration is complete.

## Testing the Integration

### Follow these steps:

1. Create a condition that activates your test rule and launches the Notifier Rule.
2. Confirm that your email has been sent to the email address in your Notifier Rule command field.
3. Proceed with activating the CA Service Desk mailbox functionality and confirming that a new ticket has been opened in response to the email that is sent.

## Troubleshooting the Integration

If the integration is not generating notifications as expected, use the eHealth oneClick tool to assist in troubleshooting.

### Follow these steps:

1. Launch the eHealth oneClick application. Click Start, All Programs, eHealth 6.X, oneClick for eHealth.
2. Navigate to the Tasks and Information, Setup node.
3. Click Advanced Logging.

The Advanced Log Components dialog is displayed.

4. Select the Notifier option.
5. Click View Advanced Logs.

You are directed to the Server Files,eHealth, Log, Advanced node.

6. In the right pane, double-click the file named nhNotifierSvr\_XXXXXX.txt, where XXXXXX is a random number generated by eHealth.

The log details for the notifier are displayed in the bottom pane.

## Integration Summary

---

To summarize, this simple integration provides a powerful way to help integrate the monitoring of your energy and cooling devices into the same management system as the rest of your IT environment. The integration lets you respond more quickly and effectively to alerts and troublesome conditions, before they can have a negative impact on the delivery of your IT services.



# Chapter 8: CA NSM

## Integration Example- Service Desk and NSM

---

### Business Challenges

An IT infrastructure comprises thousands of individual elements from the major domains in networks, systems, applications and databases. The number of potential points of failure may easily exceed 100,000. The CTO of an organization requires the VP of IT Services to coordinate all necessary components. The VP has to guarantee that when an incident occurs in the enterprise it gets resolved quickly, and with minimal impact and expense to operations. He also has to make sure that all IT resources operations are available round the clock.

### CA Approach

Organizations face many challenges — the need to control costs, the ability to manage growing IT complexity, and the increasing demand to achieve service-level objectives that support business needs. To meet these challenges, the availability and performance of the underlying IT elements that are the foundation for critical business processes. To maximize service availability, IT Management relies heavily on intelligence and automation, as specified by business-defined policy, for the automated resolution of incidents in real time.

To effectively manage the delivery of service support and meet critical SLAs, IT components must be aligned with and managed as part of the business service. When an incident occurs, it must be resolved in the least time possible. Information about the incident should be captured for both real-time tracking and historical analysis, and reports that help the IT departments to take proactive actions must also be generated. These reports and the information about the incident guarantee the enhanced productivity of IT resources, greater efficiency, and reduced operating costs. CA recommends taking advantage of the integration between Service Desk and NSM systems which are currently under production.

## Configuring a Solution

Once an operations team has defined specific Incident Management policies for business services; these policies can automatically set the severity of the Incident, the person or group to whom the incident should be assigned, priority, category, SLA and so on for each type of Incident. These definitions are used to establish automatic escalation policies. This feature, that is, the capability to verify that problems are not lost and the appropriate people are notified about the progress of the incident, makes the automation of Incident Management powerful. With the knowledge that Incident Management policies have been defined, the NSM and Service Desk integration-configuration, take advantage of the integration points available in NSM through Alert Management System (AMS), the Management Command Center (MCC) and the Unicenter Portal (UP) functionalities.

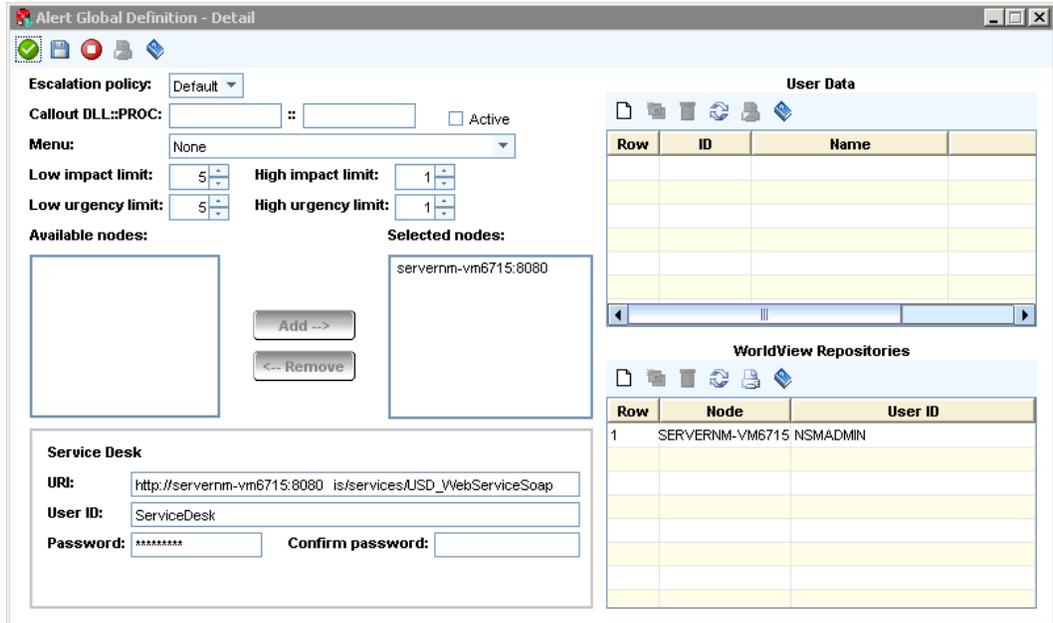
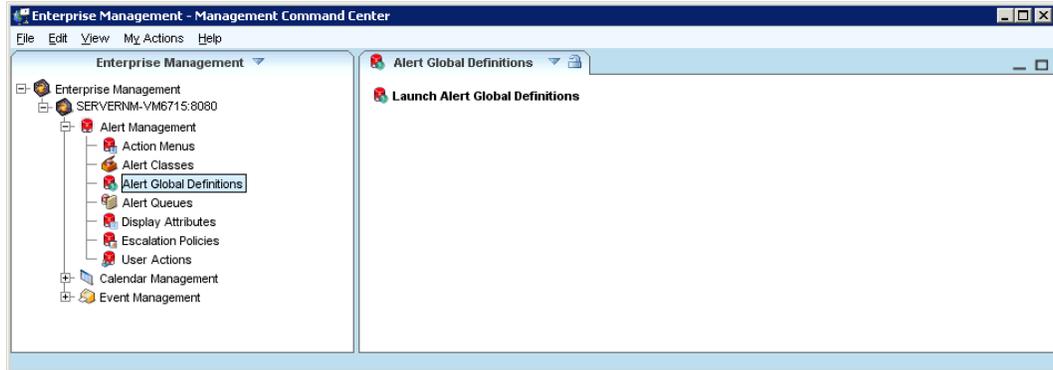
For more information on NSM installation, refer to the *NSM Installation Guide*.

## Best Practices

- Establish equipment configuration: Identify those system components that are candidates for incident tracking.
- Establish Incident Policies: Identify how incidents are going to be classified and assigned (Incident categories, status codes, and responsibility areas for example).
- Establish Incident escalations Policies: Define how priorities and responsibilities are to be changed based upon how long a problem has been unresolved.
- Be sure that Alert Management modules are installed prior to beginning the integration.

### Configuring Alert Management to Work with Service Desk Example

1. Log in to the NSM server and start configuring AMS. Launch the Alert Global Definition GUI, which can be done from either through the classic EM interface or through the MCC. The example that follows shows how to accomplish the integration using the Management Command Center(MCC).
2. Start the MCC and navigate using the left hand drop-down menu on the left of the Enterprise Management Section.
3. In the Alert Management Folder, click on Alert Global Definitions and then click the Launch Alert Global Definitions link in the right hand pane.



4. In the Service Desk Panel set the URI, User ID and Password.
  - **URI (Uniform Resource Identifier)** : Identifies the address of the web server on your Unicenter Service Desk Primary Server.
  - For Unicenter Service Desk r12.x, the default is `http://servername[:port]/axis/services/USD_WebServiceSoap`

**Note:**If the Unicenter Service Desk is hosted on a secure web server , as indicated by “https” in the URI, import the server’s SSL certificate to the server on which AMS is hosted. Refer to the Install the Service Desk SSL Certificate procedure included in the Unicenter NSM Inside Event Management and Alert Management Guide for details.
  - **User ID** : Identifies the userid used to access Unicenter Service Desk.
  - **Password** : Corresponding password for the above user.
5. In the WorldView Repositories Panel, click the New button. Enter the desired WorldView Repository, and appropriate User ID and Password. Click the Green icon to save.
6. In the available nodes panel, select nodes that this Alert Global definition applies to, and click the Add button to move your selections to the Selected nodes.
7. Click the green icon to save and exit.
8. In the Alert Management Folder click Alert Queues in the left hand pane and then click the new icon on the right hand pane to create a new Alert Queue. Name the queue,for example, Green Book Queue. Click the green icon to save and close.

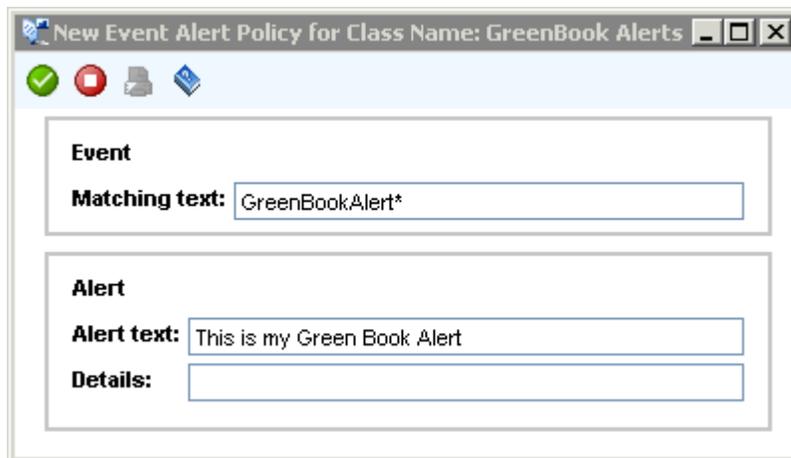
The new queue has now been created and is available in the MCC and UMP.





10. On the Asset Class detail window, click the Message Policies tab. Click the new icon to create a new event policy for the Green Book Alert Class.

Specify GreenBookAlert for the Event matching Text and "This is my Green Book Alert" for the Alert Text. Click the green icon to save.



11. From the Asset Class detail window click the Actions tab. Check the Create request when alert is opened box, and the Synchronize closure of requests alerts.box. In the URL text field above the 'Add to URL' button, enter the CA SDM URL. Click the green icon to save.

**Alert Class - Detail**

Main Limits Appearance **Actions** Message Policies AEC Policies

**Action define**

Create action: None Transfer action: None

Acknowledge action: None Close action: None

**Service Desk**

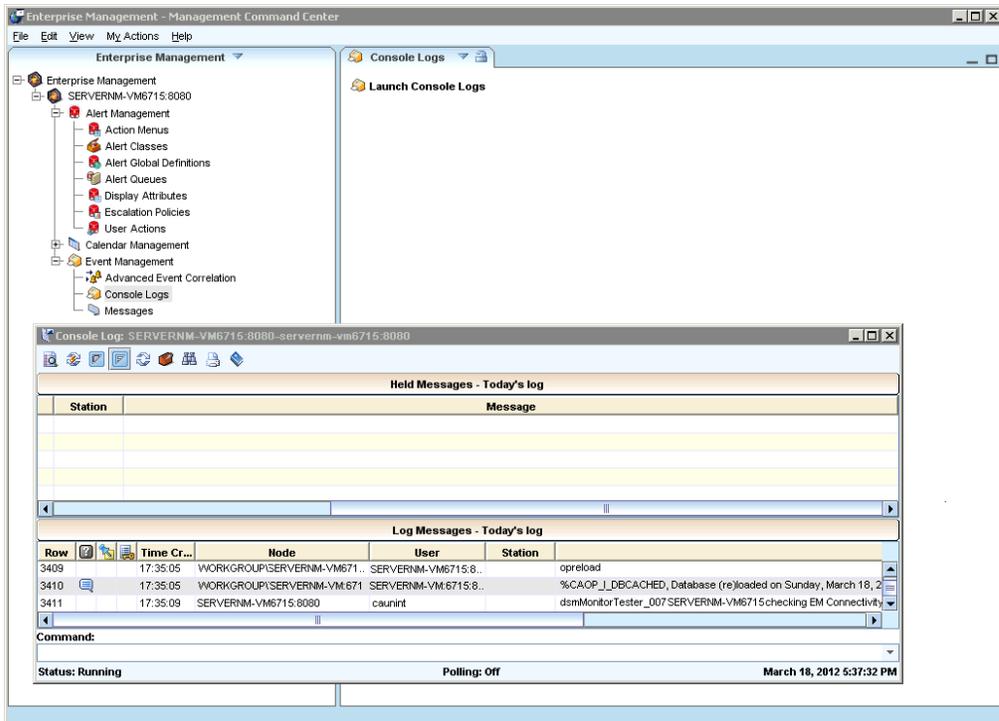
Create request when alert is opened  Synchronize closure of requests and alerts

**URL**

URL:

Available URL parameters: Ack

12. Hit the green icon to save and exit Alert Queue
13. Run the following command from a command prompt to load the new MRA (Message/Record/Action) into Event Management:  
  
"opreload"
14. Validate that the new MRA was loaded into Event Management. In the Event Management Folder click the Console Logs tab and then click the Launch Console Logs link.



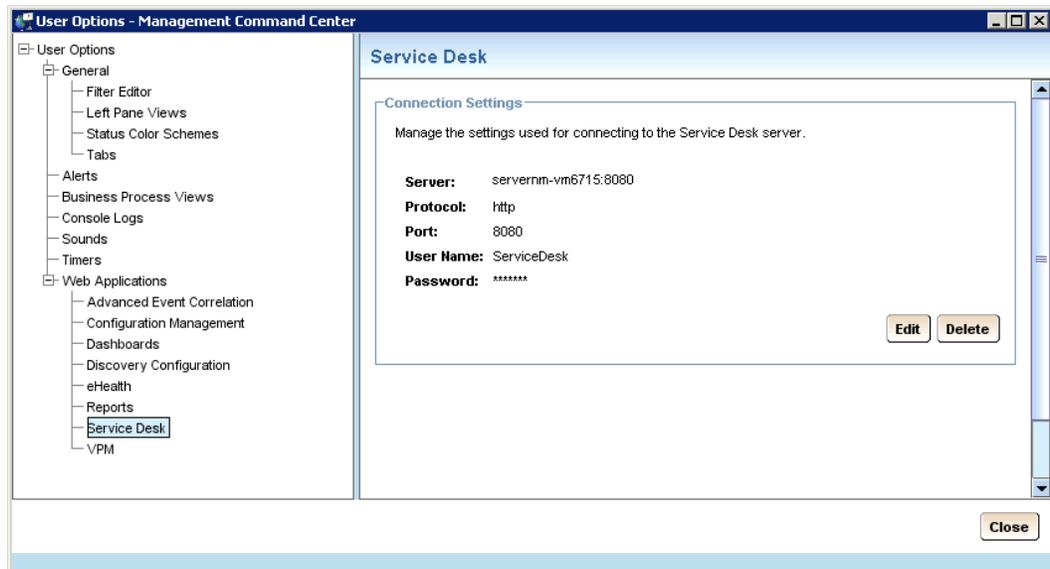
## Configuring MCC (Management Command Center) to Integrate with Service Desk Example

When Service Desk is configured with the MCC it enables you to launch Service Desk from within the Management Command Center. You can Create Request, View Alert Request, View Request and use Knowledge Tools. To configure MCC with Service Desk, launch MCC and navigate using the menu.

### Follow these steps:

1. Click View, Options, Service Desk.

The Connections Settings displays. You can view or modify the Service Desk Connection Settings as necessary.



## Testing Service Desk - NSM Integration

Once everything is configured, you can test the integrations to help ensure complete functionality. The following integrations are enabled:

- Automatic Incident Creation.
- Interactive Options in the MCC. The options are, Create Request, View Alert Request, View Request, and Searching in Knowledge Tools.
- End-User Interactive actions from 2D Map.

### Testing Automatic Incident Creation

You can simulate an alert by issuing the following command from a command prompt:

```
cawto GreenBookAlert This message was created via cawto from a command prompt
SDTicketType=I
```

**Note:** By default the integration creates a New Request. Including SDTicketType=I in the alert message text enables AMS to create a New Incident verse a new Request.

Once AMS captures and processes this alert a New Incident is created in SDM.

The screenshot displays the CA Service Desk Manager interface. At the top, the title bar reads "CA Service Desk Manager" with a search bar set to "Incident" and user information "ServiceDesk Log Out". The main menu includes "File", "View", "Activities", "Actions", "Search", "Reports", "Window", and "Help".

The incident details for "26 Incident Detail" are shown in a table format:

Reported By	Assignee	Group	Affected Service
ServiceDesk	ServiceDesk		
Urgency	Impact	Major Incident	Configuration Item
5-Immediate	3-Single Group	No	servernm-VM6715:8080
Problem	Symptom	Resolution Code	Resolution Method
Call Back Date/Time	Change	Caused by Change Order	External System Ticket

Below the details is a "Summary Information" section:

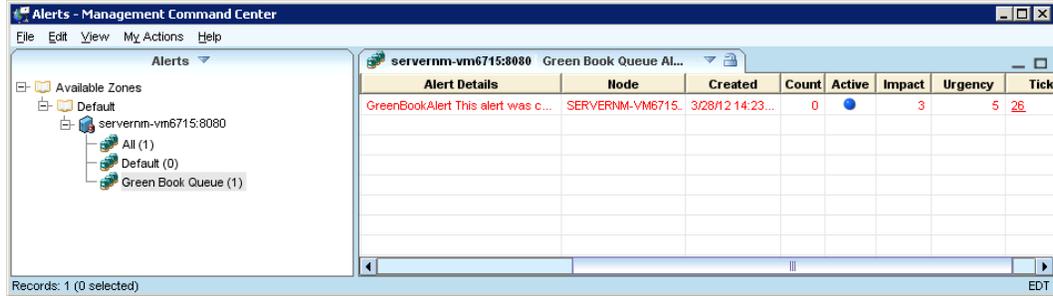
- Summary:** This is my Green Book Alert. Total Activity Time: 00:00:00.
- Description:** WORKGROUP\SERVERNM-VM6715:8080 reenBookAlert This alert was created via cawto from a command prompt.SDTicketType=I
- Open Date/Time:** 03/28/2012 02:24 pm
- Last Modified:** 03/28/2012 02:24 pm
- Resolve Date/Time:**
- Close Date/Time:**

The interface also features tabs for "1. Additional Information", "2. Logs", "3. Knowledge Management", and "4. Relationships". Under "2. Logs", there are sub-tabs for "1. Activities", "2. Event Log", and "3. Support Automation".

The "Incident Activity Log List" section includes a search bar and buttons for "Search", "Show Filter(\$)", "Clear Filter(\$)", and "Export". The log table is as follows:

Type	Created By / Description	On	Time Spent
+ Log Comment	ServiceDesk	03/28/2012 02:24 pm	00:00:00
+ Adjust Impact Urgency	ServiceDesk	03/28/2012 02:24 pm	00:00:00

In the Green Book Queue in MCC - Alert Management, you see the generated alert that caused the creation of the New Incident in SDM. The associated Ticket Number and the Impact and Urgency of the Incident is referenced in the Alert record as well.



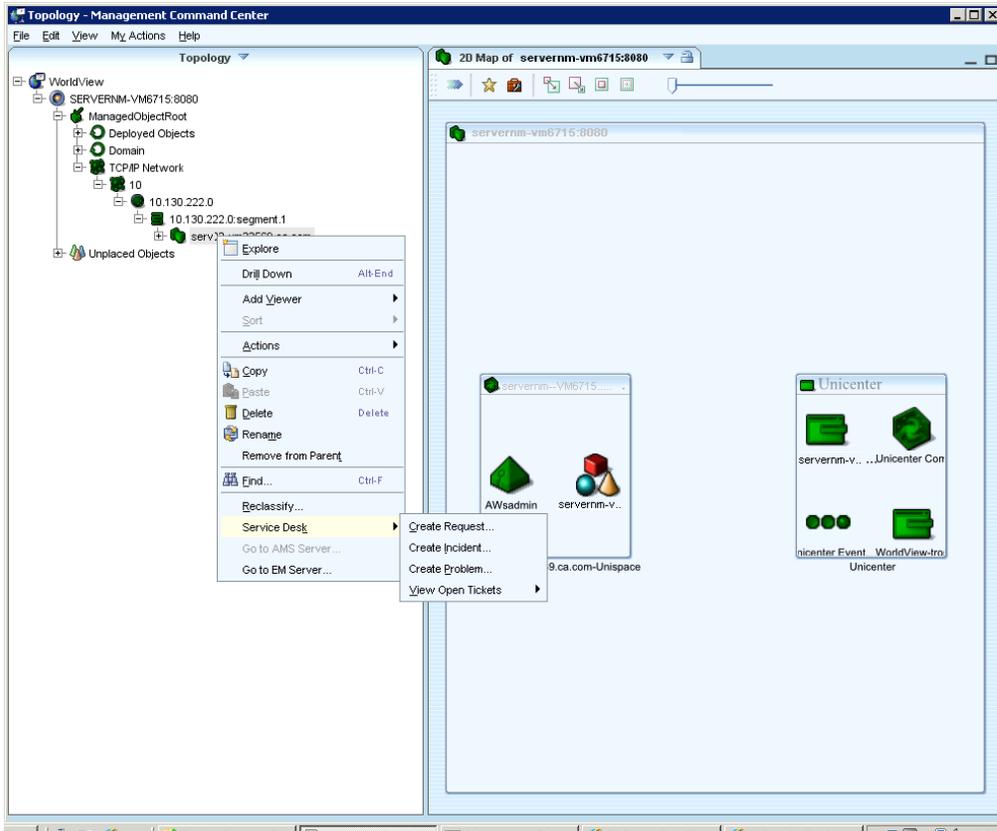
For more information on all the options available for this integration such as how to create an Incident versus a request please refer to the Inside Event Management and Alert Management Guide on the NSM r11.2 SP2 installation DVD.

## End-User Interactive Actions from Management Command Center

You can access the Service Desk Integration launch points from within the Management Center.

### Follow these steps:

1. Select either Topology or Business Process Views from the drop-down list on the left hand menu.



2. Right click any Host object in the left hand pane hierarchy tree and select Service Desk from the menu. The following submenu options are available:

#### Create Request

Lets you create a new Service Desk request using the selected object as the Configuration Item (CI) that is affected. The selected object is also the subject of the request being created.

#### Create Incident

Lets you create a new Service Desk incident using the selected object as the Configuration Item (CI) that is affected. The selected object is also the subject of the incident being created.

#### Create Problem

Lets you create a new Service Desk Problem using the selected object as the Configuration Item (CI) that is affected. The selected object is also the subject of the problem being created.

#### View Open Tickets

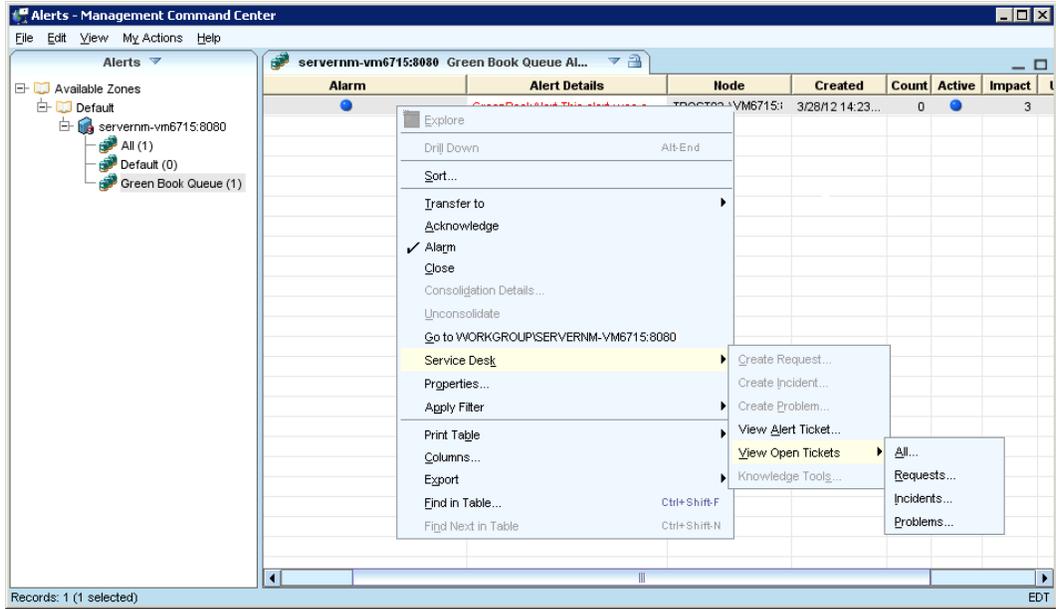
Lets you view all open Tickets which are created within Service Desk for the selected object, or all requests which are related to this CI.

A Service Desk menu is also available within the Alerts view of the MCC. You can access that menu item and its submenus.

#### **Follow these steps:**

1. Right click the alert in the right hand pane of the MCC and select Service Desk.

# Integration Example- Service Desk and NSM



The following submenu options appear:

#### Create Request/Incident/Problem

Lets you create a Service Desk ticket using information extracted from the currently selected alert. This option is only available if AMS has not already created a Service Desk ticket. The Service Desk summary field is populated from the alert text field and the Service Desk description field is populated by the alert detail field.

#### View Alert Ticket

Lets you configure AMS alert classes and escalation policies to create a Service Desk ticket automatically. This option is only available if AMS has already created a Service Desk ticket. The ticket number is stored as an attribute within the alert or request as discussed in the previous section. If a ticket has been created, this option automatically invokes the Service Desk user interface directly in context to the relevant ticket.

#### View Open Tickets

Lets you view all Service Desk requests for the node where the alert originated.

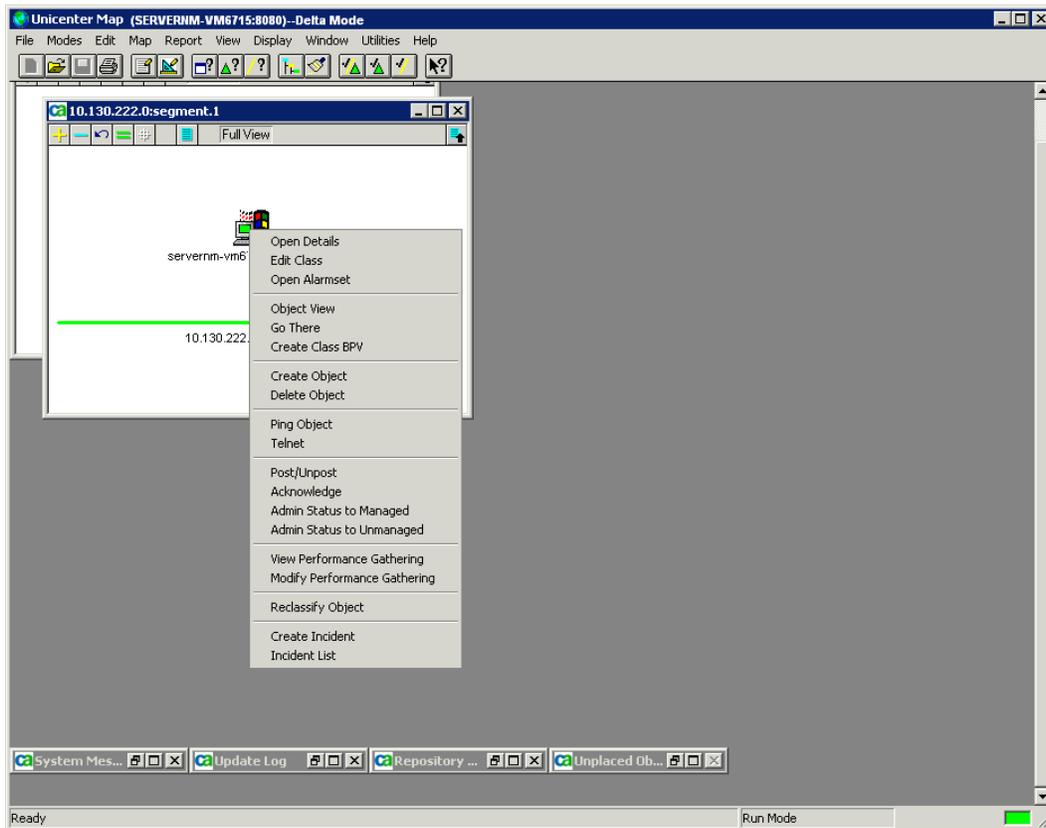
#### Knowledge Tools

Allows you to invoke a search of the Service Desk Knowledge Tools in context, using the Alert Text as a search argument. The result is a display of all Knowledge Base articles that are potentially related to the alert.

For more information on all the options available for this integration such as how to create in Incident verses a request please refer to the "Inside Event Management and Alert Management Guide" on the NSM r11.2 SP2 installation DVD.

## End-User Interactive Actions from 2D Map

Right click any Host on the 2D Map. A menu is displayed with the options of Create Incident or Incident List for the object selected. The following screenshot illustrates the menu options:



### Create Incident

Lets you view the Incident using the selected object as the Configuration Item (CI) that is affected. The selected object is also the subject of the incident being created.

### Incident List

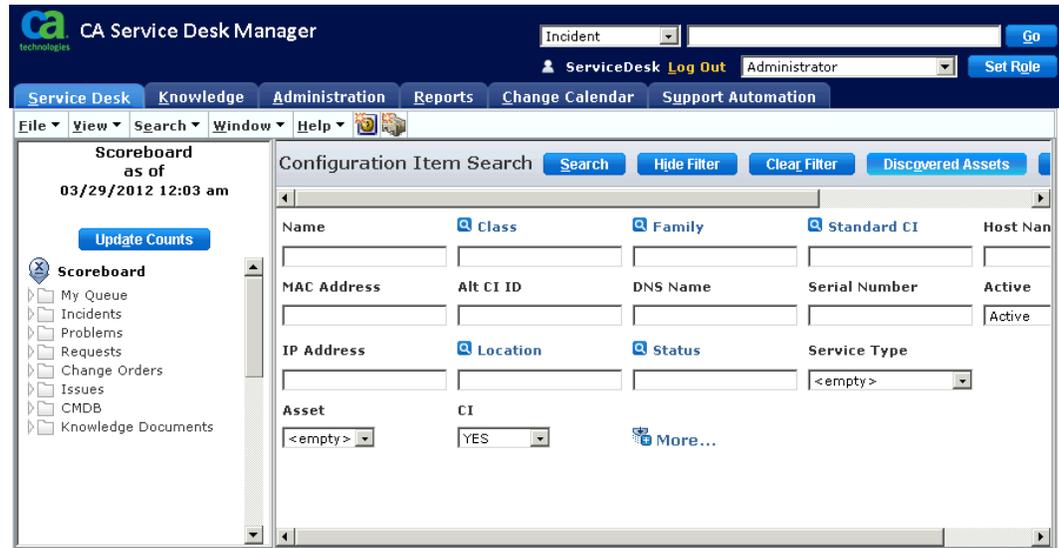
Lets you view all incidents which are created within Service Desk for the selected object, or all incidents related to this CI.

### Miscellaneous Integrations

Discovered Assets, which are Assets that are found using NSM discovery tools, can be seen and imported as Configuration Items into Service Desk.

**Follow these steps:**

1. On the Service Desk tab, click Search, then Configuration Items.
2. In the Configuration Item Search form, click the Discovered Assets button.



Copyright © 2011 CA. All rights reserved.

3. Click the Search button on the Discovered Search Form.

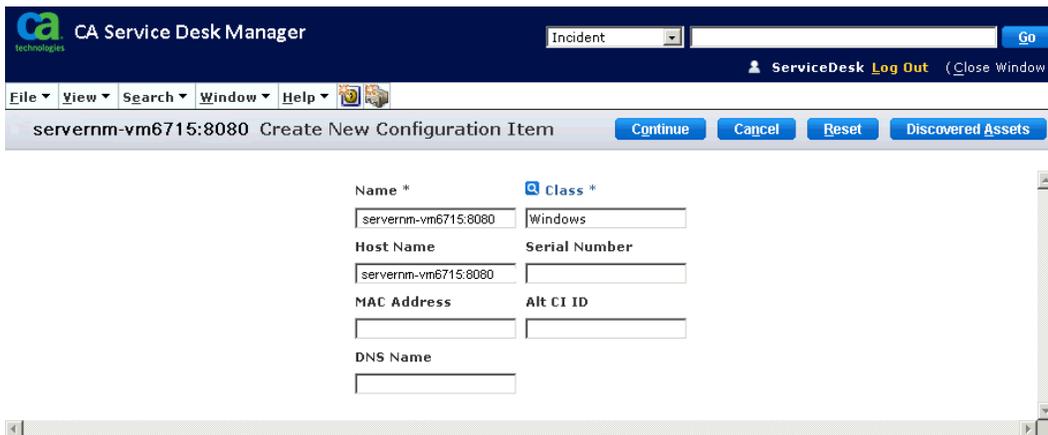
All Assets that have been discovered by NSM and not yet imported into SDM will display in the Discovered Asset List form.



- To import the Asset right click the Asset you want to import.
- Click the Create New Configuration Link.



- Select the appropriate class and enter any other known unique properties of the configuration item.
- Click Continue.



- Enter any other information related to the Configuration and click the Save button.

A new Configuration Item is created.

**Note:** A Configuration Item will automatically be created in Service Desk should a Ticket be created via an AMS alert against an Asset/Configuration Item that doesn't already exist in Service Desk

Another integration you can configure is the ability to create an Incident in Service Desk whenever an object is changed in NSM. In the Service Desk environment variable definition file, NX.ENV, the following four variables enable this behavior:

```
@NX_TNG_OBJECT_UPDATED_SUBSCRIBE=NO
```

```
@NX_TNG_OBJECT_ADDED_SUBSCRIBE=NO
```

```
@NX_TNG_OBJECT_DELETED_SUBSCRIBE=NO
```

```
@NX_TNG_OBJECT_STATUS_UPDATED_SUBSCRIBE=NO
```

These variables are set to NO during installation. To enable one or more simply edit the NX.ENV and change one or more to YES depending upon which event(s) you wish to create an Incident for.

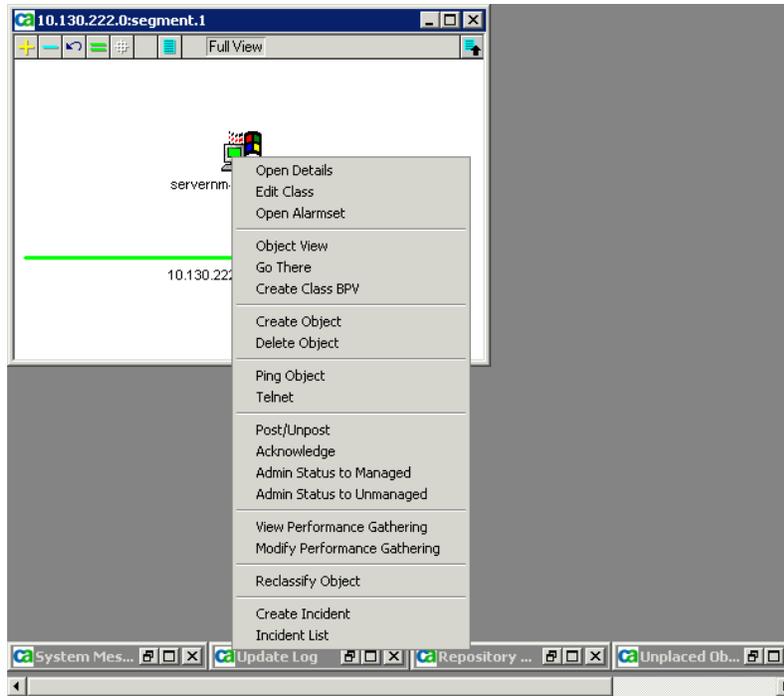
In this example we are changing @NX\_TNG\_OBJECT\_STATUS\_UPDATED\_SUBSCRIBE from NO to YES.

```
@NX_TNG_OBJECT_STATUS_UPDATED_SUBSCRIBE=YES
```

This will cause NSM to create a Service Desk Incident every time an object status changes. After the change is made a recycle of Service Desk is required.

**Follow these steps:**

1. Update navigate to an object in the Worldview Map.
2. Right click it, then click Open Details.



3. Click the Status Tab and change the Status: text to System is Unreachable and the Severity to MAJOR , then click OK.

## Service Desk - NSM Integration Summary

Unicenter NSM creates Service Desk incidents based on policies defined in Event Management System (EMS), Advanced Event Correlation (AEC), and Alert Management System (AMS). This following events take place:

- AEC rules or EMS message records and actions evaluates a situation. An alert is generated if the event is serious
- AMS class or escalation policy determines that a Service Desk request is appropriate, and creates one.
- Unicenter NSM comes with EMS, AEC, and AMS policy that can automatically create and close Service Desk requests. You can also write your own policy using message records and actions, correlation rules, and alert classes and escalation policies.
- Unicenter NSM interacts with Unicenter Service Desk in the following ways:
- Alert policy definitions specify that Service Desk incident be opened and closed during the life cycle of an alert:
- Open a Service Desk request when an alert is created. Use the Alert Class Window.

**Note:** AMS does not open an incident if an existing incident has identical summary, description, and asset properties. This prevents multiple trouble tickets describing the same root problem.

- Open a Service Desk request when an alert is escalated. Use the Escalation Policy Editor.
- Close a request when the alert that opened it is closed or made inactive. Use the context menu in the Unicenter MCC to close an alert; use the Alert Class window Main page or Alert Properties dialog Status page to make an alert inactive.
- Alerts that are associated with Service Desk requests include the request reference number. Likewise, Service Desk requests created by alerts indicate that an outside application opened the request.
- The activity log of a Service Desk request is updated automatically with additional information from AMS when duplicate alerts are created.
- The context menu in the Unicenter MCC lets you interact manually with the Service Desk. You can view requests, open a request, and search the Service Desk Knowledge Tools. For example, when you right-click an alert, you can see requests associated with that alert. When you right-click a managed object in the 2D Map or Topology view, you can see requests for the selected node.

## Use Cases

This section contains examples of situations that could trigger the creation of an alert and a Service Desk Incident.

### Use case 1: System Agent on a Critical Server

- An agent metric exceeds a threshold.
- An Event Management System (EMS) event is generated.
- EMS message record policy creates an alert for this event.
- AMS escalation policy opens a Service Desk request because the alert is opens more than 30 minutes.
- A technician resolves the issue and closes the alert, and the Service Desk incident is closed automatically.

### Use case 2: Third-Party Software

- Third-party software produces a series of events in the system log indicating a failure.
- EMS captures the events.
- AEC policy evaluates the events and creates an alert.
- AMS class policy opens a Service Desk request immediately.
- Operations staff resolves the problem and closes the alert. The Incident is closed automatically.



# Chapter 9: CA Spectrum Infrastructure Manager Integrations

## Overview

---

This chapter discusses how CA Service Desk Manager r12.6 and CA Spectrum Infrastructure Manager r9.2 (CA Spectrum IM) can be configured to work together to support event, availability, capacity, and incident management. This chapter also includes information about adding CA Service Operations Insight r3.0 (CA SOI) to the solution. The following key topics are presented:

- Overview of the CA Spectrum Infrastructure Manager integration and value
- Integration and configuration instructions
- Introducing CA Service Operations Insight into the Environment
- Introducing CA eHealth into the Environment
- Introducing CA APM into the Environment

## CA Spectrum Infrastructure Manager Integration

---

CA Spectrum is a services and infrastructure management system that monitors the state of managed elements including devices, applications, host systems, and connections. It collects and stores status information such as fault and performance data from these elements. CA Spectrum IM constantly analyzes this information to track conditions within the computing infrastructure. If an abnormal condition is detected, it is isolated and you are alerted.

CA Spectrum includes the following client applications:

- **OneClick:** The main client application providing a graphical user interface that is used to monitor the network and launch other client applications. The modeling features offered in OneClick client are used to create and maintain accurate software models of the network and to enable CA Spectrum IM to determine actual points of failure and suppress superfluous alarms.
- **AlarmNotifier:** This application is used to forward alarm data to user-defined scripts or third-party applications.

**CA Spectrum Alarm Notification Manager (SANM):** This application is used with the AlarmNotifier to specify policies that filter alarm data sent to user-defined scripts or third-party applications.

On the CA Spectrum IM side, Spectrum OneClick client and Spectrum Alarm Notification Manager (SANM) drive the integration.

## Integration Points and Value

The true value of this integration lies in its ability to identify the interrelationships between the business critical network resources which CA Spectrum IM manages and monitors, and the business services that CA Spectrum IM supports. This knowledge can reduce mean time to repair by supporting root cause analysis. It can also help minimize the future disruption of business services by providing a clearer picture of the potential business impact of changes to the CIs that support those services.

CA Spectrum IM integrates with CA Service Desk for event, availability and incident management as follows:

- Any Incident opened as a result of an Event detected from an IT Service is logged and any additional Incident opened for any other component comprising the IT Service will be linked to the original Incident.
- CA Spectrum Alarm Notification Manager (SANM) is used to provide automatic incident creation in CA SDM through SANM Policies based on date, time, alarm severity, alarm cause, IP, and device type.
- The integration with CA Spectrum IM enables the population of the CMDB with the relevant CA Spectrum discovered network resources that are crucial to helping make business services available to end users.
- With CA Spectrum IM, CA SDM allows for a federated approach of the collection of capacity attributes by utilizing Management Data Repository (MDR) links from Configuration Item (CI) records.
- Defining CA Spectrum IM as a CA SDM Management Data Repository (MDR) gives a broad view of the resources used in the environment, and, particularly when coupled with information provided by other MDRs, supports root cause analysis and change impact analysis scenarios.

## Integration Preparation

Before you implement the integration between CA Spectrum IM and CA SDM, the following important considerations have to be carefully evaluated:

- Are there different requirements between the initial CI load situation and the subsequent CA Spectrum export\CA SDM import, and how frequently must these updates be made?
- Which types of CIs will be exported from CA Spectrum and imported into the CMDB?
- The default export configuration limits the exported CI types to CA Spectrum device models and service models.
- Which CI attributes and relationships per CI type are going to be exported from CA Spectrum and imported into the CMDB?
- Which other sources, typically referred to as Management Data Repositories (MDRs), are going to contribute information regarding the same CIs exported from CA Spectrum?
- How is proper reconciliation of a CI object ensured when attributes of the same object are imported from other MDRs? For example, if CA Spectrum service objects are imported into the CMDB as CIs of the CMDB Service family, it will not reconcile with any existing CIs or if the same CI has other MDRs with the default configuration. In these situations, it is recommended that you modify the CA Spectrum export prior to loading the CIs into the CMDB.
- How are updates of attributes controlled when the same attributes can be imported from different sources?

For example, should you be able to update the exact same attributes from different sources, and if yes, which source takes precedence?

- How are updates of relationships between CIs controlled when relationships are imported from multiple sources?
- What are the MDR relationships and launch capabilities when importing from different sources?
- How has the CA Spectrum architecture been deployed? For example:
  - A single SpectroSERVER propagating data into CA SDM
  - Multiple SpectroSERVERs in a single CA Spectrum cluster propagating data into CA SDM.  
**Note:** Some CIs will overlap on the SpectroSERVERs.
  - Multiple stand-alone, non-distributed SpectroSERVERs propagating data into CA SDM.

**Note:** Some CIs may overlap on the SpectroSERVERs.

### Use Fully Qualified Domain Names(FQDN)

Configure CA Spectrum IM to use Fully Qualified Domain Names (FQDN) to improve the likelihood of matching and reconciling CA SDM CI resources which are imported from CA Spectrum IM, with the resources imported from other MDRs.

See the CA Spectrum IM documentation for instructions on updating the System Name to reference the FQDN.

### Define Services in CA Spectrum IM

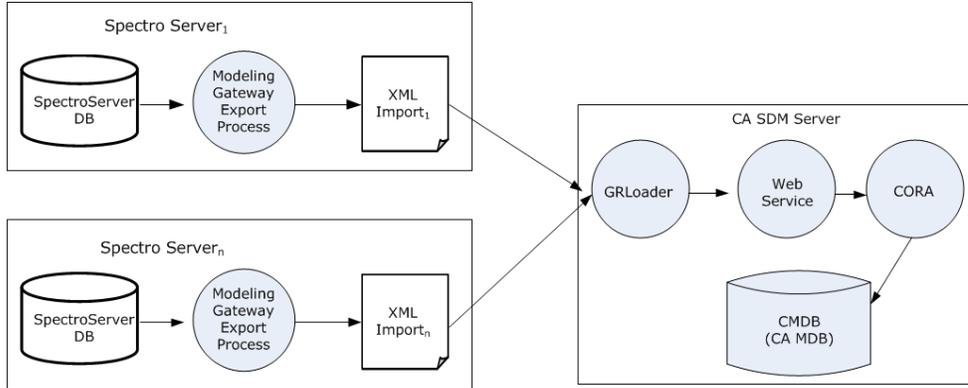
A CA Spectrum IM service model, or service, is an abstract entity. It can represent any process or group of processes, which are identified as ones which a group of resources managed in CA Spectrum are supporting. In fact, any conceivable activity supported by infrastructure resources managed in CA Spectrum can be modeled as a service. A service might typically represent a Web-based retail transaction service, an application server service, a printing service, an email service, a routing service, or a source control service. These are a few familiar examples of the many IT-based services that can be modeled as services in CA Spectrum.

Define services in CA Spectrum IM before integrating with CA SDM. Before you create a service, carefully consider the following factors:

- What the service represents.
- The resources or Spectrum models which affect the viability of the service.
- The level of service viability or service health that can be inferred from the condition of the resources supporting the service.

## How the Integration Works

The following diagram illustrates how data integration between CA Spectrum IM and CA SDM is accomplished:



1. A scheduled job that is external to CA Spectrum IM, such as a Windows Scheduler or Cron job, is used to run the CA Spectrum Modeling Gateway Export utility periodically, with a full export of all models and relationships available for export.

An XML file is created which contains all models and relationships available for export into CA SDM.

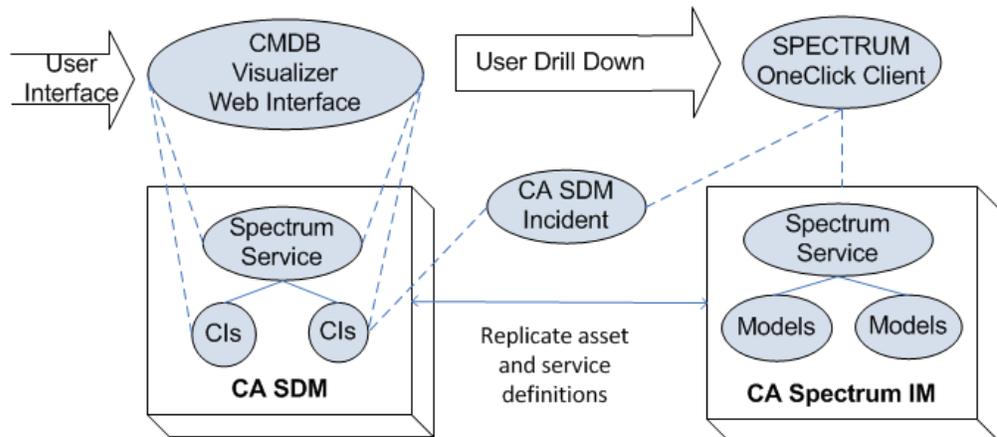
**Note:** This does not include any “delta” information, such as what has been added, changed or deleted.

2. The CA SDM CI Import tool, GRLoader, is then used to load the converted file into CA SDM. Typically, the GRLoader is called by the same script used to call the Modeling Gateway Export. In other words, it is called through the script run by the scheduled job or through a scheduled job on the CA SDM Server.

Once the data is submitted through GRLoader, CA SDM runs the imported data through the CORA reconciliation process.

**Note:** Multiple SpectroSERVERs, as depicted in the example, can run the export utility. As a result, the process must account for data coming from more than one SpectroSERVER – in other words, more than one MDR for CA Spectrum IM.

The following diagram illustrates the end-user interaction with the integration between CA Spectrum IM and CA SDM:



1. The end user is logged into either the CMDB Visualizer directly or through CA SDM to view the CMDB Visualizer through the CI Detail Screen.
2. CIs depicted in the CMDB Visualizer are synchronised with CA Spectrum IM services and models.
3. End users logged into the CMDB Visualizer can access additional CI details by launching in context to replicated asset in CA Spectrum's OneClick client.
4. End users logged into CA SDM and can access additional CI details by launching in context to CA Spectrum's OneClick client when viewing the CI detail screen in CA SDM.
5. End Users can view CA SDM Incidents created from CA Spectrum IM directly from CA SDM or from a link to the incident in the CA Spectrum OneClick Client.

With these considerations in mind, the CA Spectrum IM to CA SDM integration has to be properly designed and the CA Spectrum IM default CMDB resource mapping file may have to be changed to match the requirements of the integration. Execution of the CA Spectrum Modeling Gateway export and the CA SDM GRLoader import processes will also have to be scheduled based on the CMDB update frequency requirements.

### Prerequisites for Integration

- CA SDM r12.6 has been installed and configured.
- CA Spectrum IM 9.2 is installed and functioning in your environment with discovered assets and/or Services defined.
- At least one CA Spectrum OneClick client is installed.
- The integration between CA SDM and CA Spectrum IM is bi-directional. Both applications will send updates to each other on an as-needed basis. In order to accommodate this, the CA Spectrum web server port on the OneClick host must be accessible from CA SDM Server, and vice versa.

## Installation Documentation

CA Spectrum IM 9.2 has a supported integration with CA SDM. This integration is well documented in the Spectrum and CA Service Desk Integration Guide which is included with Spectrum. Although the documentation specifically mentions integration with CA SDM versions r11, r11.1, r11.2, and r12, it is also valid for CA SDM r12.5 and r12.6.

Follow the instructions in the Spectrum and CA Service Desk Integration Guide, shipped with CA Spectrum IM to integrate the two products.

CA Spectrum Infrastructure Manager and CA Service Desk Integration Guide for CA Spectrum r9.2 H04/CA Service Desk r11, r11.1, r11.2, r12. <https://support.ca.com>

Once all the integration steps are successfully completed, you will be able to define CA Spectrum IM alarms that will communicate to CA SDM. CA SDM will create incidents as appropriate and create CIs based on the CA Spectrum model. The CA SDM incident status will be communicated back to CA Spectrum OneClick for defined activity notification methods in CA SDM, such as “Closed” or “Transferred.”

**Note:** The documents listed specifically reference CA SDM r12.5 but are also valid for CA SDM r12.6.

## Export and Import Options

The following CA Spectrum export\CA SDM import options are available by default:

- Device-to-Device This includes the following:
  - Devices that are connected through ports
  - Devices that are directly connected (no ports)
  - Devices that are connected through a fanout
  - Devices that are connected through a WA\_Link (wide area link)
- "Service-to-Device". This includes the following:
  - Devices that are monitored directly by a service
  - Devices with a port that is monitored directly by a service
  - Devices inside a resource monitor that are monitored by a service
  - Devices with a port inside a resource monitor that is monitored by a service
  - Devices that are dynamically added inside a global collection that is monitored by a service
  - Devices statically inside a global collection that is monitored by a service
- "Service-to-Service". This includes the following:
  - Services that are monitored directly by a service
  - Services inside a resource monitor that are monitored by a service
  - Services dynamically inside a global collection that is monitored by a service
  - Services statically inside a global collection that is monitored by a service

## Modify the CMDB Resource Mapping File

The CMDB Resource file, `cmdbresource.xml`, defines the mappings between the CA Spectrum model types and the CA SDM families and classes. The CA SDM classes used must exist in CA SDM. For example, the default mapping values cause exported Cisco routers from CA Spectrum to be classified as Network Switch CIs in CA SDM. If CA Spectrum can distinguish between routers and switches in the infrastructure, you can change the mapping file to include appropriate values.

The default mapping also causes servers exported from CA Spectrum IM to be classified as Other Operating System. As a result, you can change the mapping file if servers are included in the scope of CIs that have CA Spectrum IM as an MDR.

### Follow these steps:

1. Open the `cmdbresource.xml` file located on the CA Spectrum server in a text editor. The default location is: `$SPECROOT/SS-Tools/.cmdbresource.xml`.

The file opens with default mapping values as shown in the following screenshot:

```

<!-- Defines the mappings between CMDB Families/Classes and SPECTRUM model
types. The CMDB classes used must exist in the CMDB or else errors will
be generated. The family attribute is used to group the classes together
for CMDB attribute definitions. -->
<CMDBClassMappings>|
...
<CMDBClassMapping>
  <CMDBClass family="Network" class="Network Switch" />
  <SPECTRUMModelClass>2</SPECTRUMModelClass> <!-- Switch -->
  <SPECTRUMModelClass>4</SPECTRUMModelClass> <!-- Switch-Router -->
  <SPECTRUMModelClass>6</SPECTRUMModelClass> <!-- ATM Switch -->
</CMDBClassMapping>
...
<CMDBClassMapping>
  <CMDBClass family="Hardware" class="Other Operating System"/>
  <SPECTRUMModelClass>9</SPECTRUMModelClass> <!-- Workstation-Server -->
  <SPECTRUMModelClass>113</SPECTRUMModelClass> <!-- File Server -->
</CMDBClassMapping>

```

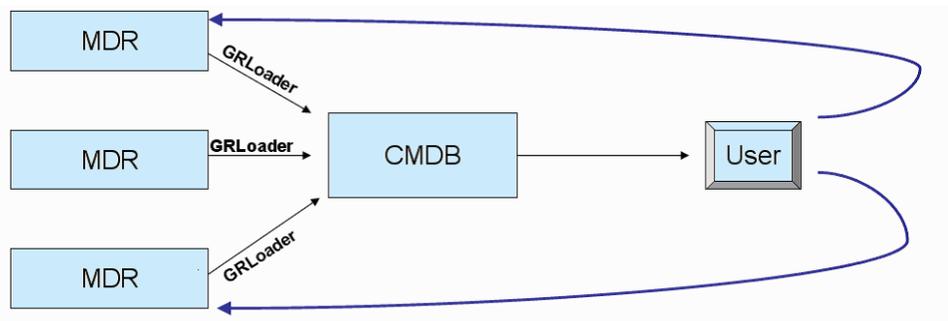
2. Update the file by replacing the CMDB families and classes that you want to map to Spectrum model types.

## Configure CA SDM for the Integration

The following CA Service Desk Manager actions are recommended to support this integration:

- Configure an MDR definition for each CA Spectrum IM object and relationship data source.
- Configure MDR definitions for the CA SOI object and relationship data source.
- Use GRLoader to load data from remote MDRs.

The CA SDM GRLoader utility provides facilities for importing and loading CIs into the CMDB and also for associating CIs with their origins. Additionally, by using the MDR Launcher capability when viewing a CI in CA SDM, you can navigate seamlessly back into the system from which the CI originated, as shown in the following diagram:



CA SDM provides the transaction work area (TWA) for inspecting and modifying CI and relationship data before you load the data into the CMDB. You can load data into the transaction work area using GRLoader with the `-littwa` (load to TWA) option.

In TWA mode, instead of creating CIs and relationships directly, GRLoader inserts the information into the transaction work area tables.

For more information on using GRLoader and loading CI data into the TWA, refer to the CA Service Desk Manager r12.6 Administration Guide.

## Define the CA Spectrum MDR

Define the CA Spectrum IM as an MDR Provider before importing managed object and relationship information from CA Spectrum IM into CA SDM. A separate MDR definition is created for each CA Spectrum IM object and relationship data source. Environments with several SpectroSERVERs require separate MDR definitions. If all the SpectroSERVERs are members of a single CA Spectrum IM distributed SpectroSERVER environment only one MDR needs to be defined for CA Spectrum IM OneClick. CA Spectrum OneClick MDR

### Create an MDR Launch for CA Spectrum OneClick

To enable launch of CA Spectrum OneClick, do the following:

1. Login to CA SDM as an Administrator and select the Administration tab.
2. Expand the CA CMDB node and click MDR Management.
3. Click the MDR List.
4. Click Create New. Provide information for the following fields:
  - **Button Name:** OneClick
  - **MDR Name:** OneClick
  - **MDR Class:** SPECTRUM
  - **Active:** Active
  - **Owner:** ServiceDesk
  - **Description:** Context launch for CA Spectrum OneClick.
  - **Hostname:** <your CA Spectrum OneClick server host>
  - **Port:** <your CA Spectrum OneClick server port> Default: 80
  - **Path:** /spectrum/oneclick.jnlp
  - **Parameters:** topology={federated\_asset\_id}
  - **URL to launch in Context:** http://{hostname}:{port}/{path}?{parameters}
5. Click Save
 

A success message saying that the the MDR was created appears.
6. Click Close.

## Setting up the Service Dashboard Launch

To enable launch of the Service Dashboard do the following:

1. Login to CA SDM as an Administrator and select the Administration tab.
2. Expand the CA CMDB node and click MDR Management.
3. Click the MDR List.
4. Click Create New. Provide information for the following fields:
  - **Button Name:** SLM Dashboard
  - **MDR Name:** ServiceManager
  - **MDR Class:** SPECTRUM
  - **Active:** Active
  - **Owner:** ServiceDesk
  - **Description:** Context launch for Service Manager CI.
  - **Hostname:** <your CA Spectrum OneClick server host>
  - **Port:** <your CA Spectrum OneClick server port>
  - **Path:** /spectrum/oneclick.jnlp
  - **Parameters:** mh={federated\_asset\_id}
  - **URL to launch in Context** (no spaces):  
`http://{hostname}:{port}/{path}?-app=com.aprisma.spectrum.slm.SLMDashBoardConsole@slm?{parameters}`
5. Click Save .

A service message saying that the MDR was created appears.
6. Click Close.

## Use GRLoader to Copy Data from Remote MDRs

An MDR is considered remote if it is not installed on the same system as the CA SDM. GRLoader can be used to copy data from a remote MDR to CA SDM in either of two ways:

- Copy the XML data from the remote system which runs the MDR to the system running CA SDM and execute GRLoader on the CA SDM system.
- Execute GRLoader on the remote MDR system itself.

To prepare and execute GRLoader from a remote system, perform the following tasks on the SpectroSERVER:

1. Create `$SPECROOT\custom\grloader` directory for GRLoader to reside in.
2. Copy the contents of the `%NX_ROOT%\java\lib` directory from the CA CMDB system to a directory on the remote system that you want to run it on. This will be called the `%ROOT%` system.
3. Create directory `%ROOT%\site\cfg`
4. Create directory `%ROOT%\log`
5. Create a file called `NX.ENV` in the `%ROOT%` directory. Add the following line to the file:  
`@NX_LOG=<path_which_will_contain_log_files, defined in the previous step.`

For the SpectroSERVERs it is a best practice is to install Install GRLoader in `$SPECROOT\custom\GRLoader` on the SpectroSERVER.

This will protect the GRLoader install during CA Spectrum upgrades or patches as the `$SPECROOT/custom` directory is protected/retained during either of these processes.

**Note:** When GRLoader is first run it converts the contents of the `<GRLOADERDIR>\NX.ENV` file into the `<GRLOADER>\site\cfg\GRLoader.properties` file. If you ever update the `NX.ENV` file (for example, because you moved GRLoader to a different directory) delete or rename the `<GRLOADER>\site\cfg\GRLoader.properties` file and let GRLoader create the new/updated `GRLoader.properties` file.

6. Export CA Spectrum CI data to load into CA SDM. One way to do this is with the Modeling Gateway command line tool, `modelinggateway.bat`. This file is located under the `SS-Tools` directory on the CA Spectrum IM server. Refer to the CA Spectrum Infrastructure Manager Integration Guide for instructions on how to use the Modeling Gateway command line tool.
7. Execute the following command to run GRLoader from the system where you installed GRLoader:

```
java -cp %ROOT% -jar %ROOT%/GRLoader.jar -N %ROOT% -u [userid] -p [password]
-s [SDM server URL including port] -i [other GRLoaderxml import file name
options]
```

%ROOT% is the fully qualified path containing the files copied.

The integration is complete. When a Configuration Item is created from CA Spectrum IM, the Configuration Item Detail page for that CI in CA SDM will have a OneClick button on the Attributes tab. When the OneClick button is clicked, a launch in context of the CI is done into Spectrum OneClick.

### CI Import Notes

Consider the following when integrating CA Spectrum and the CMDB component of CA SDM:

- If you are using the CA Spectrum Modeling Gateway tool, complete the CI extraction and load only once, in case you are also populating server information with CA Configuration Automation at the same time. You should use CA Configuration Automation with the CMDB Export Report only to populate the Server attributes and build out the Virtual Machine environment. A second run of the CA Spectrum Modeling Gateway tool overrides the CA Configuration Automation data and the proper class and families which would result in having to re-import all of the CA Configuration Automation servers into the CMDB again.
- CA Spectrum builds peer-to-peer relationships with the out of the box CMDB mapping file that it uses. The peer-to-peer relationship does not allow you to perform Impact and Root Cause analysis.
- Currently, all of the CI server information is extracted and passed to the CMDB when an extract is run, not just the new CIs. You can use the CA Catalyst to perform this task. You can run the Spectrum extract and place it on a server that is discovered by Configuration Automation. A simple Configuration Automation blueprint for this XML data would be used to identify the new CIs in the file, and then used to send only the new CIs to the CMDB.

### Troubleshooting

The integration can be debugged from the CA Spectrum side by reviewing the CA Spectrum Tomcat log in the following location:

*Spectrum\_Install\_Directory\win32app\Spectrum\tomcat\logs\stdout.log*

### Special Characters in FQDN fail with OneClickIntegrationSetup.exe

The OneClickIntegrationSetup.exe program currently has a bug that fails to check the formation of the server FQDN value, if the FQDN has special characters in the domain portion.

**Example:** samepleserver.my-domain.co.uk

As a workaround, enter ANY alpha-numeric based value for the server when prompted (example: ABC123.sample.com), and continue with the configuration using valid values for the rest of the attributes, so that the \$NX\_ROOT/bin/oc-integration.cfg file is created.

After the configuration completes, you can manually edit the oc-integration.cfg file and replace the server value with the correct server FQDN.

**Example:** sampleserver.my-domain.co.uk

### CA SDM r12.6 and CA Spectrum r9.2 Hotfixes

+CA Spectrum Infrastructure Manager r9.2 H04 is the fourth cumulative hot fix rollup for Spectrum r9.2, and the integration with CA SDM r12.6 works as designed. This hot fix contains significant updates and improvements to the base r9.2 release as well as to the r9.2 H03 release.

Integrating CA Spectrum Infrastructure Manager 9.2 (hot fix H03 applied) with CA SDM r12.6, as documented in the CA SDM r12.6 release notes, produces the following issue:

- When an alarm is triggered through CA Spectrum, the associated service desk ticket is not automatically created in CA SDM as expected. A solution is still being worked out.

## Introducing CA Service Operations Insight into the Solution

---

CA Service Operations Insight (CA SOI), formerly known as CA Spectrum Service Assurance (CA SSA), helps unify the health and availability of information from domain management tools and aligns that information to IT services. CA SOI pulls data from the domain management systems such as CA SDM, CA APM, Spectrum IM, and eHealth and presents it in a single view. CA SOI detects infrastructure or service alert conditions, and uses escalation policies to automate the process of raising a CA SDM incident for that condition.

The process of building services in CA SOI is done through the Service Modeler in the CA SOI Operations Console. Service Models can be built using CIs from integrated products such as CA NSM, CA Spectrum IM, eHealth, CA APM, and CA SDM.

## Integration Points and Value

CA SOI integrates with CA SDM for event, availability and incident management as follows:

- CA SDM incidents are automatically created via web services based on CA SOI alert escalation policies or can be manually submitted from the CA SOI Operations Console.
- The incident number is added to the CA SOI alert and associates the incident with the alert. The alert data provides a description of the problem for the ticket.
- The CA SOI “assignee” alert property can be synchronized with the CA SDM incident Assignee so that if one is set, the other is set to the same value.
- The modeling of the infrastructure is maintained in the CMDB component of CA SDM. The CIs that the infrastructure solutions manage are imported into the CMDB component, associated to a Management Database Repository (MDR), and visualized at a service layer.
- The CA SOI Service Console can provide quick drill-down capability to service detail in the CA SDM incident. Clicking the incident number within CA SOI lets you launch CA SDM in context to view the incident details.
- After the associated problem is resolved, the CA SOI alert and CA SDM incident can be synchronized so that if one is cleared, the other is cleared automatically.
- The SOI Dashboard presents the quality level of a service, the measure of the end-user experience when using a service, by showing the number of CA SDM incidents against the service in the Quality column.
- CA SOI support synchronization of all CI types and relationships from CA SOI to CA SDM.

## CA SOI Integration Details

CA SOI r3.0 has a supported integration with CA SDM r12.5 and r12.6. This integration is well documented in the Configure Help Desk Integration section of the CA Service Operations Insight Administration Guide r3, shipped with CA SOI.

The CA SOI integration is only an import into CA SOI from the CA SDM CMDB component at the time of this chapter being written. The current Service Desk Catalyst Connector is 2.5.

### Prerequisites for Integration

- CA SDM r12.6 is installed and configured.
- The following CA Service Operations Insight r3.0 Components are installed and configured:
  - Manager
  - User Interface Server
  - Universal Connector Client
- The latest CA SOI 3.0 cumulative update release patch is installed.
- CA Spectrum IM 9.2 is installed and configured (Optional).

### Installation Documentation

To configure the integration between CA SDM and CA SOI follow the instructions in the Configure Help Desk Integration section in Chapter 3 of the CA Service Operations Insight Administration Guide r3 shipped with CA SOI.

This document specifically references CA SDM r12.5 but is also valid for CA SDM r12.6.

## CA Event Integration

A connector is software that provides the interface for data exchange between the CA Catalyst infrastructure and a domain manager. Connectors are the gateway through which data is retrieved from various domain managers for consolidated management. Each integrated product has its own connector that supports outbound, inbound or both types of operations.

In order to allow CA SOI to gather accurate and timely information from monitored applications, Connectors must -be installed.

Event management is crucial to understanding the dynamic state of an enterprise across network, security, system, application, service, and other domains. As the number of resources grow exponentially, so do the challenges of understanding and administering diverse management events from those resources.

CA SOI provides an event connector, which uses CA Event Integration technology, to integrate raw event sources with CA SOI. The connector collects events from the sources, transforms them into the CA SOI alert format, and displays them as infrastructure alerts in CA SOI. The connector creates CIs automatically for objects associated with alerts, such as servers, routers, and CPUs. You can then create services from the created CIs to manage the event sources from a service-oriented perspective. This in turn creates incidents and CIs in CA SDM when configured to do so.

CA Event Integration is a lightweight event integration and processing solution that collects events from diverse sources, normalizes them into a common format with uniform semantics, and dispatches the reformatted and enhanced events to an event manager for subsequent actions. Implementing and deploying CA Event Integration in a complex distributed environment can result in a unified event management system with a common format for all events, regardless of their source.

CA Event Integration collects events from the following sources and send them to CA SOI:

- CA NSM Event Management (Windows only)
- Operating system sources such as the Windows Event Log
- CA OPS/MVS Event management and Automation
- CA SYSVIEW Performance Management
- HP Business Availability Center
- Device sources such as SNMP traps
- Web services events

CA Event Integration transforms events from these sources so that all events reporting a similar problem look the same, making events easier to classify, understand, and ultimately simpler to resolve. During processing, the product can also enrich events with supplemental information from any external source, increasing event quality and facilitating more effective diagnostics and automation at the event destination.

For more information, including installation instructions, refer to the CA Event Integration product documentation on <https://support.ca.com>.

## CA Event Integration Connector

CA SOI provides an event connector, which uses CA Event Integration technology, to integrate raw event sources with CA SOI. The connector collects events from the sources, transforms them into the CA SOI alert format, and displays them as infrastructure alerts in CA SOI. The connector creates CIs automatically for objects which are associated with alerts, such as servers, routers, and CPUs. You can then create services from the created CIs to manage the event sources from a service-oriented perspective. This in turn creates incidents and CIs in CA SDM when configured to do so.

CA Event Integration collects events from the following sources and sends them to CA SOI:

- Event management sources such as CA NSM, CA Spectrum Infrastructure Manager (CA Spectrum), CA SOI
- Operating system sources such as the Windows Event Log
- CA OPS/MVS Event management and Automation
- CA SYSVIEW Performance Management
- Application sources such as text log files
- Device sources such as SNMP traps
- Web services events

CA Event Integration transforms events from these sources so that all events reporting a similar problem look the same, making events easier to classify, understand, and ultimately simpler to resolve. During processing, the product can also enrich events with supplemental information from any external source, increasing event quality and facilitating more effective diagnostics and automation at the event destination.

For more information, including installation instructions, refer to the CA Event Integration product documentation on <http://support.ca.com>.

CA Event Integration 3.0 ships as a component of CA SOI, installable from the CA SOI installation media. To install the connector, refer to the installation instructions shipped with the CA SOI media.

## CA Spectrum IM Connector

The Catalyst Connector installation file, Connector\_SpectrumIM\_921.exe, for Spectrum IM, 2.5 can be downloaded from the CA Support web site, under Published Solutions in the Download Center. To install the connector, select CA Service Operations Insight release 2.5.

### Follow these steps:

1. Download the CA Spectrum IM Connector from CA Support.
2. Add the remote connector system to the Server List on the SpectroSERVER, if you are not installing the connector locally on the SpectroSERVER. The remote connector system is the server on which you install the CA Spectrum IM Connector.
3. On the remote connector system prepared in the previous set, or the SpectroSERVER, copy the entire SAM directory from the CA Service Operations Insight r3.0 media locally. For example, to C:\Downloads\SAM.
4. Copy the spectrum connector file, Connector\_SpectrumIM\_921.exe, to the directory created previously. For example: C:\Downloads\SAM folder.
5. Double click the C:\Downloads\SAM\Connector\_SpectrumIM\_921.exe to initiate the installation.
6. Complete the installation following the instructions in the CA Catalyst CA Spectrum Infrastructure Manager Connector Guide.

## CA Service Desk Manager Connector

Before installing the Service Desk Manager 2.5 connector on either the CA SDM Primary server or a CA SDM Secondary Server, install the Integration Services . The SOI 3.0 Integration Services for Connectors is provided to facilitate the installation of the current suite of Catalyst 2.5 connectors, such as the Service Desk Manager 2.5 connector, with CA SOI 3.0.

The Integration Services Catalyst Connector can be downloaded from the CA Support web site, under Published Solutions in the Download Center. Select CA Service Operations Insight release 3.0. To install Integration Services, select WIN-SOI 3.0 Integration Services for Connectors, from the Published Solutions Downloads page.

### Follow these steps:

1. Download the SOI 3.0 Integration Services from CA Support.
2. Copy the entire SAM directory from the CA Service Operations Insight r3.0 media locally to the CA SDM Primary or a Secondary server, for example to C:\Downloads\SAM.
3. Copy the Integration Services file and the IntegrationServices.exe, to the directory created previously. For example C:\Downloads\SAM folder.
4. Double click the C:\Downloads\SAM\IntegrationServices.exe to initiate the installation.
5. Open the Services window and validate that a new service named CA SAM Integration Services has been added and its Status is Started.

The Catalyst Connector for Service Desk Manager, 2.5 can be downloaded from the CA Support web site, under Published Solutions in the Download Center. To install the Service Desk Connector, select CA Service Operations Insight release 2.5.

### Follow these steps:

1. Download Catalyst Connector for Service Desk Manager 2.5, Fix#RO25052, from support.ca.com.
2. Copy the Catalyst Connector for Service Desk Manager 2.5 file, Connector\_ServiceDeskManager.exe, to the directory created previously. For example C:\Downloads\SAM folder.
3. Double click C:\Downloads\SAM\ Connector\_ServiceDeskManager.exe to initiate the installation.

4. Follow the installation instructions in the documentation which is shipped with the connector. During the installation you will be asked to enter the top-level class and class family:
  - a. **Top Level Class Family:** Specifies the top-level class family to import from CA SDM into CA SOI as a service. You can enter a comma-separated list of families and classes in this field. Format: Service, Enterprise Service.
  - b. **Top Level Class:** Specifies the top-level class to import from CA SDM into CA SOI as a service. You can enter a comma-separated list of families and classes in this field. Format: Service, Infrastructure Service, Business Service.

The screenshot shows the CA Service Desk Manager Administration console. On the left is a navigation tree with 'CA Cmdb' expanded to 'CI Classes'. The main area displays a table titled 'Configuration Item Class List' with the following data:

Class	Family
Business Service	Enterprise Service
Infrastructure Service	Enterprise Service
Other Service	Enterprise Service

Below the table is a 'Service Desk Manager Connector Configuration' dialog box. It contains the following fields:

- Service Desk Manager Connector User:** ServiceDesk
- Service Desk Manager Connector Password:** \*\*\*\*\*
- Top Level Family:** Enterprise Service
- Top Level Class:** Business Service

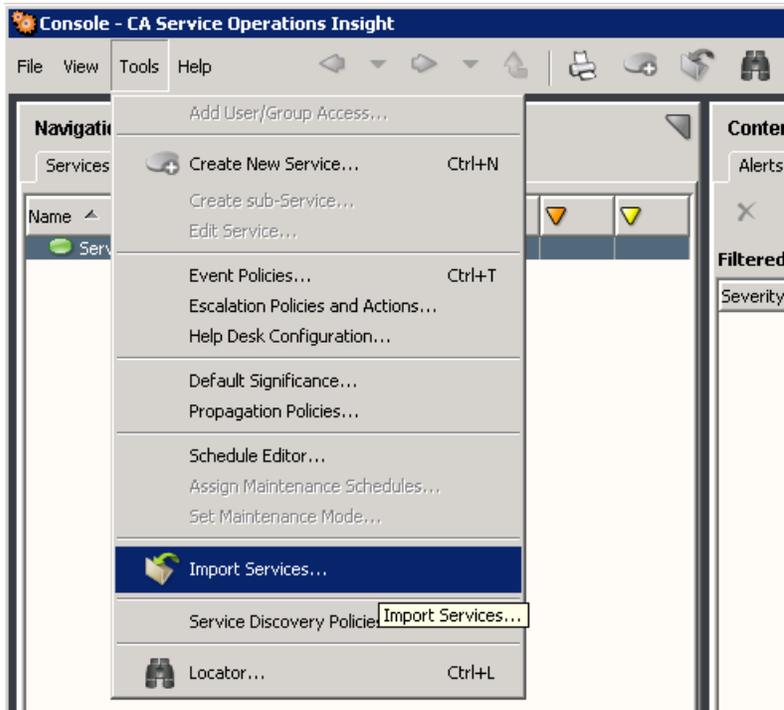
At the bottom of the dialog are 'Cancel', 'Previous', and 'Next' buttons. The footer of the console reads 'Copyright © 2011 CA. All rights reserved.'

## Import Services to CA SOI

Once the connectors for CA Spectrum IM and CA SDM are installed, services that have been previously created in either application can be imported into CA SOI.

### Follow these steps:

1. Login to the CA SOI Console.
2. From the menu, select Tools, Import Services.



3. The Configure Data Sources window launches and presents the available data sources.
4. Select the source that the Service exists in. For example, to select CA Spectrum IM Services or ServiceDeskCMDB running on host <ServerName>”, select the data source with a Source Description of SpectrumInfrastructureManager running on host <ServerName>.

The Import Services window launches.

5. Select the Services to import and click OK.
6. The Configure Data Sources window reappears. The Import Status displays as Waiting.

## Introducing eHealth into the Solution

---

### What is eHealth

eHealth Performance Manager (eHealth) provides the real-time and historical performance reporting and analysis. eHealth is able to trend and baseline all KPIs to provide intelligent alerting for deviation from normal and time over threshold conditions.

### Integration Value

Events from CA eHealth can open tickets in CA SDM directly or through CA Spectrum. Passing CA eHealth events through CA Spectrum is the recommended approach to creating tickets in CA SDM. The CA Spectrum integration, described previously is then utilized to manage CA eHealth events.

- The addition of CA eHealth into the environment helps maintain critical service levels across complex network environments by combining CA eHealth's automated availability and performance management with the CA Spectrum network service and analysis platform.
- CA SDM stores capacity and availability level violations received from tools such as CA Spectrum as Incidents against a specific CI. Incidents are opened in CA SDM for a capacity violation reported to CA Spectrum from CA eHealth due to a performance violation.
- CA Spectrum IM and CA eHealth collect availability and performance data against all Infrastructure elements and allow you to group any of these Infrastructure elements into IT Services and run reports against them. Incidents opened against service, system, or component utilization violations are stored in the CA Management Database (CA MDB).
- CA eHealth is able to leverage historical performance and capacity patterns to identify when a device or component has deviated from the norm, which will result in Incidents in CA SDM.

### Configuring the Integration

To configure CA eHealth to pass event data to CA Spectrum to open incidents in CA SDM, refer to the instructions in the *CA eHealth Performance Manager and CA Spectrum Infrastructure Manager Integration and User Guide for CA eHealth r6.2/CA Spectrum r9.2*.

## Introducing CA Application Performance Management into the Environment

---

### What is CA Application Performance Management

CA APM allows you to monitor, analyze, and report on transactions throughout your IT environment whether physical, virtual or in the cloud so you can quickly identify issues and resolve problems before they disrupt critical services. Innovative transaction performance management capabilities also let you prioritize problem resolution according to business impact.

CA Application Performance Management (APM) provides predictive performance analysis of application software degradations, such as advance warnings of SLA violations, and detailed application, application server, web server and portal software root cause determination.

CA APM solution has two main components, end-user experience monitoring (CEM) and application deep-dive using Introscope agents. CEM provides detailed end-user response measurements which are mapped to specific business transactions. It measures 100% of all transactions from HTML-based web applications. CA CEM's Introscope agents provide deep visibility and diagnostics into Java and .NET applications with automatic discovery of Web Services, SOA dependency mapping and cross enterprise tracing even into the Mainframe via CICS, Web Services, or MQ.

### Integration Value

- The CA SOI Console provides cross-domain visibility throughout the infrastructure and applications for each IT service when integrated with CA Application Performance Management and CA eHealth Network Performance Management.
- CA APM can individually measure end-user performance of all critical business transactions for defined service. When CA APM detects a large number of users experiencing slow response times with a transaction, it sends an Alarm detailing this degradation in service quality to CA Spectrum IM or CA SOI, resulting in an incident in CA SDM.
- The Introscope agent inside the application's Java Virtual Machine (JVM) can also record a spike in response times for a critical Web Service component of a service. It sends an alarm to CA Spectrum or CA SOI showing the increase in Risk, resulting in an incident in CA SDM.

## Single Sign ON with CA Embedded Entitlements Manager

---

Single Sign-On can be configured in both CA SDM and CA Spectrum IM to utilize either a CA SiteMinder Policy Server or a CA Embedded Entitlements Manager (EEM) server for processing user authentication. In both cases, user access control is still maintained through the respective applications, that is, CA SDM or CA Spectrum IM. CA Spectrum IM users must be configured with appropriate access controls within the Spectrum application before a successful login can occur while contacts in CA SDM must have an appropriate Access Type associated with the user ID.

A single instance of CA Embedded Entitlements Manager (EEM) can be used for user authentication for:

- CA SDM
- CA Spectrum IM OneClick console
- CA SOI Manager and CA SOI UI Server components

The OneClick console can be configured to utilize EEM as the external authentication source for authenticating users against the Spectrum User database.

For CA Spectrum IM, the Single Sign-On configuration is performed through the Spectrum OneClick web administration GUI. For CA SDM, the configuration is performed through the Option Manager settings.

For CA SOI, the EEM server connection parameters are specified during the CA Service Operations Insight installation. An EEM Application Name of SSA-<SOI\_ServerName> is created.

Install the CA EEM server on its own separate server.

## Summary

---

The integrated solution addresses how different IT domains can contribute to business service degradation and how the end-to-end service assurance solution is designed to integrate the monitoring of those domains, correlate data across those domains and provide root cause analysis when service degradations occur. The end result is an understanding of how IT supports and aligns to the business, reduces the amount of time, effort and resources it takes to resolve service disruptions and begin to proactively identify IT problems before they impact service delivery.

- CA Service Operations Insight – CA SOI pulls data from the domain management systems (Spectrum IM, eHealth, etc.) and presents it in a single pane of glass. It provides service impact analysis, service visualization and integration to service management and the CMDB.
- Spectrum Infrastructure Manager – Spectrum IM is the infrastructure management console. It provides discovery and relationship mapping, topology views, event management, and root cause analysis, and network configuration management for the entire infrastructure (networks, physical and virtual systems, etc).
- eHealth Performance Manager – eHealth is what provides the real-time and historical performance reporting and analysis. eHealth is able to trend and baseline all KPIs to provide intelligent alerting for “deviation from normal” and “time over threshold” conditions.
- CA CEM – CA Customer Experience Manager provides detailed application transaction data. It measures application transaction data for all transactions all the time for Java and .NET applications. CEM provides critical insight into service quality, based on the overall response of the user experience.